HackerGuardian
A SECTIGO COMPANY

Powered by Qualys.

Payment Card Industry (PCI) Technical Report

05/20/2020

ASV Scan Report Attestation of Scan Compliance

A1. Scan Customer Information				A2. Approved Scanning Vendor Information			
Company:	Gimmonix Technologies LTD			Company:	Sectigo Limited		
Contact Name:	Hanan Milman	Job Title:		Contact Name:	HackerGuardian Support	Job Title:	Manager
Telephone:		Email:	hanan@gimmonix.com	Telephone:	+44 (0) 161 874 7070	Email:	hg.support@sectigo.com
Business Address:	Soncino 3,			Business Address:	3rd Floor Building 26, Office Village Exchange Quay, Trafford Road		
City:	tel aviv	State/Province:		City:	Salford	State/Province:	None
ZIP/postal code:		Country:	Israel	ZIP/postal code:	M5 3EQ	Country:	United Kingdom
URL:				URL:	https://sectigo.com/		

A3. Scan Status			
Date scan completed	05/20/2020	Scan expiration date (90 days from date scan completed)	08/18/2020
Compliance Status	PASS	Scan report type	Full scan
Number of unique in-scope components scanned			1
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			24

A.4 Scan Customer Attestation

Gimmonix Technologies LTD attests on 05/20/2020 at 10:29:24 GMT that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions - including compensating controls if applicable- is accurate and complete.
Gimmonix Technologies LTD also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by Sectigo Limited under certificate number 4172-01-14, according to internal processes that meet PCI DSS requirement 11.2.2 and the ASV Program Guide.
Sectigo Limited attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by HackerGuardian Support

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company:	Gimmonix Technologies LTD	ASV Company:	Sectigo Limited
Date scan was completed:	05/20/2020	Scan expiration date:	08/18/2020

Part 2. Component Compliance Summary

51.145.178.10	PASS

Part 2. Component Compliance Summary - (Hosts Not Current)

Part 3a. Vulnerabilities Noted for each Component

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
-	-	-	-	-	-

Part 3b. Special Notes by Component

Component	Special Note	Item Noted (remote access software, POS software, etc.)	Scan customer's description of actions taken and declaration that software is either implemented securely or removed
-	-	-	-

Part 3c. Special Notes Full Text

Note

-

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Addresses/ranges/subnets, domains, URLs, etc.

IP Addresses/Ranges : 51.145.178.10
Domains :

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.

IP Addresses/Ranges : - (not active) Scan customer attests that this IP address is not issued/assigned to any physical or virtual host. ASV confirmed it is nonresponsive.

Report Summary	
Company:	Gimmonix Technologies LTD
Hosts in Account:	1 IPs, 0 DNS
Hosts Active:	1
Hosts Scanned:	1
Scan Date:	05/20/2020 at 09:34:26 GMT
Report Date:	05/20/2020 at 10:29:28 GMT
Report Title:	SaaS PCI Report
Template Title:	Payment Card Industry (PCI) Technical Report

Summary of Vulnerabilities

Vulnerabilities Total	39	Average Security Risk	0.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	0	0
2	0	0	6	6
1	0	0	33	33
Total	0	0	39	39

by PCI Severity

PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	0	0	0
Low	0	0	0
Total	0	0	0

Vulnerabilities by PCI Severity

Potential Vulnerabilities by PCI Severity

Vulnerabilities by Severity

Potential Vulnerabilities by Severity

51.145.178.10 Windows Vista / Windows 2008

Vulnerabilities Total	39	Security Risk	0.0

Information Gathered (39)

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **1**
QID: 6
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/04/2018

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
51.145.178.10	No registered hostname

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
Microsoft-HTTPAPI/2.0	Microsoft-HTTPAPI/2.0

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:	03/29/2019

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.

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) and
- Certain requests from QID 150172 (Requests Crawled)

RESULT:

Duration of crawl phase (seconds): 12.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

https://51.145.178.10/

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.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found. Aborting the CMS Detection phaseCMSDetection: 1 vulnsigs tests, completed 38 requests, 10 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.
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.
WebCgiOobTests: no test enabled
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK 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 (45 tests, 0 inputs)
Batch #4 Cookie manipulation: 45 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (45 tests, 1 inputs)
Batch #4 Header manipulation: 45 vulnsigs tests, completed 59 requests, 3 seconds. Completed 59 requests of 124 estimated requests (47.5806%). XSS optimization removed 28 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.
cve_2017_9805 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, 1 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:(3 x 0) + files:(10 x 0) + directories:(87 x 1) + paths:(9 x 1) = total (96)
Batch #5 Path manipulation: estimated time < 1 minute (109 tests, 1 inputs)
Batch #5 Path manipulation: 109 vulnsigs tests, completed 95 requests, 4 seconds. Completed 95 requests of 96 estimated requests (98.9583%). All tests completed.
WebCgiGenericTests: no test enabled
Total requests made: 220
Average server response time: 0.30 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

SSL Web Server Version

pci.travolutionary.com: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
Microsoft-HTTPAPI/2.0	Microsoft-HTTPAPI/2.0

Links Crawled

pci.travolutionary.com:443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	03/29/2019

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.

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) and
- Certain requests from QID 150172 (Requests Crawled)

RESULT:

Duration of crawl phase (seconds): 12.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

https://pci.travolutionary.com/

Scan Diagnostics

pci.travolutionary.com: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.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found. Aborting the CMS Detection phaseCMSDetection: 1 vulnsigs tests, completed 38 requests, 11 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.
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.
WebCgiOobTests: no test enabled
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK 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 (45 tests, 0 inputs)
Batch #4 Cookie manipulation: 45 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (45 tests, 1 inputs)
Batch #4 Header manipulation: 45 vulnsigs tests, completed 59 requests, 3 seconds. Completed 59 requests of 124 estimated requests (47.5806%). XSS optimization removed 28 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, 1 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.
cve_2017_9805 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:(3 x 0) + files:(10 x 0) + directories:(87 x 1) + paths:(9 x 1) = total (96)
Batch #5 Path manipulation: estimated time < 1 minute (109 tests, 1 inputs)
Batch #5 Path manipulation: 109 vulnsigs tests, completed 95 requests, 4 seconds. Completed 95 requests of 96 estimated requests (98.9583%). All tests completed.
WebCgiGenericTests: no test enabled
Total requests made: 220
Average server response time: 0.30 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Web Server Version

pci.travolutionary.com:80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/26/2016

RESULT:

Server Version	Server Banner
Microsoft-HTTPAPI/2.0	Microsoft-HTTPAPI/2.0

Links Crawled

pci.travolutionary.com:80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150009
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/29/2019

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.

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) and
- Certain requests from QID 150172 (Requests Crawled)

RESULT:

Duration of crawl phase (seconds): 8.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

http://pci.travolutionary.com/

Scan Diagnostics

pci.travolutionary.com: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.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found. Aborting the CMS Detection phaseCMSDetection: 1 vulnsigs tests, completed 38 requests, 7 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.
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.
WebCgiOobTests: no test enabled
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK 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 (45 tests, 0 inputs)
Batch #4 Cookie manipulation: 45 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (45 tests, 1 inputs)
Batch #4 Header manipulation: 45 vulnsigs tests, completed 59 requests, 2 seconds. Completed 59 requests of 124 estimated requests (47.5806%). XSS optimization removed 28 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.
cve_2017_9805 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:(3 x 0) + files:(10 x 0) + directories:(87 x 1) + paths:(9 x 1) = total (96)
Batch #5 Path manipulation: estimated time < 1 minute (109 tests, 1 inputs)
Batch #5 Path manipulation: 109 vulnsigs tests, completed 95 requests, 2 seconds. Completed 95 requests of 96 estimated requests (98.9583%). All tests completed.
WebCgiGenericTests: no test enabled
Total requests made: 220
Average server response time: 0.18 seconds
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:	03/16/2019

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

RESULT:

```
GET / HTTP/1.1
Host: 51.145.178.10
Connection: Keep-Alive


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 20 May 2020 09:47:13 GMT
Connection: close
Content-Length: 315

      <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY> Not Found
  HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
GET / HTTP/1.1
Host: pci.travolutionary.com
Connection: Keep-Alive


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 20 May 2020 09:50:07 GMT
Connection: close
Content-Length: 315

      <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY> Not Found
  HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

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:	03/07/2020

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

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	ee:be:73:6d:5f:55:95:a3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.travolutionary.com
(0)Valid From	Aug 4 11:54:30 2019 GMT
(0)Valid Till	Aug 31 07:31:38 2020 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:e0:8b:a5:ee:42:a1:da:ad:24:93:1b:50:ea:53:
(0)	99:7b:a2:2f:a4:86:91:4b:1b:80:41:b8:40:72:b1:
(0)	67:5e:1c:63:21:23:92:98:ed:8f:e3:d6:ce:b7:f7:
(0)	6c:a0:bb:e1:25:7a:00:97:ec:82:08:ee:6e:b3:07:
(0)	5b:f1:4f:0d:2e:e1:f7:fb:3e:80:f5:da:77:74:ae:
(0)	1f:a5:bf:5a:33:26:c0:6f:ca:98:a4:99:7c:4f:88:
(0)	1d:ab:86:ed:eb:35:19:20:11:e5:42:91:2c:95:e4:
(0)	e6:32:d0:03:5f:83:5f:c7:03:17:5e:96:2b:d4:d5:
(0)	0e:e2:45:99:c1:b9:33:ca:40:27:47:16:f1:c8:1c:
(0)	bb:0e:38:6f:81:68:46:d3:a8:b8:d3:32:ee:df:83:
(0)	2b:bf:c5:09:13:eb:15:79:b8:70:fc:2b:85:5d:56:
(0)	f9:66:07:65:af:18:31:a9:42:a5:05:07:14:27:e2:
(0)	f7:da:89:e0:b3:61:e6:d8:a6:e2:35:72:7e:c8:e2:
(0)	12:0e:f5:25:16:6b:bf:dd:04:f5:4c:34:71:bc:0f:
(0)	49:63:26:c2:f4:fb:01:dd:39:f0:01:84:a6:aa:74:
(0)	87:c5:53:ea:32:7e:79:25:f4:e9:0b:9d:74:49:c7:
(0)	7a:c8:39:81:db:ab:54:e1:cb:f7:05:f9:9e:0e:cc:
(0)	b4:d3
(0)	Exponent: 65537 (0x10001)

(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-1278.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.travolutionary.com, DNS:travolutionary.com
(0)X509v3 Subject Key Identifier	02:3A:2D:E5:2A:0B:21:9C:D5:A7:FF:B5:7D:1D:8E:CE:47:C4:12:EB
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:
(0)	3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10
(0)	Timestamp : Aug 4 11:54:33.496 2019 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:20:42:B8:6D:52:37:26:1A:46:6C:4D:76:07:
(0)	61:9F:C4:6B:D4:9C:1C:8D:1E:A1:16:13:B2:6B:8C:71:
(0)	A9:48:2C:54:02:20:1F:F4:EF:27:C4:BA:48:AC:78:E0:
(0)	06:53:ED:F5:2B:6E:47:1C:27:46:53:96:26:E6:AC:26:
(0)	D2:18:B1:DA:E5:66
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 5E:A7:73:F9:DF:56:C0:E7:B5:36:48:7D:D0:49:E0:32:
(0)	7A:91:9A:0C:84:A1:12:12:84:18:75:96:81:71:45:58
(0)	Timestamp : Aug 4 11:54:34.770 2019 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:AD:D3:96:DC:6A:5D:98:E8:A5:B3:6D:
(0)	1A:CB:BE:13:22:02:9C:9C:B9:9D:E5:01:C1:B9:1D:D4:
(0)	21:5B:CE:33:4F:02:21:00:BD:6B:F4:50:C5:D2:C9:FF:
(0)	E8:1D:5D:AD:EC:D9:E8:87:08:4D:56:32:3A:63:04:D1:
(0)	96:0A:66:34:29:7F:C0:B8
(0)Signature	(256 octets)
(0)	45:59:a4:e3:a5:35:e9:91:0d:a6:14:4a:f5:e3:04:73
(0)	4c:97:c1:2c:f4:0a:41:c6:c3:2f:a4:a4:53:84:2c:78
(0)	a6:3e:b2:12:ab:bb:c7:d7:39:80:ab:d4:25:fc:10:d7
(0)	79:a7:b7:49:78:dc:db:be:ff:43:b0:c3:cc:dc:ed:50
(0)	90:19:9e:e2:f3:c3:ca:a7:29:35:dd:16:7a:fb:92:6a
(0)	aa:2b:26:36:3b:43:fb:23:3c:07:70:68:b5:fe:59:ed
(0)	2b:bf:05:bb:80:c0:35:1c:c0:9e:f3:fc:62:4b:76:8a
(0)	49:5c:e4:ee:bb:9c:86:33:7a:08:25:2d:44:26:53:f1
(0)	d0:a6:b3:58:84:4e:22:17:7c:59:2f:20:5b:38:40:21
(0)	a5:37:5b:18:72:00:4e:3f:74:2a:4b:e0:34:db:97:05
(0)	5c:b4:0e:60:e8:f2:3f:ac:18:6c:5a:6b:6d:b3:97:85
(0)	41:21:fd:13:2a:cb:5d:3a:8a:c6:80:27:f6:7a:bd:61
(0)	68:1e:01:fe:08:53:18:7a:b7:49:72:07:3d:d8:91:1c

(0)	c3:f8:6a:01:5f:c4:b4:b6:62:25:4a:3f:92:35:f9:55
(0)	2c:30:20:02:d5:e0:ef:91:d3:53:b1:17:38:8f:d2:54
(0)	64:f9:3f:9b:17:a1:d4:bc:5a:a5:d7:d8:d1:f4:a9:45
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:

(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	1828629 (0x1be715)
(2)Signature Algorithm	sha256WithRSAEncryption
(2)ISSUER NAME	
countryName	US
organizationName	"The Go Daddy Group, Inc."
organizationalUnitName	Go Daddy Class 2 Certification Authority
(2)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(2)Valid From	Jan 1 07:00:00 2014 GMT
(2)Valid Till	May 30 07:00:00 2031 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(2048 bit)
(2)	RSA Public-Key: (2048 bit)
(2)	Modulus:
(2)	00:bf:71:62:08:f1:fa:59:34:f7:1b:c9:18:a3:f7:
(2)	80:49:58:e9:22:83:13:a6:c5:20:43:01:3b:84:f1:
(2)	e6:85:49:9f:27:ea:f6:84:1b:4e:a0:b4:db:70:98:
(2)	c7:32:01:b1:05:3e:07:4e:ee:f4:fa:4f:2f:59:30:
(2)	22:e7:ab:19:56:6b:e2:80:07:fc:f3:16:75:80:39:
(2)	51:7b:e5:f9:35:b6:74:4e:a9:8d:82:13:e4:b6:3f:
(2)	a9:03:83:fa:a2:be:8a:15:6a:7f:de:0b:c3:b6:19:
(2)	14:05:ca:ea:c3:a8:04:94:3b:46:7c:32:0d:f3:00:
(2)	66:22:c8:8d:69:6d:36:8c:11:18:b7:d3:b2:1c:60:
(2)	b4:38:fa:02:8c:ce:d3:dd:46:07:de:0a:3e:eb:5d:
(2)	7c:c8:7c:fb:b0:2b:53:a4:92:62:69:51:25:05:61:
(2)	1a:44:81:8c:2c:a9:43:96:23:df:ac:3a:81:9a:0e:
(2)	29:c5:1c:a9:e9:5d:1e:b6:9e:9e:30:0a:39:ce:f1:
(2)	88:80:fb:4b:5d:cc:32:ec:85:62:43:25:34:02:56:
(2)	27:01:91:b4:3b:70:2a:3f:6e:b1:e8:9c:88:01:7d:

(2)	9f:d4:f9:db:53:6d:60:9d:bf:2c:e7:58:ab:b8:5f:
(2)	46:fc:ce:c4:1b:03:3c:09:eb:49:31:5c:69:46:b3:
(2)	e0:47
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Key Usage	critical
(2)	Certificate Sign, CRL Sign
(2)X509v3 Subject Key Identifier	3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(2)X509v3 Authority Key Identifier	keyid:D2:C4:B0:D2:91:D4:4C:11:71:B3:61:CB:3D:A1:FE:DD:A8:6A:D4:E3
(2)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.godaddy.com/gdroot.crl
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)	CPS: https://certs.godaddy.com/repository/
(2)Signature	(256 octets)
(2)	59:0b:53:bd:92:86:11:a7:24:7b:ed:5b:31:cf:1d:1f
(2)	6c:70:c5:b8:6e:be:4e:bb:f6:be:97:50:e1:30:7f:ba
(2)	28:5c:62:94:c2:e3:7e:33:f7:fb:42:76:85:db:95:1c
(2)	8c:22:58:75:09:0c:88:65:67:39:0a:16:09:c5:a0:38
(2)	97:a4:c5:23:93:3f:b4:18:a6:01:06:44:91:e3:a7:69
(2)	27:b4:5a:25:7f:3a:b7:32:cd:dd:84:ff:2a:38:29:33
(2)	a4:dd:67:b2:85:fe:a1:88:20:1c:50:89:c8:dc:2a:f6
(2)	42:03:37:4c:e6:88:df:d5:af:24:f2:b1:c3:df:cc:b5
(2)	ec:e0:99:5e:b7:49:54:20:3c:94:18:0c:c7:1c:52:18
(2)	49:a4:6d:e1:b3:58:0b:c9:d8:ec:d9:ae:1c:32:8e:28
(2)	70:0d:e2:fe:a6:17:9e:84:0f:bd:57:70:b3:5a:e9:1f
(2)	a0:86:53:bb:ef:7c:ff:69:0b:e0:48:c3:b7:93:0b:c8
(2)	0a:54:c4:ac:5d:14:67:37:6c:ca:a5:2f:31:08:37:aa
(2)	6e:6f:8c:bc:9b:e2:57:5d:24:81:af:97:97:9c:84:ad
(2)	6c:ac:37:4c:66:f3:61:91:11:20:e4:be:30:9f:7a:a4
(2)	29:09:b0:e1:34:5f:64:77:18:40:51:df:8c:30:a6:af

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:	07/12/2018

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

RESULT:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

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: 07/12/2018

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

RESULT:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

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:	05/24/2016

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 DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
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-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-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
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

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:	08/22/2018

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.

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.travolutionary.com, OU=Domain Control Validated			
Certificate	yes	Google 'Pilot' log	ct.googleapis.com/pilot/	a4b90990b418581487bb13a2cc67700a3c359804f91bdfb8e377cd0ec80ddc10	Sun 04 Aug 2019 11:54:33 AM GMT
Certificate	yes	Cloudflare 'Nimbus2020' Log	ct.cloudflare.com/logs/nimbus2020/	5ea773f9df56c0e7b536487dd049e0327a919a0c84a112128418759681714558	Sun 04 Aug 2019 11:54:34 AM GMT
Certificate #0		CN=*.travolutionary.com, OU=Domain Control Validated			
Certificate	yes	Google 'Pilot' log	ct.googleapis.com/pilot/	a4b90990b418581487bb13a2cc67700a3c359804f91bdfb8e377cd0ec80ddc10	Sun 04 Aug 2019 11:54:33 AM GMT
Certificate	yes	Cloudflare 'Nimbus2020' Log	ct.cloudflare.com/logs/nimbus2020/	5ea773f9df56c0e7b536487dd049e0327a919a0c84a112128418759681714558	Sun 04 Aug 2019 11:54:34 AM GMT

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: 01/29/2016

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=*.travolutionary.com,OU=Domain_Control_Validated The certificate will expire within six months: Aug 31 07:31:38 2020 GMT

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: 01/29/2016

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.

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

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:	03/21/2016

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 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:	03/19/2020

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:

TLSv1.2 session caching is enabled on the target.

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:	10/26/2016

RESULT:

Server Version	Server Banner
Microsoft-HTTPAPI/2.0	Microsoft-HTTPAPI/2.0

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:	03/16/2019

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

RESULT:

```
GET / HTTP/1.1
Host: pci.travolutionary.com
Connection: Keep-Alive


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 20 May 2020 09:39:48 GMT
Connection: close
Content-Length: 315

      <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY> Not Found
  HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
GET / HTTP/1.1
Host: 51.145.178.10
Connection: Keep-Alive


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 20 May 2020 09:41:25 GMT
Connection: close
```

Content-Length: 315

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY> Not Found
HTTP Error 404. The requested resource is not found.</p>
</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:	03/29/2019

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.

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) and
- Certain requests from QID 150172 (Requests Crawled)

RESULT:

Duration of crawl phase (seconds): 9.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

http://51.145.178.10/

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.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found. Aborting the CMS Detection phaseCMSDetection: 1 vulnsigs tests, completed 38 requests, 7 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.
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.
WebCgiOobTests: no test enabled
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK 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 (45 tests, 0 inputs)
Batch #4 Cookie manipulation: 45 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (45 tests, 1 inputs)
Batch #4 Header manipulation: 45 vulnsigs tests, completed 59 requests, 2 seconds. Completed 59 requests of 124 estimated requests (47.5806%). XSS optimization removed 28 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.
cve_2017_9805 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, 1 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:(3 x 0) + files:(10 x 0) + directories:(87 x 1) + paths:(9 x 1) = total (96)
Batch #5 Path manipulation: estimated time < 1 minute (109 tests, 1 inputs)
Batch #5 Path manipulation: 109 vulnsigs tests, completed 95 requests, 2 seconds. Completed 95 requests of 96 estimated requests (98.9583%). All tests completed.
WebCgiGenericTests: no test enabled
Total requests made: 220
Average server response time: 0.18 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

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

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 1050803334 with a standard deviation of 534441542. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4989 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: 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3 3 3 4 4 4 5
Duration: 30 milli seconds

Host Name Not Available

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/07/2004

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

RESULT:

No results available

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	04/22/2019

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 are probed.
1-79,81-442,444-1705,1707-1999,2001-2146,2148-2512,2514-2701,2703-3388,
3390-5630,5632-6128,6130-42423,42425-65535

Host Scan Time

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	03/18/2016

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.

For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

RESULT:

Scan duration: 2372 seconds

Start time: Wed, May 20 2020, 09:35:52 GMT

End time: Wed, May 20 2020, 10:15:24 GMT

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	Port
1	64.39.99.3	0.14ms	ICMP	
2	216.52.125.61	2.72ms	ICMP	
3	216.52.127.8	0.78ms	ICMP	
4	64.95.158.246	26.37ms	ICMP	
5	64.95.159.29	0.43ms	ICMP	
6	*.*.*.*	0.00ms	Other	80
7	104.44.233.18	1.30ms	ICMP	
8	104.44.21.207	87.49ms	ICMP	
9	104.44.16.19	87.68ms	ICMP	
10	104.44.17.155	86.27ms	ICMP	
11	104.44.16.113	88.25ms	ICMP	
12	104.44.17.57	86.24ms	ICMP	
13	104.44.22.224	87.26ms	ICMP	
14	*.*.*.*	0.00ms	Other	80
15	*.*.*.*	0.00ms	Other	80
16	*.*.*.*	0.00ms	Other	80
17	*.*.*.*	0.00ms	Other	80
18	*.*.*.*	0.00ms	Other	80
19	*.*.*.*	0.00ms	Other	80
20	*.*.*.*	0.00ms	Other	80
21	*.*.*.*	0.00ms	Other	80
22	*.*.*.*	0.00ms	Other	80
23	*.*.*.*	0.00ms	Other	80
24	*.*.*.*	0.00ms	Other	80
25	*.*.*.*	0.00ms	Other	80
26	*.*.*.*	0.00ms	Other	80
27	51.145.178.10	89.48ms	TCP	80

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: RIPE-ERX-51
Network description:
RIPE Network Coordination Centre

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: PNAP-05-2000
ISP Network description:
Internap Corporation

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	09/24/2019

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
Windows Vista / Windows 2008	TCP/IP Fingerprint	M4438:6611::80

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:	05/29/2007

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.

RESULT:
Based on TCP timestamps obtained via port 80, the host's uptime is 0 days, 19 hours, and 58 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

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:	04/24/2017

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

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

Web Server HTTP Protocol Versions — pci.travolutionary.com:80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	04/24/2017

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

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

Web Server HTTP Protocol Versions pci.travolutionary.com:443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	04/24/2017

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

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

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:	04/24/2017

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

RESULT:

Appendices

Hosts Scanned

51.145.178.10

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

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
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	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.