

Scan Results

07/08/2015

The scan was started on 07/08/2015 at 06:05:33 and took 03:28:17 to complete. The scan was run against the following IP addresses:

Not a certified PCI report

IP Addresses

23.227.38.71

The scan option profile used includes:

Scan Settings

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
Overall Performance	Custom
Hosts to Scan in Parallel-External Scanner	10
Hosts to Scan in Parallel-Scanner Appliances	10
Processes to Run in Parallel-Total	10
Processes to Run in Parallel-HTTP	1
Packet (Burst) Delay	Maximum

Advanced Settings

Host Discovery	TCP Standard Scan
	UDP Standard Scan
	ICMP On
Ignore RST packets	Off
Ignore firewall-generated SYN-ACK packets	Off
ACK/SYN-ACK packets during discovery	Send

Report Summary	
Company:	CultureLabel UK Ltd
User:	Alex Stanhope
Template Title:	Scan Results
Active Hosts:	1
Total Hosts:	1
Scan Type:	On Demand
Scan Status:	Finished
Scan Title:	cl-shopify-www-only (medium-low impact)
Scan Date:	07/08/2015 at 06:05:33
Reference:	scan/1436335540.65121
Scanner Appliance:	64.39.105.41 (Scanner 7.15.28-1, Vulnerability Signatures 2.3.58-3)
Duration:	03:28:17
Options:	Payment Card Industry (PCI) Options
Target:	23.227.38.71

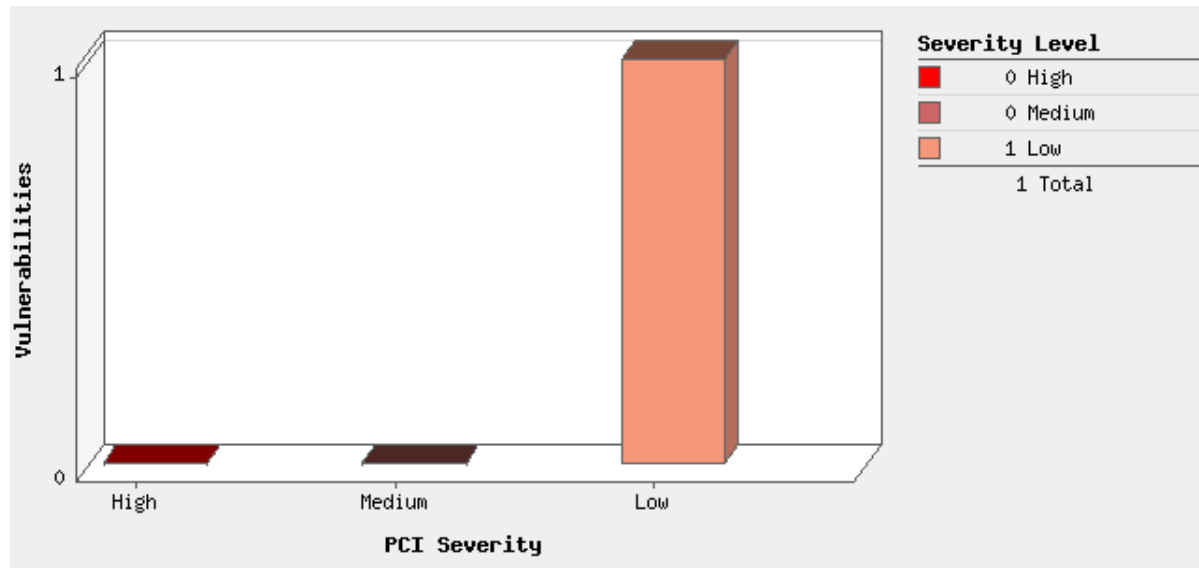
Summary of Vulnerabilities

Vulnerabilities Total	33	Average Security Risk		3.0
-----------------------	----	-----------------------	---	-----

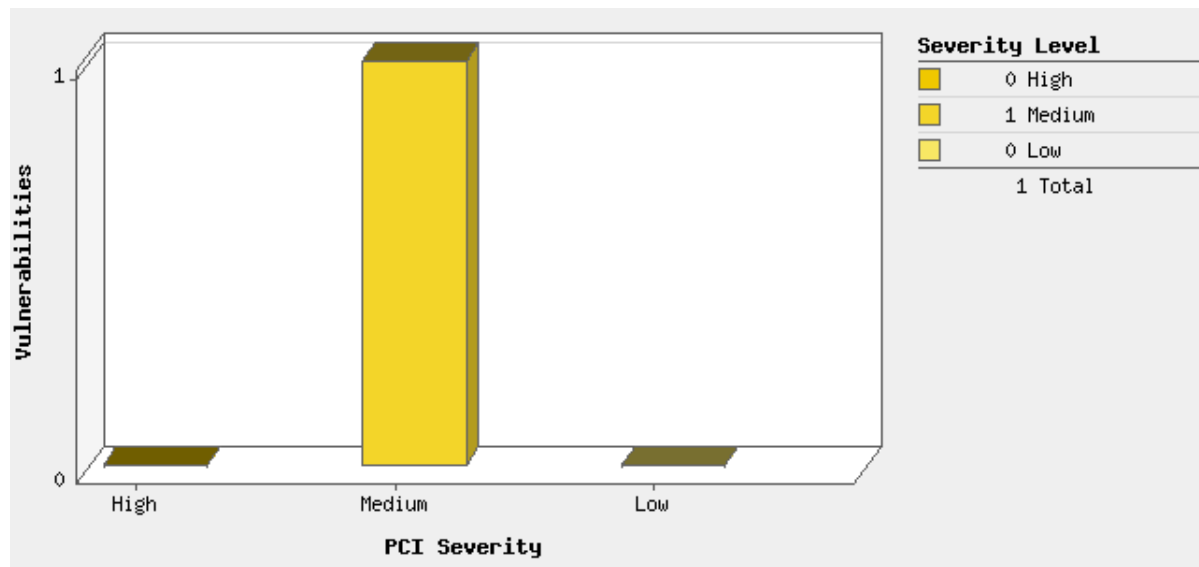
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	1	1	1	3
2	0	0	3	3
1	0	0	27	27
Total	1	1	31	33

by PCI Severity			
PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	0	1	1
Low	1	0	1
Total	1	1	2

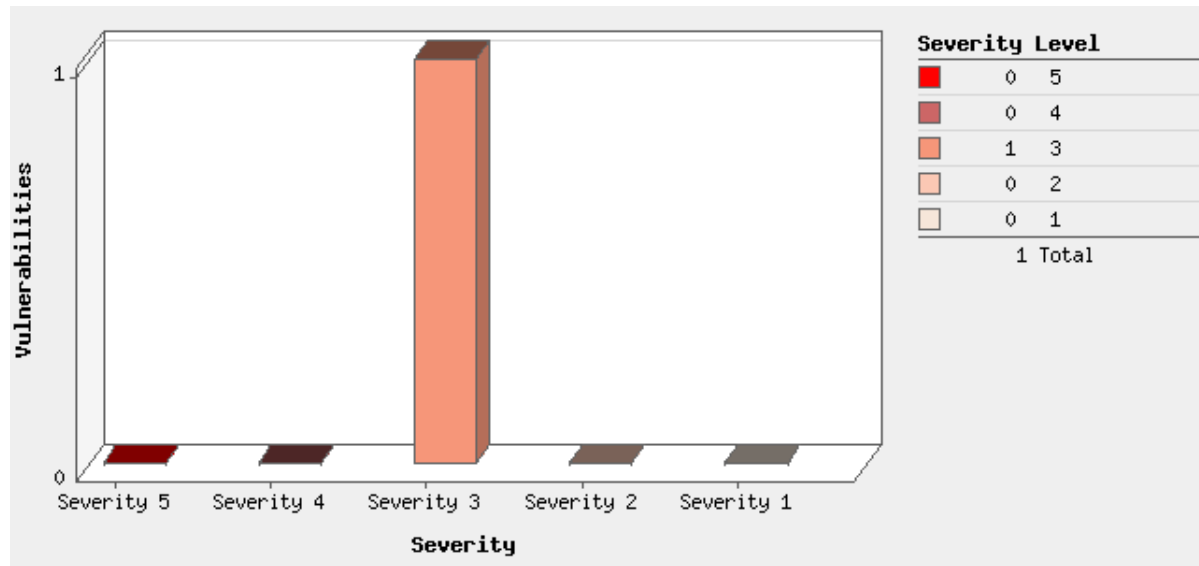
Vulnerabilities by PCI Severity



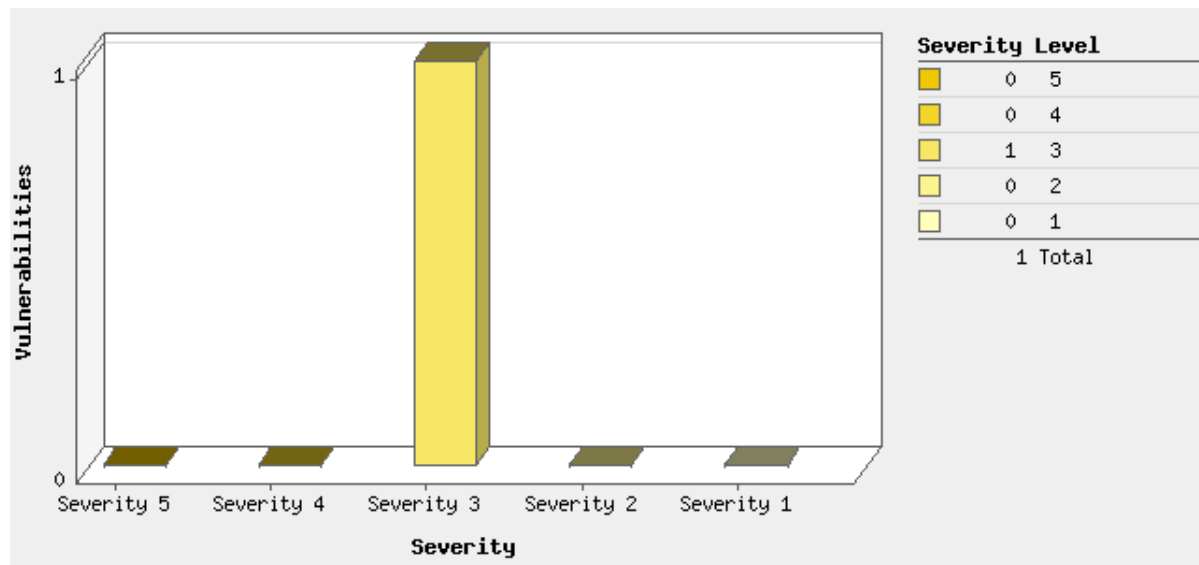
Potential Vulnerabilities by PCI Severity



Vulnerabilities by Severity



Potential Vulnerabilities by Severity



Detailed Results

23.227.38.71 (23-227-38-71.shopify.com,-)

Vulnerabilities Total

33

Security Risk



3.0

Compliance Status

FAIL

Vulnerabilities (1)

TCP Source Port Pass Firewall

PCI COMPLIANCE STATUS

PCI Severity:

LOW

FAIL

VULNERABILITY DETAILS

CVSS Base Score: 0

CVSS Temporal Score: 0

Severity: 3

QID: 34000

Category: Firewall

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 04/13/2009

THREAT:

Your firewall policy seems to let TCP packets with a specific source port pass through.

IMPACT:

Some types of requests can pass through the firewall. The port number listed in the results section of this vulnerability report is the source port that unauthorized users can use to bypass your firewall.

SOLUTION:

Make sure that all your filtering rules are correct and strict enough. If the firewall intends to deny TCP connections to a specific port, it should be configured to block all TCP SYN packets going to this port, regardless of the source port.

RESULT:

The host responded 4 times to 4 TCP SYN probes sent to destination port 20 using source port 80. However, it did not respond at all to 4 TCP SYN probes sent to the same destination port using a random source port.

Potential Vulnerabilities (1)

Slow HTTP POST vulnerability

port 80/tcp

PCI COMPLIANCE STATUS


PCI Severity:

MED

PASS

This denial of service is out of scope of PCI.

VULNERABILITY DETAILS

CVSS Base Score: **6.8** AV:A/AC:L/Au:N/C:N/I:P/A:C
CVSS Temporal Score: **6.1** E:H/RL:U/RC:UC
Severity: **3** 
QID: 150085
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/02/2011

THREAT:

Application scanner discovered, that web application is probably vulnerable to slow HTTP POST DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending properly crafted HTTP POST headers, that contain a legitimate Content-Length header to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources. By waiting for complete request body, server supports clients with slow or intermittent connections
More information can be found at the in this presentation.

IMPACT:

All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:

Solution would be server-specific, but general recommendations are:
- to limit the size of the acceptable request to each form requirements
- establish minimal acceptable speed rate
- establish absolute request timeout for connection with POST request
Easy to use tool for intrusive testing is available here.

RESULT:

url: http://23.227.38.71/
matched: Vulnerable to slow HTTP POST attack

Server resets timeout after accepting request data from peer.


Information Gathered (31)

HTTPS Compression Information Retrieval

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **3** 
QID: 42416
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 08/10/2013

THREAT:

HTTP data is compressed before it is sent from the server

The following is a list of supported HTTP Compression methods on remote server.

HTTP/1.1 404 Not Found
Server: nginx
Date: Wed, 08 Jul 2015 06:51:02 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Sorting-Hat-PodId: -1
Vary: Accept-Encoding
Status: 404 Not Found
X-XSS-Protection: 1; mode=block; report=/xss-report/bd23c239-2ec2-437b-a309-9e549a006571?source%5Baction%5D=index&source%5Bcontroller%5D=shop&source%5Bsection%5D=storefront
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Security-Policy-Report-Only: default-src 'self' https: safari-extension: chrome-extension-resource: chrome-extension: chromeinvoke: chromeinvokeimmediate: webviewprogressproxy: webkit-fake-url: chromenull: blob; connect-src 'self' https: safari-extension: chrome-extension-resource: chrome-extension: chromeinvoke: chromeinvokeimmediate: webviewprogressproxy: webkit-fake-url: chromenull: blob; wss:; font-src 'self' https: safari-extension: chrome-extension-resource: chrome-extension: chromeinvoke: chromeinvokeimmediate: webviewprogressproxy: webkit-fake-url: chromenull: blob; data:; frame-src 'self' https: safari-extension: chrome-extension-resource: chrome-extension: chromeinvoke: chromeinvokeimmediate: webviewprogressproxy: webkit-fake-url: chromenull: blob; data:; img-src 'self' https: safari-extension: chrome-extension-resource: chrome-extension: chromeinvoke: chromeinvokeimmediate: webviewprogressproxy: webkit-fake-url: chromenull: blob; data:; media-src 'self' https: safari-extension: chrome-extension-resource: chrome-extension: chromeinvoke: chromeinvokeimmediate: webviewprogressproxy: webkit-fake-url: chromenull: blob; data:; object-src 'self' https: safari-extension: chrome-extension-resource: chrome-extension: chromeinvoke: chromeinvokeimmediate: webviewprogressproxy: webkit-fake-url: chromenull: blob; script-src 'self' https: safari-extension: chrome-extension-resource: chrome-extension: chromeinvoke: chromeinvokeimmediate: webviewprogressproxy: webkit-fake-url: chromenull: blob; 'unsafe-inline' 'un
safe-eval'; style-src 'self' https: safari-extension: chrome-extension-resource: chrome-extension: chromeinvoke: chromeinvokeimmediate: webviewprogressproxy: webkit-fake-url: chromenull: blob: 'unsafe-inline'; report-uri /csp-report/bd23c239-2ec2-437b-a309-9e549a006571?source%5Baction%5D=index&source%5Bcontroller%5D=shop&source%5Bsection%5D=storefront;
X-Request-Id: bd23c239-2ec2-437b-a309-9e549a006571
Content-Encoding: gzip

8b7

_1F_8B_08_00_00_00_00_00_03_CDY_EBs_DB6_12_FF_EE_BfBM%g_A9_16_1F_92_Y_D6+_938_CELfz_D3_BB:_FD_D0v:_10
lpH_82_07@_96U_D7_FF_FB-_C0_87H_89_BA_A8_B9_DC_DC_D9_F1_88Z_EC_FE_F6b_91_C9y_C0)

_B5M(_ACT_14_CE_CE&_E7_B6_FD3[@_A8_E0_E3_1D\ _FF:_83_89^_00?SRN_AD_98_DB_0F_12_18
_1D_00_0F_03F-_08L_BC_9CZ4_B6_90_F1_FCg_1A_07L_F1_AbM_EFp_FE_1D_C8_F5_9F_00_19_1E_03_19_9E
_B2T_19_8E&_D4_81_EDA_D8v_05_E6l_B2_A2\$ _98_9D_81Y_82_BFRE@_D3_F1{ _A4_9F_FD_15_11_92_AA_A9_F5_E3_A7_0F_F6_D0_D2_0B_B8_A4_98

_E9_ECVP_A2(_90_18_EE|_1EET_F8_14~_A2s_C9_0C1_80(_1A_86_F0C_1C_B2_98_9E_97X_EE_F
9Bm_88_A00_DF_C2_FD_8A\B1_9D_B8)b_A16&_11_9DZ_01_95_BE' _89b<_B6_C0_E7_B1_A21Z_92_C9@'_F8#C_16_h_C8_C8<_A4%-IH_D4_82_8B_08\$ _87~_C3_82_Fbk
<_06_89V_B1x_89_8F_A9a_1F_11v)_D0_91_00V\^j_83D_15_89f_F2_89P_C6_97_120_D9Fh_07
_E2_86km_19_10_F4_92_C5_88G_CF-p1_A4y_ _F9_9C_A1l_8F_8Cn_12_8E0_E5_B0_A6_FE_E5K%_E76,P_ABi_A7_E3ym_04e_8A_91_D0_96>
_E9_B4S_01_FF_88_122_87DG>_EB_18L4\(_7F_AD_80_F9:f_BA_03_A6_16_8B_C8_92_BAOvJ|
_BA_98Z_AE_EB_07_B1#_D3P:_E8_9C_8B_15C_95t_17_E4Q_F39l_BC_B4v_EA_DE_D1%_BAx[_7F_
_A3RmC*W_94_AA\9F_A2O_CA_F5_A5_FC_A2_AE_9D_A8tQ_86_A8_18_BDM_D7_1C#_1F_D1_80_11T_E1_0BJ_E3_B6_CE_F8_03_F5M9_EC_9B_F6_F0_F75_15_DB_DC_BA_B4l@

_k'_0F_E4_C9Yr_BE_0C)l_98L-@_9A_1B_B2_B9t_1F_FE_A9%_DD_8Es_Edt_B2N/C4b_07;g6q\$S\$

_D4f'_B5_BDY_0B_A0j'_F3_E0~_07_7F_C3_F0_C2_BD_F1_05_BEsu_CE_83<_C3_9C_F8_9F_97_8
2_AF_E3'_04_8D_0F_03_FD:_C6J_8C_95-_D9_Eft_04_83_AE_D3_7F=_86_17#_E3H_B6_8C_D7
8s_15_DBK_ED1*\$\$_08_B0_10G_D0_F1_92'_E8%O9(C_AE_E7_89_D6_DC_C8_8A_7C_DE_08_92\$T_C0_B3Y_070_B5_A4%_BB(_CE_88_8B_90_135_82_90.TN_
AAX_B9X,rzD_04_86_16_01z)_D4_ED_A5&_D8e_B0_C2:_C3Q^_B17t_FE_99){_CE_9Fl_B9"_01_DF_8C_10_C13<
_96s_D2_F4_DA_E6_D7_E9_B4_DA_9A_96_FF_95_D7Z_05Z_C4_7F_FFFP_DF_02%K@_B2_B4_A5_E2

_82*yW_95L_F5_BC4lW_E6s'_C7_BE_EA_A0D_A9_10_BA_82F_9A_D1p.8W:_8D_95_C4_C4_B8_BF_

8CA_B7_96MB_94_11_F8_98s*_F5_D4_E9_EA_FA(_E9W_0C_C8'_13_04_F6y_C8_05&_FB_E6_E
6\A4_D9_83s_16_E9_ED_88_C4_EA@_86_B4K_CF_A3_15_7F_A4_A2B!_D8_96_8F_B4_04)}}_9D_99_1BP_9F_E3_FE_8Aj:_02t_85

_BD_EF_16E~_14_FBs*_A9_0B_B0l_C8_06v_C60_BC_BB_F5_BA_BD_F1_9C_0B_C4_B2_150F_8D_

F7_EF>|_18_DE_E5\$ _C1_96+5_EA_A0_EF_B8G_B3_00_1A_83_FE_DB^_B7X_9Es_A5xTY_7Fw_F3_B

6_EB_E5_EB_BA5j'_A4_8D/Y_E5x'k_06_FD_D7_B8_A27W_DE_CD_B8(_F8_92_BDlKFY2t_F5_D6_F8

r_DD_7F7_F0_BC_F2_82_D9_ACG6_B7u_94_88_C0_D8_10<_07_C4_AA_D9_B8_99_07~_F7_BA_8D_
A1_ED_CFQ_A8U#_95_D9P_C8_A4_18m_D3_ED_90_FA_9D)_C1_B0_B5_D3\ _E9_A2L_B0_C0_0B_DC
_BD_83_F4Tq_ABN_A1_EE_CB(C)_D3_BA_ _D4e_B0_E0_BD_A0p'_F1^_B7_C65(_84gb_AA_FB_B2A_06_F4_A6?_C7_97
_BE_0E_DA)_BDk_D6_B2_86_84_EC_9F_D3C_A4_BD_FD_E1+a_BE_81!_DCV_82_C4x_04_D2_E5_AE

{V_D3%P"_A9_Cdb_9B_E3_AB_D9_93_85_E7'_F1j_DF_FE_0Ch_DE_05_98_8E_B5_1C_F5pG_C8_C2

_B3O>_A4_BC_EC_DA1_ED_F1_E7_FF_9B_F6_F3_D7B_A2_FA_843_B3_EB_1D_ED_C6_FE_B0_EF_F5

_BF_B6_1B_BD_B7w'wc?_18t_BB_BA_BC=B_FF+_DD_98_E2_1Ev_A3Q_FC_F5_DDh'_B3n4P_A7v_A3

wR_13t_BF_D4_8D'_C3_FC_E7_08_FB_AF_98_EC-U*_EAQ_E3f_F8_BE_D7_EBf_C5W_AE_BB_FEpX_

DB_E9_1F_AF_DA_BE7_BC_F3_8E_BF_16_06=r_85mrJ!_D6F_DE_83_01_C2_F4_0C_D4p_DE_EF_0C
_9BPxX_AB_87_B1>Q_F0kd_D2xfgl7;_9FM_Dct_84<_9B_98S/_0B_F0_C0_9E_1EM_0FN_E9_11_C1_ED&_8F9C_0C_1E_F3Y5;_BCZ_A9j;+h_D6|_E4_B1
_BE_C9_A8U;6J_AFX_C0%R_CC_1F_9B_CD_A6<_7F_94_98_F4_A9>_C1
Vk_9D_E3&_AB_93_82_E7~_A9_04_8F_97_B3|_D4_DCM_7F_B6_19Y_CDlx_ABg_C3_BF_90(_19_17

#_AD_0E_8A_11_C4_07D-_D9_E2_92_C2b_17M>b_FEM_D9|t_BEb_E7_BA_98_EB1_BC6_CE_A0_EB_8A_1Ff(_9B_1Dw_DA)_B3V_D1o_92_AF_D1_8D_E9_DDS_C2_04_DEs_9D_91_EFq_963~h_06=r_AD_

A3_A9_.EB_B0L_F7_F1_81_E0_B9_F3P_D4_9A_FD_84_075_DC_C3p_B4V8_BF_908_9B_AD_C1_1Cw_DFh_DF8k_1D_18[_B8c_E6_1E_EB_7Fc(_9A_FE_CC_92b_A7_B0f_F7_C8_0F_E8_CD_82_8B_

DD_85lj_9D?_13w_1D_96_B3[_CA])_DF_C5_E3_EEA_F7_C6[_1CT;_A3_DA4_D9xw_BCgr_8ESZE_

D7_F9_DE_BCh_15_05_88_F3_B1X_B0_A7_B4m_F7_84J_D3Ky_BD_C4_A1_F3e_C7\ _D9_0B_BD_CD_

ED_D5&_F2_E1_CC_93)R>_C6_97_0B_B1m_83Z1i_AE[_00?_F1_1D/_D0_B0p_8Bs_02y\$__D4w:_0E_

_EE/_9Dj_ACM_F0_EAL_F0_D7hcdGri_81_D9_9E_A6V_C0d_12_92_AD96_ED_F7K_D5_A2_13_F4d_F7_

_A5k_8E_07_B43_A5_EE_81_BFj_ _D6_B1_B9_ABh_B6_9E_F7B_F1H_84_B9k_D2_B7@0_C59=_C6m_D8_B9o_A6\$'_1A_D7_88_

_E0_FE_E24_B3_EE_F8#_FB\$A_C4_E2_D6/_BAY^_B9_FB_82l_01_CD_1C_D4_89_88_F2WMA[_D8_

_B7+U_11m3_CC_B4MP_1F_8D)_1E_D0_1F_FF_F1q_87"(F_D5_A7_88_D3_B6_9CB_C2l_AE_AD_D6_BE_FE_CCc_EC_ED

_D8_81_DF_C8P_00_E7_9A_DA_FB_F6_D4_C1_BFjZ_8D]_EEq_BA_B6Z_8E_BE_08m^_BC_C7W_B5_B

E_FE_8B(vy_B1_C1_EA_CF_CB_0Bkvq_B9_07_7Fy_A1_FB_FB_CD_C5_11-{E_8EjX@_9B_4_

_19Qrs_C8_F8_024_94_D4d_E8|E_98_E5_C2_B6_ _B1_B59C[_8E_BE_CEj_D6-_01_ACE8_82_8B_

95R_89_1C_B9.v|ec_95T<2_9FJ_17_FB@_FD_A6W_9C_07_C9_E3_8Bv-V@_14_F9_84_C5_8F_80_9

A+9_C2f_D6_90_C7'a_A8_0F>G_D8_E4_DAG_CDr_04E_A7_08*_13_8E'_8F_83_8E_C9_7Ft_9Cr&_

A70_19_CE_A7_E6fa_81/_9D_A0>DY_A0_8E_D6_C9_0F1_EE:_DC_BC_B3hb_0E_E5_E7_93_B9_98)

_E2_80_A0L_AE_F4_BBM_DF_EBW_02_D6_93_80_98n_00_CFm_80_E784H_B6a_C9_F5+_B0(_B1<_E

0_17_97_87_F6^_B8_A6_DD_0CT_BA_81_A9=i_CD_0Cv_FA-W)uA_E2_18_102_FF3Xo_83_00_E8

_133_17_D5_19_A3_D56W_D4_E6_A0_8FQ_BF_CC_EB_A8_A6*_CB_818_B9_94_EB_A3w_B4_A4_F3_

9F_97Zz_1D_F5_E5_B0-_CE_F6_D7+_1Bsqa_BB#_95_F7_EA_D3^_B9_E5_F7_AA_A6_A7_B7Y)o_FE

_8C_87[_A8_9D_E9C_AE_F9_8F_A4_7F_01_FCG_B1\Y_1A_00_00

0


Connection Error Occurred During Web Application Scan

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 

QID: 150018

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 05/15/2009

THREAT:
Some of requests timed out or unexpected errors were detected in the connection while crawling or scanning the Web application.

IMPACT:
Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

SOLUTION:
Investigate the root cause of failure accessing the listed links.

RESULT:
Links that timed out:
<http://23.227.38.71/%27>
<http://23.227.38.71/>

http://23.227.38.71/.bak
http://23.227.38.71/.inc
http://23.227.38.71/.old
http://23.227.38.71/.orig
http://23.227.38.71/.tar.bz2
http://23.227.38.71/.tar.gz
http://23.227.38.71/.tar
http://23.227.38.71/.zip
http://23.227.38.71/.gz
http://23.227.38.71/CVS/Entries
http://23.227.38.71/INSTALL
http://23.227.38.71/common/
http://23.227.38.71/config/
http://23.227.38.71/css/
http://23.227.38.71/docs/
http://23.227.38.71/external/
http://23.227.38.71/history/
http://23.227.38.71/include/
http://23.227.38.71/includes/
http://23.227.38.71/js/
http://23.227.38.71/lib/
http://23.227.38.71/admin/
http://23.227.38.71/admin.aspx
http://23.227.38.71/admin.jsp
http://23.227.38.71/admin.php
http://23.227.38.71/administration/
http://23.227.38.71/bin/
http://23.227.38.71/BUGS
http://23.227.38.71/ChangeLog
http://23.227.38.71/ChangeLog.txt
http://23.227.38.71/CHANGELOG
http://23.227.38.71/CHANGELOG.txt
http://23.227.38.71/functions/
http://23.227.38.71/db/
http://23.227.38.71/adm/
http://23.227.38.71/image/
http://23.227.38.71/images/
http://23.227.38.71/install/
http://23.227.38.71/jsp/
http://23.227.38.71/backup/
http://23.227.38.71/cache/
http://23.227.38.71/classes/
http://23.227.38.71/core/
http://23.227.38.71/_core/
http://23.227.38.71/data/
http://23.227.38.71/documents/
http://23.227.38.71/errors/
http://23.227.38.71/export/
http://23.227.38.71/files/
http://23.227.38.71/download/


Web Applications and Plugins Detected

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 
QID: 45114
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/07/2015

THREAT:

The result section of this QID lists web applications and plugins that were detected on the target using web application fingerprinting. This technique compares static files at known locations against precomputed hashes for versions of those files in all available releases. The technique is fast, low-bandwidth, non-invasive, generic, and highly automatable.

Following open source and free applications are currently supported:

Joomla!
MediaWiki
WordPress
phpBB
MovableType
Drupal
osCommerce
PHP-Nuke
Moodle
Liferay
Tikiwiki
Twiki
phpmyadmin
SPIP
Confluence(free versions)
Wikka
Wacko
Usemod
e107
Flyspray
AppRain
V-CMS
AjaxPlorer/Pydio
eFront Learning Management System
vTigerCRM (Open source versions)
MyBB
WebCalendar
PivotX WebLog
DokuWiki
MODX Revolution
MODX Evolution
Collabtive
Achievo
Magento
iCE Hrm (Opensource Version)
AdaptCMS
ownCloud
HumHub
Redaxscript
phpwcms
Wolf CMS
Pligg CMS
Zen Cart
Xoops

Following Drupal plugins are supported:

Date
ImageField
Pathauto
Spamicide
CCK
FileField
ImageAPI
IMCE
Print
TagaDelic
Token
Views

Following WordPress plugins are supported:

Akismet
Buddypress
stats
WP-E-Commerce
WP-Super-Cache
Citizen Space Integration
WPTouch
Add to Any

WooCommerce
Simple Tags
Contact Form 7
Platinum SEO Pack
Lazy SEO
NextGEN Gallery
W3 Total Cache
AdRotate (Free)
Ad-Minister
Tweet-Blender
Social Sharing Toolkit
Sociable
Yet Another Related Posts Plugin
All In One SEO Pack
Media File Renamer
Search Everything!
CommentLuv!
BulletProof Security
Marekkis Watermark
Contus/WordPress Video Gallery
Search Everything
XCloner Backup and Restore
MailPoet/WYSIJA Newsletters
Pretty Link Lite
WP-Print
underConstruction
qTranslate
WP-PostViews
Twitget
Quick Page/Post Redirect Plugin
Stream Video Player
WordPress Content Slide
Lazyest Gallery
TinyMCE Color Picker
bib2html
WP e-Commerce Shop Styling
Calendar
Related Posts by Zemanta
Booking System (Booking Calendar)
Mail On Update
Contact Bank
Contextual Related Posts
Related Posts
Participants Database
Profile Builder
Digg Digg
WP-Property
WordPress Mobile Pack
Font Uploader
Blogstand Smart Banner
WP EasyCart
ENL Newsletter
Disqus Comment System
WP Google Maps
2 Click Social Media Buttons
EWWW Image Optimizer
WP-DBManager
CM Download Manager
Wordfence
Photo Gallery
Annonces
Another Wordpress Classifieds
Apptivo Business Site
WP-Slimstat
Fancybox for WordPress
Image Metadata Cruncher
Easing Slider
Google Document Embedder
WordPress SEO by Yoast
Shareaholic
AB Google Map Travel
Google Captcha
WP Media Cleaner
WPshop

The Cart Press
Reflex Gallery
N-Media Website Contact Form with File Upload
WP Photo Album Plus
WP Useronline
WP Survey and Poll
WP Symposium
Spider Event Calendar
Simple Ads Manager
Work the Flow File Upload
Landing Pages
NewStatPress

Following Joomla! plugins are supported:
2Glux Sexy Polling (com_sexypolling)
Joomla JCE Component (com_jce)

This QID is based on the Blind Elephant project.

RESULT:

iCEHRM	v3.0
MyBB	1.21.4


Web Applications and Plugins Detected

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 

QID: 45114

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 07/07/2015

THREAT:

The result section of this QID lists web applications and plugins that were detected on the target using web application fingerprinting. This technique compares static files at known locations against precomputed hashes for versions of those files in all available releases. The technique is fast, low-bandwidth, non-invasive, generic, and highly automatable.

Following open source and free applications are currently supported:

Joomla!
MediaWiki
WordPress
phpBB
MovableType
Drupal
osCommerce
PHP-Nuke
Moodle
Liferay
Tikiwiki
Twiki
phpmyadmin
SPIP
Confluence(free versions)

Wikka
Wacko
Usemod
e107
Flyspray
AppRain
V-CMS
AjaxPloer/Pydio
eFront Learning Management System
vTigerCRM (Open source versions)
MyBB
WebCalendar
PivotX WebLog
DokuWiki
MODX Revolution
MODX Evolution
Collabtive
Achievo
Magento
iCE Hrm (Opensource Version)
AdaptCMS
ownCloud
HumHub
Redaxscript
phpwcms
Wolf CMS
Pligg CMS
Zen Cart
Xoops

Following Drupal plugins are supported:

Date
ImageField
Pathauto
Spamicide
CCK
FileField
ImageAPI
IMCE
Print
TagaDelic
Token
Views

Following WordPress plugins are supported:

Akismet
Buddypress
stats
WP-E-Commerce
WP-Super-Cache
Citizen Space Integration
WPTouch
Add to Any
WooCommerce
Simple Tags
Contact Form 7
Platinum SEO Pack
Lazy SEO
NextGEN Gallery
W3 Total Cache
AdRotate (Free)
Ad-Minister
Tweet-Blender
Social Sharing Toolkit
Sociable
Yet Another Related Posts Plugin
All In One SEO Pack
Media File Renamer
Search Everything!
CommentLuv!
BulletProof Security
Marekkis Watermark

Contus/WordPress Video Gallery
Search Everything
XCloner Backup and Restore
MailPoet/WYSIJA Newsletters
Pretty Link Lite
WP-Print
underConstruction
qTranslate
WP-PostViews
Twitget
Quick Page/Post Redirect Plugin
Stream Video Player
WordPress Content Slide
Lazyest Gallery
TinyMCE Color Picker
bib2html
WP e-Commerce Shop Styling
Calendar
Related Posts by Zemanta
Booking System (Booking Calendar)
Mail On Update
Contact Bank
Contextual Related Posts
Related Posts
Participants Database
Profile Builder
Digg Digg
WP-Property
WordPress Mobile Pack
Font Uploader
Blogstand Smart Banner
WP EasyCart
ENL Newsletter
Disqus Comment System
WP Google Maps
2 Click Social Media Buttons
EWWW Image Optimizer
WP-DBManager
CM Download Manager
Wordfence
Photo Gallery
Annonces
Another Wordpress Classifieds
Apptivo Business Site
WP-Slimstat
Fancybox for WordPress
Image Metadata Cruncher
Easing Slider
Google Document Embedder
WordPress SEO by Yoast
Shareaholic
AB Google Map Travel
Google Captcha
WP Media Cleaner
WPshop
The Cart Press
Reflex Gallery
N-Media Website Contact Form with File Upload
WP Photo Album Plus
WP Useronline
WP Survey and Poll
WP Symposium
Spider Event Calendar
Simple Ads Manager
Work the Flow File Upload
Landing Pages
NewStatPress

Following Joomla! plugins are supported:
2Glux Sexy Polling (com_sexypolling)
Joomla JCE Component (com_jce)

This QID is based on the Blind Elephant project.

RESULT:


iCEHRM	v3.0
MyBB	1.21.4

ICMP Replies Received

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 
QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2003

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

RESULT:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply

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: 11/19/2004

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.

RESULT:


Average change between subsequent TCP initial sequence numbers is 989745650 with a standard deviation of 577955142. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4996 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

IP ID Values Randomness

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82046
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/27/2006

THREAT:

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.

RESULT:


IP ID changes observed (network order) for port 80: 0
Duration: 31 milli seconds

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: 06/15/2009

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	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 6
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/2000

THREAT:

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

RESULT:


IP address	Host name
23.227.38.71	23-227-38-71.shopify.com

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 45006

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 05/09/2003

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.

RESULT:

Hops	IP	Round Trip Time	Probe
1	64.39.105.3	0.35ms	ICMP
2	63.229.56.185	0.29ms	ICMP
3	67.14.41.18	0.56ms	ICMP
4	4.68.62.189	0.66ms	ICMP
5	4.69.149.18	74.71ms	ICMP
6	4.69.149.18	74.11ms	ICMP
7	4.53.116.90	74.02ms	ICMP
8	199.19.69.182	74.87ms	ICMP
9	23.227.38.71	75.08ms	ICMP


SSL Server default Diffie-Hellman prime information

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38609

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 05/26/2015

THREAT:

Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS.

- For fixed primes: 1024 and below are considered unsafe.

- For variable primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

RESULT:

SSL server default to use Diffie-Hellman key exchange method with variable 1024(bits) prime


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: 07/29/2005

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.

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	None			
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM

AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH


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: 01/16/2009

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:

Ineffective Session Protection. no tests enabled.
HSTS Analysis no tests enabled.
Collected 1 links overall.
Batch #0 Path manipulation: estimated time < 1 minute (115 tests, 1 inputs)
Path manipulation: 115 vulnsigs tests, completed 100 requests, 7 seconds. Completed 100 requests of 115 estimated requests (86.9565%). All tests completed.
WSEnumeration no tests enabled.
Arbitrary File Upload no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Static Session ID no tests enabled.
Batch #2 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)
Batch #2 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Batch #2 Cookie manipulation: estimated time < 1 minute (33 tests, 0 inputs)

Batch #2 Cookie manipulation: 33 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #2 Header manipulation: estimated time < 1 minute (33 tests, 1 inputs)
Batch #2 Header manipulation: 33 vulnsigs tests, completed 17 requests, 2 seconds. Completed 17 requests of 66 estimated requests (25.7576%).
XSS optimization removed 24 links. All tests completed.
Batch #2 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)
Batch #2 shell shock detector: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #2 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #2 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookies Without Consent no tests enabled.
Batch #3 HTTP Time Bandit: estimated time < 1 minute (0 tests, 10 inputs)
Batch #3 HTTP Time Bandit: 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Total requests made: 122
Average server response time: 0.16 seconds
Most recent lin
ks:
404 https://23.227.38.71/
404 https://23.227.38.71/
404 https://23.227.38.71/
404 https://23.227.38.71/
404 https://23.227.38.71/
404 https://23.227.38.71/
404 https://23.227.38.71/
404 https://23.227.38.71/
404 https://23.227.38.71/
404 https://23.227.38.71/
404 https://23.227.38.71/
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found


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: 06/17/2014

THREAT:

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

RESULT:

```
<!doctype html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en"> <!--<![endif]-->

<head>
<!-- Meta -->
<meta charset="UTF-8">
  <title>Create an Ecommerce Website and Sell Online! Ecommerce Software by Shopify</title>
  <meta name="description" content="Shopify provides a reliable Ecommerce platform so you focus on selling online! Integrated hosting, shopping
cart and Ecommerce payment solution all in one!" />

  <!-- Mobile viewport -->
  <meta name="viewport" content="width=1100, initial-scale=1" />

  <!-- Icons -->
  <link rel="shortcut icon" type="image/x-icon" href="//cdn.shopify.com/assets/favicon.png">
```

```

<!-- Begin CSS -->
<link rel="stylesheet" type="text/css" href="//cdn.shopify.com/assets/stylesheets/external-assets.css" media="screen, projection">

<!-- Begin jQuery -->
<script src="//ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js"></script>

<style>
<!--
/* Page Styles */
body { background: #F6F6F6; font-size: 62.5%; }
.signup .btn-green { padding: 10px 14px; }
#subpage #content-wrapper {
  width: 1020px;
  float: left;
  background: #fff;
  margin: 135px 0 10px -20px;
  padding: 35px 20px;
  -webkit-box-shadow: 0 0 20px rgba(0,0,0,0.1),0px 0px 0px rgba(0,0,0,0);
  -moz-box-shadow: 0 0 20px rgba(0,0,0,0.1),0px 0px 0px rgba(0,0,0,0);
  box-shadow: 0 0 20px rgba(0,0,0,0.1),0px 0px 0px rgba(0,0,0,0);
}
#pg-store404 { padding: 130px 0 140px 0; }
#pg-store404 h1 { font-size: 2rem; }

footer { background: none; text-align: center; font-size: 12px; padding: 50px 0; }
footer p { color: #999; margin: 0 !important; }
footer p a, footer p a:hover, footer p a:active { color: #777; text-decoration: underline; }
.btn-green{color:#fff !important;background-color:#8EC023;border-top:#DBFF8E;border-right:1px solid #65A32E;border-bottom:1px solid #6B9A20;border-left:1px solid #65A32E;text-shadow:0 -1px 1px #4e9409;-webkit-background-clip:padding-box;background-color:#75B600;background-image:-o-linear-gradient(#9bdc27,#75b600);background-image:-webkit-gradient(linear, left bottom, left top, color-stop(0, #75b600), color-stop(1, #9bdc27));background-image:-moz-linear-gradient(center bottom, #75b600 0%, #9bdc27 100%);-webkit-box-shadow:0 1px 0 0 #a6e95b inset,0 1px 2px 0 rgba(0, 0, 0, 0.3);-moz-box-shadow:0 1px 0 0 #a6e95b inset,0 1px 2px 0 rgba(0, 0, 0, 0.3);box-shadow:0 1px 0 0 #a6e95b inset,0 1px 2px 0 rgba(0, 0, 0, 0.3);-o-transition:none 0.3s ease-in-out 0s;-webkit-transition:none 0.3s ease-in-out 0s;-moz-transition:none 0.3s ease-in-out 0s;-webkit-border-radius:3px;-moz-border-radius:3px;border-radius:3px;}.btn-green:active{background-color:#98D332;border:1px solid #588C15;border-bottom:1px solid #508E0E;text-shadow:0 -1px 1px #63a423;-webkit-background-clip:padding-box;-webkit-box-shadow:0 0 6px 3px #68b516 inset,0 1px 0 0 #000;-moz-box-shadow:0 0 6px 3px #68b516 inset,0 1px 0 0 #000;box-shadow:0 0 6px 3px #68b516 inset,0 1px 0 0 #000;}
-->
</style>

</head>

<body id="subpage">

<!-- Begin main-nav -->
-->
<div class="wrapper" id="shopify-nav">
  <div class="row">
    <div class="col3">

      <span id="branding"><strong>Shopify Ecommerce - Shopping Cart & Software</strong></span>
      (//www.shopify.com)
    </div>
    <div class="col9">
      <nav>
        <ul class="sub-menu">
          Want to setup an online store?
          (//www.shopify.com/?utm_source=ExpiredDomainLink&utm_medium=textlink&utm_campaign=ExpiredDomainLink)
          <li class="signup"><span class="btn-green">Sign up for Shopify</span>
          (//www.shopify.com/?utm_source=ExpiredDomainLink&utm_medium=textlink&utm_campaign=ExpiredDomainLink)
        </ul>
      </div>
    </div>
  </div>
<!-- End main-nav -->

<!-- Begin content -->

```

```

<div class="wrapper content">
<div class="row">
  <div id="content-wrapper" class="clearfix">

    <div id="pg-store404">

      <div id="shop-not-found">
        <h1 class="tc">Sorry, this shop is currently unavailable.
      </div>

      <div id="custom-msg" style="display:none">
        <h1 class="tc">
      </div>

      <script type="text/javascript">
        $(function(){
          var hostname = window.location.hostname;
          var re = /\.(shopify|shopifyadmin)\.com$/;
          if (hostname.match(re)) {
            var myshopifyDomain = encodeURI(hostname.replace(re, ".myshopify.com"));
            var href = encodeURI(window.location.href.replace(hostname, myshopifyDomain));
            $("#custom-msg h1").html('Did you mean '+myshopifyDomain+' ()?');
            $("#shop-not-found").hide();
            $("#custom-msg").show();
          } else if (!hostname.match(/\.(myshopify)\.com$/)) {
            $.ajax({
              url: 'https://app.shopify.com/services/last_shop.json',
              dataType: 'jsonp',
              jsonp: 'callback',
              success: function(response){

                if (response.last_shop != undefined) {
                  $("#custom-msg h1").html("Only one step left! To finish setting up your new web address, go to your domain settings (https://), click
"Add existing domain", and enter: '+hostname);
                  $("#shop-not-found").hide();
                  $("#custom-msg").show();
                }
              }
            });
          }
        });
      </script>

    </div>

  </div>
</div>
</div>
<!-- End content -->

<footer>
</footer>

</body>
</html>
-CR-

```


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: 01/01/1999

RESULT:

Server Version	Server Banner
nginx	nginx


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: 04/14/2015

THREAT:

The list of unique links crawled and HTML forms submitted by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 23.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

http://23.227.38.71/


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: 10/19/2007

THREAT:

The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:

Number of links: 6
http://cdn.shopify.com/assets/favicon.png
http://cdn.shopify.com/assets/stylesheets/external-assets.css
https://+response.last_shop+/admin/settings/domains
http://www.shopify.com/
http://www.shopify.com/?utm_source=ExpiredDomainLink&utm_medium=textlink&utm_campaign=ExpiredDomainLink
https://app.shopify.com/services/last_shop.json


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: 01/16/2009

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:

Ineffective Session Protection. no tests enabled.
HSTS Analysis no tests enabled.
Collected 1 links overall.
Batch #0 Path manipulation: estimated time < 1 minute (115 tests, 1 inputs)
Path manipulation: 115 vulnsigs tests, completed 100 requests, 1563 seconds. Completed 100 requests of 115 estimated requests (86.9565%). All tests completed.
WSEnumeration no tests enabled.
Arbitrary File Upload no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Static Session ID no tests enabled.
Batch #2 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)
Batch #2 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Batch #2 Cookie manipulation: estimated time < 1 minute (33 tests, 0 inputs)
Batch #2 Cookie manipulation: 33 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #2 Header manipulation: estimated time < 1 minute (33 tests, 1 inputs)
Batch #2 Header manipulation: 33 vulnsigs tests, completed 17 requests, 1 seconds. Completed 17 requests of 66 estimated requests (25.7576%).
XSS optimization removed 24 links. All tests completed.
Batch #2 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)
Batch #2 shell shock detector: 1 vulnsigs tests, completed 1 requests, 1 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #2 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #2 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookies Without Consent no tests enabled.
Batch #3 HTTP Time Bandit: estimated time < 1 minute (0 tests, 10 inputs)
Batch #3 HTTP Time Bandit: 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Total requests made: 122
Average server response time: 0.13 seconds

Most recent
links:
404 http://23.227.38.71/
404 http://23.227.38.71/
404 http://23.227.38.71/
404 http://23.227.38.71/
404 http://23.227.38.71/
404 http://23.227.38.71/
404 http://23.227.38.71/
404 http://23.227.38.71/
404 http://23.227.38.71/
404 http://23.227.38.71/
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found


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: 06/17/2014

THREAT:

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

RESULT:

```
<!doctype html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en"> <!--<![endif]-->

<head>
<!-- Meta -->
<meta charset="UTF-8">
  <title>Create an Ecommerce Website and Sell Online! Ecommerce Software by Shopify</title>
  <meta name="description" content="Shopify provides a reliable Ecommerce platform so you focus on selling online! Integrated hosting, shopping
  cart and Ecommerce payment solution all in one!" />

  <!-- Mobile viewport -->
  <meta name="viewport" content="width=1100, initial-scale=1" />

  <!-- Icons -->
  <link rel="shortcut icon" type="image/x-icon" href="//cdn.shopify.com/assets/favicon.png">

  <!-- Begin CSS -->
  <link rel="stylesheet" type="text/css" href="//cdn.shopify.com/assets/stylesheets/external-assets.css" media="screen, projection">

  <!-- Begin jQuery -->
  <script src="//ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js"></script>

  <style>
  <!--
  /* Page Styles */
  body { background: #F6F6F6; font-size: 62.5%; }
  .signup .btn-green { padding: 10px 14px; }
  #subpage #content-wrapper {
    width: 1020px;
```

```

float: left;
background: #fff;
margin: 135px 0 10px -20px;
padding: 35px 20px;
-webkit-box-shadow: 0 0 20px rgba(0,0,0,0.1),0px 0px 0px rgba(0,0,0,0);
-moz-box-shadow: 0 0 20px rgba(0,0,0,0.1),0px 0px 0px rgba(0,0,0,0);
box-shadow: 0 0 20px rgba(0,0,0,0.1),0px 0px 0px rgba(0,0,0,0);
}
#pg-store404 { padding: 130px 0 140px 0; }
#pg-store404 h1 { font-size: 2rem; }

footer { background: none; text-align: center; font-size: 12px; padding: 50px 0; }
footer p { color: #999; margin: 0 !important; }
footer p a, footer p a:hover, footer p a:active { color: #777; text-decoration: underline; }
.btn-green{color:#fff !important;background
ound-color:#8EC023;border-top:#DBFF8E;border-right:1px solid #65A32E;border-bottom:1px solid #6B9A20;border-left:1px solid
#65A32E;text-shadow:0 -1px 1px
#4e9409;-webkit-background-clip:padding-box;background-color:#75B600;background-image:-o-linear-gradient(#9bdc27,
#75b600);background-image:-webkit-gradient(linear, left bottom, left top, color-stop(0, #75b600), color-stop(1,
#9bdc27));background-image:-moz-linear-gradient(center bottom, #75b600 0%, #9bdc27 100%);-webkit-box-shadow:0 1px 0 0 #a6e95b inset,0 1px
2px 0 rgba(0, 0, 0, 0.3);-moz-box-shadow:0 1px 0 0 #a6e95b inset,0 1px 2px 0 rgba(0, 0, 0, 0.3);box-shadow:0 1px 0 0 #a6e95b inset,0 1px 2px 0
rgba(0, 0, 0, 0.3);-o-transition:none 0.3s ease-in-out 0s;-webkit-transition:none 0.3s ease-in-out 0s;-moz-transition:none 0.3s ease-in-out
0s;-webkit-border-radius:3px;-moz-border-radius:3px;border-radius:3px;}.btn-gree
n:hover{background-color:#8EC023;border-top:#DBFF8E;border-right:1px solid #65A32E;border-bottom:1px solid #6B9A20;border-left:1px solid
#65A32E;cursor:pointer;text-shadow:0 -1px 1px
#458505;-webkit-background-clip:padding-box;background-color:#70AE00;background-image:-o-linear-gradient(#95d622,
#70ae00);background-image:-webkit-gradient(linear, left bottom, left top, color-stop(0, #70ae00), color-stop(1,
#95d622));background-image:-moz-linear-gradient(center bottom, #70ae00 0%, #95d622 100%);-webkit-box-shadow:0 1px 0 0 #a6e05b inset,0 1px
2px 0 rgba(0, 0, 0, 0.2);-moz-box-shadow:0 1px 0 0 #a6e05b inset,0 1px 2px 0 rgba(0, 0, 0, 0.2);box-shadow:0 1px 0 0 #a6e05b inset,0 1px 2px 0
rgba(0, 0, 0, 0.2);}
.btn-green:active{background:#98D332;border:1px solid #588C15;border-bottom:1px solid #508E0E;text-shadow:0 -1px 1px
#63a423;-webkit-background-clip:padding-box;-webkit-box-shadow:0 0 6px 3px #68b516 inset,0 1px 0 0 #000;-moz-box-shadow:0 0 6px 3px
#68b516 inset,0 1px 0 0 #000;box-shadow:0 0 6px 3px #68b516 inset,0 1px 0 0 #000;}
-->
</style>

</head>

<body id="subpage">

<!-- Begin main-nav
-->
<div class="wrapper" id="shopify-nav">
<div class="row">
<div class="col3">

<span id="branding"><strong>Shopify Ecommerce - Shopping Cart & Software</strong></span>
(//www.shopify.com)
</div>
<div class="col9">
<nav>
<ul class="sub-menu">
Want to setup an online store?
(//www.shopify.com/?utm_source=ExpiredDomainLink&utm_medium=textlink&utm_campaign=ExpiredDomainLink)
<li class="signup"><span class="btn-green">Sign up for Shopify</span>
(//www.shopify.com/?utm_source=ExpiredDomainLink&utm_medium=textlink&utm_campaign=ExpiredDomainLink)

</nav>
</div>
</div>
</div>
<!-- End main-nav -->

<!-- Begin content -->
<div class="wrapper content">
<div class="row">
<div id="content-wrapper" class="clearfix">

<div id="pg-store404">

<div id="shop-not-found">
<h1 class="tc">Sorry, this shop is currently unavailable.
</div>

<div id="custom-msg" style="display:none">
<h1 class="tc">
</div>

```

```

<script type="text/javascript">
$(function(){
  var hostname = window.location.hostname;
  var re = /\.shopify\.shopifyadmin\..com$/;
  if (hostname.match(re)) {
    var myshopifyDomain = encodeURIComponent(hostname.replace(re, ".myshopify.com"));
    var href = encodeURIComponent(window.location.href.replace(hostname, myshopifyDomain));
    $("#custom-msg h1").html('Did you mean '+myshopifyDomain+'()?');
    $("#shop-not-found").hide();
    $("#custom-msg").show();
  } else if (!hostname.match(/\..myshopify\..com$/)) {
    $.ajax({
      url: 'https://app.shopify.com/services/last_shop.json',
      dataType: 'jsonp',
      jsonp: 'callback',
      success: function(response){

        if (response.last_shop != undefined) {
          $("#custom-msg h1").html("Only one step left! To finish setting up your new web address, go to your domain settings (https://), click
"Add existing domain", and enter: '+hostname);
          $("#shop-not-found").hide();
          $("#custom-msg").show();
        }
      }
    });
  }
});
});
</script>

</div>

</div>
</div>
</div>
<!-- End content -->

<footer>
</footer>

</body>
</html>
-CR-

```


SSL/TLS Server supports TLS_FALLBACK_SCSV

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38610

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 06/08/2015

THREAT:

TLS cipher suite TLS_FALLBACK_SCSV is a signaling cipher suite value (SCSV).

TLS servers support TLS_FALLBACK_SCSV will prevent downgrade attack.


RESULT:

TLS_FALLBACK_SCSV is supported on port 443.

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 38291
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/16/2004

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.

RESULT:

TLSv1 session caching is enabled on the target. TLSv1.1 session caching is enabled on the target. TLSv1.2 session caching is enabled on the target.


SSL Web Server Version

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 86001
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/2000

RESULT:

Server Version	Server Banner
nginx	nginx

Links Crawled

port 443/tcp

PCI COMPLIANCE STATUS


PASS

VULNERABILITY DETAILS

Severity: 1 

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150010
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/19/2007

THREAT:

The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:

Number of links: 6
<https://cdn.shopify.com/assets/favicon.png>
<https://cdn.shopify.com/assets/stylesheets/external-assets.css>
https://+response.last_shop+/admin/settings/domains
<https://www.shopify.com/>
https://www.shopify.com/?utm_source=ExpiredDomainLink&utm_medium=textlink&utm_campaign=ExpiredDomainLink
https://app.shopify.com/services/last_shop.json


TLS Secure Renegotiation Extension Supported

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: 12/01/2011

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.

RESULT:

TLS Secure Renegotiation Extension Status: supported.


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: 01/24/2003

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	06:bd:80:5b:03:ba:66:48:af:f1:0f:b3:f1:79:da:40
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
organizationName	DigiCert Inc
organizationalUnitName	www.digicert.com
commonName	DigiCert SHA2 High Assurance Server CA
(0)SUBJECT NAME	
countryName	CA
stateOrProvinceName	Ontario

localityName	Ottawa
organizationName	Shopify Inc.
commonName	*.myshopify.com
(0)Valid From	Jul 29 00:00:00 2014 GMT
(0)Valid Till	Oct 4 12:00:00 2017 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:ae:55:67:67:42:e5:52:5a:fc:17:af:db:23:2d:
(0)	11:91:ad:34:81:45:08:0e:64:da:a5:23:9b:42:3f:
(0)	ff:5d:b3:6b:0a:7c:d0:7a:47:66:84:61:d1:06:15:
(0)	9e:01:07:9d:26:c9:cc:e7:ec:9c:2b:9a:06:27:f1:
(0)	42:eb:ed:14:5e:5e:5b:fd:a8:16:d2:4a:80:4c:a0:
(0)	b0:2d:c7:1e:84:fd:31:1b:b9:fe:11:59:3a:b9:a1:
(0)	3f:14:eb:fd:a3:84:4b:2f:1d:4b:0f:ca:fe:87:00:
(0)	df:47:17:a5:1b:e8:30:92:fc:d2:4f:1e:82:44:bc:
(0)	60:3c:2b:ad:d8:7d:23:09:c8:18:22:94:ab:cc:2e:
(0)	13:e5:af:63:1c:4b:ad:8b:2f:3e:74:76:49:0e:2a:
(0)	da:e3:78:d1:79:5d:7a:8f:a9:45:e8:3e:91:97:71:
(0)	ee:1d:8d:b4:80:5b:66:ae:2f:c9:4d:4f:50:a4:f9:
(0)	60:15:3b:4c:e6:f9:37:ea:56:6a:4a:cf:2d:59:90:
(0)	91:e6:1c:dd:85:f4:b9:99:07:5b:dc:5a:5d:f3:09:
(0)	ca:12:35:17:97:4c:e2:cd:37:2d:7b:8e:48:64:05:
(0)	2d:64:cd:71:c0:5f:a5:bd:5e:d4:24:5f:b9:0d:fe:
(0)	f0:1b:b3:03:80:56:ab:3b:73:6d:2a:fc:5b:82:b6:
(0)	eb:35
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:51:68:FF:90:AF:02:07:75:3C:CC:D9:65:64:62:A2:12:B8:59:72:3B
(0)X509v3 Subject Key Identifier	9F:A3:09:8A:D1:28:F5:2B:7A:9D:9C:6D:3C:DD:B8:C0:E7:5B:9F:79
(0)X509v3 Subject Alternative Name	DNS:*.myshopify.com, DNS:myshopify.com, DNS:*.shopifyadmin.com, DNS:shopifyadmin.com
(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 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl3.digicert.com/sha2-ha-server-g2.crl
(0)	
(0)	Full Name:
(0)	URI:http://crl4.digicert.com/sha2-ha-server-g2.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114412.1.1
(0)	CPS: https://www.digicert.com/CPS
(0)Authority Information Access	OCSP - URI:http://ocsp.digicert.com
(0)	CA Issuers - URI:http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)Signature	(256 octets)
(0)	ae:53:65:64:55:6e:c4:28:7c:19:d5:ae:18:71:ab:52
(0)	ef:89:2b:21:7d:0c:84:c5:b0:34:e8:49:86:8d:1a:a9
(0)	d4:42:37:aa:02:e0:9d:9a:61:87:44:9c:8b:b9:48:cd
(0)	ac:e3:a9:75:57:9d:3a:e1:e4:64:82:5f:cd:03:e5:c1
(0)	6e:a8:9a:ea:d2:de:31:cd:5d:82:1c:ee:69:c8:08:1b
(0)	61:a6:df:af:b4:76:d7:1b:ab:10:f5:68:b2:79:16:38
(0)	c2:c0:3f:7d:f4:1f:4b:39:84:03:c0:c1:a3:f9:f2:85

(0)	fb:a8:60:85:4d:f4:2a:f9:ea:ea:f0:d0:50:d5:58:a2
(0)	2c:63:73:14:fd:b2:ef:4e:db:45:4d:db:af:14:ab:3e
(0)	f8:b0:1f:f1:3a:6d:69:3d:06:08:23:50:92:43:c8:b9
(0)	72:c9:0a:48:24:a7:9d:c3:60:34:7e:b8:50:e5:a1:aa
(0)	af:b8:83:cd:25:43:89:98:40:e6:76:75:f4:b8:61:0a
(0)	6f:4a:e5:39:1d:f4:f4:a4:7d:24:13:7d:f7:79:21:ec
(0)	e7:83:20:fc:bc:ce:a6:48:40:db:df:7b:ee:20:09:59
(0)	d7:5a:7a:f1:8e:d7:c0:84:7f:c2:e9:c0:14:37:d9:e4
(0)	04:e9:00:bb:f4:f3:da:ed:8b:9f:d6:4b:f1:98:00:67
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	04:e1:e7:a4:dc:5c:f2:f3:6d:c0:2b:42:b8:5d:15:9f
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
organizationName	DigiCert Inc
organizationalUnitName	www.digicert.com
commonName	DigiCert High Assurance EV Root CA
(1)SUBJECT NAME	
countryName	US
organizationName	DigiCert Inc
organizationalUnitName	www.digicert.com
commonName	DigiCert SHA2 High Assurance Server CA
(1)Valid From	Oct 22 12:00:00 2013 GMT
(1)Valid Till	Oct 22 12:00:00 2028 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b6:e0:2f:c2:24:06:c8:6d:04:5f:d7:ef:0a:64:
(1)	06:b2:7d:22:26:65:16:ae:42:40:9b:ce:dc:9f:9f:
(1)	76:07:3e:c3:30:55:87:19:b9:4f:94:0e:5a:94:1f:
(1)	55:56:b4:c2:02:2a:af:d0:98:ee:0b:40:d7:c4:d0:
(1)	3b:72:c8:14:9e:ef:90:b1:11:a9:ae:d2:c8:b8:43:
(1)	3a:d9:0b:0b:d5:d5:95:f5:40:af:c8:1d:ed:4d:9c:
(1)	5f:57:b7:86:50:68:99:f5:8a:da:d2:c7:05:1f:a8:
(1)	97:c9:dc:a4:b1:82:84:2d:c6:ad:a5:9c:c7:19:82:
(1)	a6:85:0f:5e:44:58:2a:37:8f:fd:35:f1:0b:08:27:
(1)	32:5a:f5:bb:8b:9e:a4:bd:51:d0:27:e2:dd:3b:42:
(1)	33:a3:05:28:c4:bb:28:cc:9a:ac:2b:23:0d:78:c6:
(1)	7b:e6:5e:71:b7:4a:3e:08:fb:81:b7:16:16:a1:9d:
(1)	23:12:4d:e5:d7:92:08:ac:75:a4:9c:ba:cd:17:b2:
(1)	1e:44:35:65:7f:53:25:39:d1:1c:0a:9a:63:1b:19:
(1)	92:74:68:0a:37:c2:c2:52:48:cb:39:5a:a2:b6:e1:
(1)	5d:c1:dd:a0:20:b8:21:a2:93:26:6f:14:4a:21:41:
(1)	c7:ed:6d:9b:f2:48:2f:f3:03:f5:a2:68:92:53:2f:
(1)	5e:e3
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)Authority Information Access	OCSP - URI:http://ocsp.digicert.com

(1)X509v3 CRL Distribution Points


(1)	Full Name:
(1)	URI:http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://www.digicert.com/CPS
(1)X509v3 Subject Key Identifier	51:68:FF:90:AF:02:07:75:3C:CC:D9:65:64:62:A2:12:B8:59:72:3B
(1)X509v3 Authority Key Identifier	keyid:B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3
(1)Signature	(256 octets)
(1)	18:8a:95:89:03:e6:6d:df:5c:fc:1d:68:ea:4a:8f:83
(1)	d6:51:2f:8d:6b:44:16:9e:ac:63:f5:d2:6e:6c:84:99
(1)	8b:aa:81:71:84:5b:ed:34:4e:b0:b7:79:92:29:cc:2d
(1)	80:6a:f0:8e:20:e1:79:a4:fe:03:47:13:ea:f5:86:ca
(1)	59:71:7d:f4:04:96:6b:d3:59:58:3d:fe:d3:31:25:5c
(1)	18:38:84:a3:e6:9f:82:fd:8c:5b:98:31:4e:cd:78:9e
(1)	1a:fd:85:cb:49:aa:f2:27:8b:99:72:fc:3e:aa:d5:41
(1)	0b:da:d5:36:a1:bf:1c:6e:47:49:7f:5e:d9:48:7c:03
(1)	d9:fd:8b:49:a0:98:26:42:40:eb:d6:92:11:a4:64:0a
(1)	57:54:c4:f5:1d:d6:02:5e:6b:ac:ee:c4:80:9a:12:72
(1)	fa:56:93:d7:ff:bf:30:85:06:30:bf:0b:7f:4e:ff:57
(1)	05:9d:24:ed:85:c3:2b:fb:a6:75:a8:ac:2d:16:ef:7d
(1)	79:27:b2:eb:c2:9d:0b:07:ea:aa:85:d3:01:a3:20:28
(1)	41:59:43:28:d2:81:e3:aa:f6:ec:7b:3b:77:b6:40:62
(1)	80:05:41:45:01:ef:17:06:3e:de:c0:33:9b:67:d3:61
(1)	2e:72:87:e4:69:fc:12:00:57:40:1e:70:f5:1e:c9:b4

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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.

RESULT:


The network handle is: SHOPIFY-NET
Network description:
Shopify, Inc.

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45005
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/27/2013

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.

RESULT:


The ISP network handle is: NSI001001
ISP Network description:
Datatility, Inc.

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/14/2005

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.

RESULT:


Host Name	Source
23-227-38-71.shopify.com	FQDN

Host Scan Time

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/19/2004

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.

RESULT:

Scan duration: 12493 seconds

Start time: Wed, Jul 08 2015, 06:06:23 GMT


End time: Wed, Jul 08 2015, 09:34:36 GMT

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

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).

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 is probed.

Appendices

Hosts Scanned

23.227.38.71

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
Overall Performance:	Custom
Hosts to Scan in Parallel-External Scanner:	10
Hosts to Scan in Parallel-Scanner Appliances:	10
Processes to Run in Parallel-Total:	10
Processes to Run in Parallel-HTTP:	1
Packet (Burst) Delay:	Maximum

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

The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.






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 PASSED indicates that all hosts in the report passed 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. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

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	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.
 MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
 HIGH	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
<div><div></div><div></div><div></div><div></div><div></div></div> 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.
<div><div></div><div></div><div></div><div></div><div></div></div> 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.
<div><div></div><div></div><div></div><div></div><div></div></div> 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.
<div><div></div><div></div><div></div><div></div><div></div></div> 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.
<div><div></div><div></div><div></div><div></div><div></div></div> 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	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.
 MED	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	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.