PCI Scan Vulnerability Report

PCI Status

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

Overall PCI Status	FAIL

Live IP Address Scanned	Security Risk Rating	PCI Status
66.49.252.119		FAIL

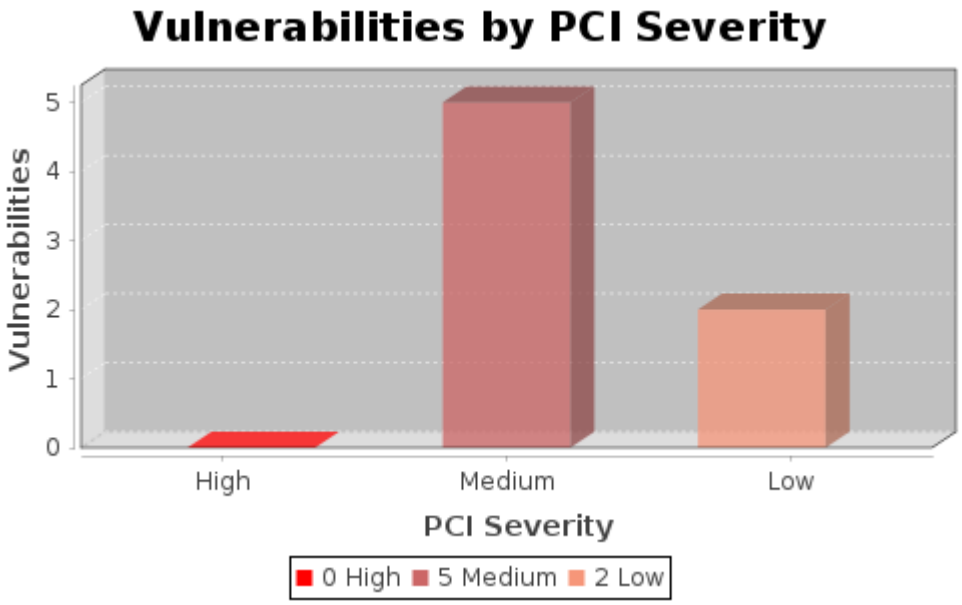
Report Summary	
Company:	Maximumsettings.com
Hosts in account	1
Hosts scanned	1
Hosts active	1
Scan date	November 25, 2022
Report date	November 25, 2022

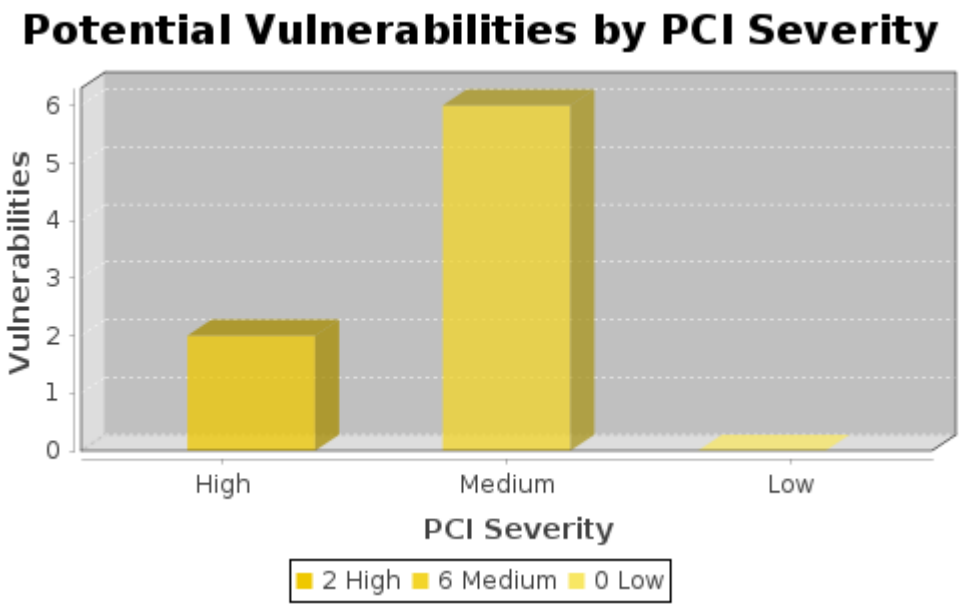
Summary of Vulnerabilities

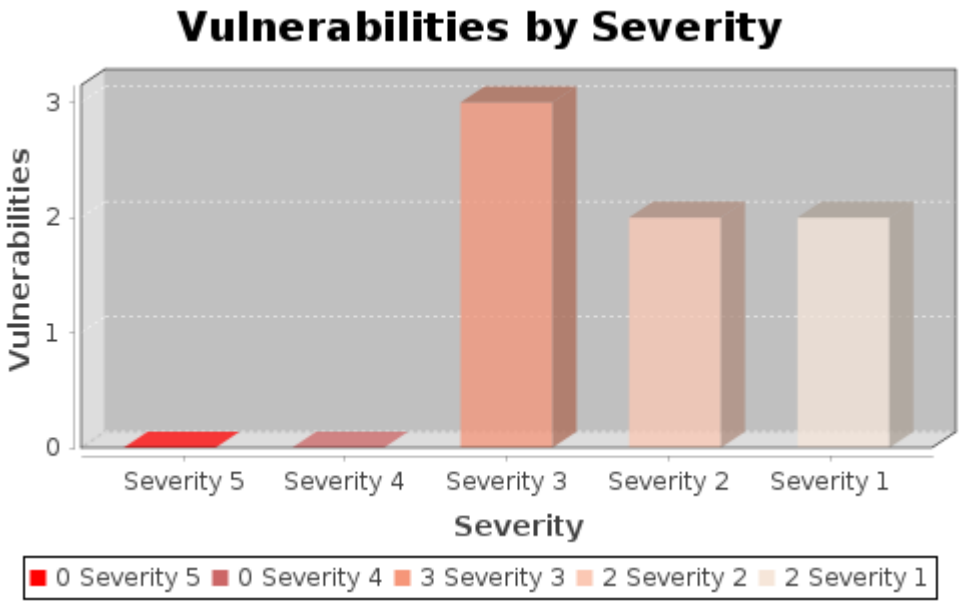
Vulnerabilities total:	76	Security risk:	5

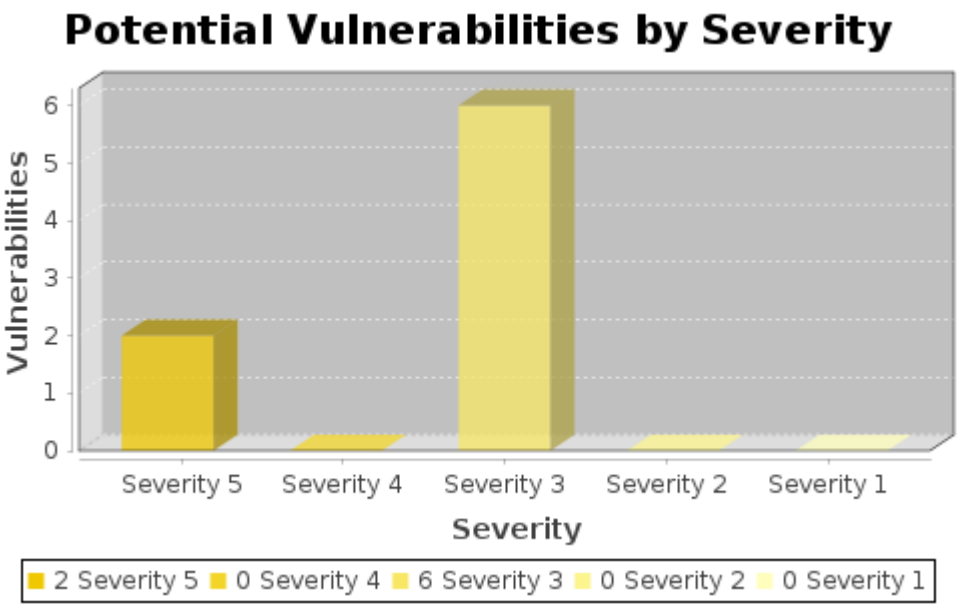
by Severity				
Severity	**Confirmed**	**Potential**	**Information gathered**	**Total**
5	0	2	0	2
4	0	0	0	0
3	3	6	3	12
2	2	0	8	10
1	2	0	50	52
Total	7	8	61	76

by PCI Severity			
PCI Severity	**Confirmed**	**Potential**	**Total**
High	0	2	2
Medium	5	6	11
Low	2	0	2
Total	7	8	15




Potential Vulnerabilities by PCI Severity
Vulnerabilities
0
1
2
3
4
5
6
High
Medium
Low
PCI Severity
2 High
6 Medium
0 Low


Vulnerabilities by Severity
Vulnerabilities
0
1
2
3
Severity 5
Severity 4
Severity 3
Severity 2
Severity 1
Severity
0 Severity 5
0 Severity 4
3 Severity 3
2 Severity 2
2 Severity 1


Potential Vulnerabilities by Severity
Vulnerabilities
0
1
2
3
4
5
6
Severity 5
Severity 4
Severity 3
Severity 2
Severity 1
Severity
2 Severity 5
0 Severity 4
6 Severity 3
0 Severity 2
0 Severity 1

Detailed Results

66.49.252.119 (order.maximumsettings.com,) Ubuntu/Linux

Vulnerabilities total:	76	Security risk:	5

Vulnerabilities (7)

Same Site Scripting port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P
CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:

Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:

The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:

Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:

url: https://orders.maximumsettings.com/
matched: Same site scripting detected
Host: localhost.orders.maximumsettings.com IP: 127.0.0.1
Host: localhost.maximumsettings.com IP: 127.0.0.1

Same Site Scripting port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P
CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:

Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:

The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:

Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:

url: https://order.maximumsettings.com/
matched: Same site scripting detected
Host: localhost.maximumsettings.com IP: 127.0.0.1

HTTP Security Header Not Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**3.5** E:U/RL:U/RC:UR
Severity:	**2**
QID:	11827
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-08-03 12:34:37.0

THREAT:

This QID reports the absence of the following HTTP headers according to CWE-693: Protection Mechanism Failure:
X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:
This unauthenticated QID looks for the presence of the following HTTP responses:
The Valid directives are as belows: X-Content-Type-Options: nosniff

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

IMPACT:

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

SOLUTION:

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

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

Customers are advised to set proper X-Content-Type-Options and Strict-Transport-Security HTTP response headers.

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

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

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

Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

RESULT:

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

GET / HTTP/1.0
Host: orders.maximumsettings.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

HTTP/1.1 200 OK
Date: Fri, 25 Nov 2022 21:05:50 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Set-Cookie: ci_session=remdqn12gpecd97ncgbvgpe3mfdoo01h; expires=Fri, 25-Nov-2022 21:15:50 GMT; Max-Age=600; path=/; HttpOnly;HttpOnly;Secure; SameSite=Strict
Connection: close
Content-Type: text/html; charset=UTF-8

HTTP Security Header Not Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**3.5** E:U/RL:U/RC:UR
Severity:	**2**
QID:	11827
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-08-03 12:34:37.0

THREAT:
This QID reports the absence of the following HTTP headers according to CWE-693: Protection Mechanism Failure:
X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:
This unauthenticated QID looks for the presence of the following HTTP responses:
The Valid directives are as belows: X-Content-Type-Options: nosniff

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

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

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

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

Customers are advised to set proper X-Content-Type-Options and Strict-Transport-Security HTTP response headers.

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

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

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

Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.
RESULT:
Strict-Transport-Security HTTP Header missing on port 443.

GET / HTTP/1.0
Host: order.maximumsettings.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

HTTP/1.1 200 OK
Date: Fri, 25 Nov 2022 19:54:13 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Set-Cookie: ci_session=3pb51qukhnbeqj7po9sq5n6ontaabgg4; expires=Fri, 25-Nov-2022 20:04:13 GMT; Max-Age=600; path=/; HttpOnly;HttpOnly;Secure; SameSite=Strict
Connection: close
Content-Type: text/html; charset=UTF-8

TCP Sequence Number Approximation Based Denial of Service

PCI COMPLIANCE STATUS

PCI Severity Level: MED

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

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score:	**4.3** E:F/RL:T/RC:C
Severity:	**3**
QID:	82054
Category:	TCP/IP
CVE ID:	CVE-2004-0230
Vendor Reference:	-
Bugtraq ID:	10183
Last Update:	2022-05-04 10:15:26.0

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

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

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

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

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

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

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

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

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

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

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

For Microsoft: Refer to MS05-019 and MS06-064 for further details.

For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P

For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14

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

For NetBSD: Refer to NetBSD-SA2004-006

For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml.

For IBM : Refer to IBM-tcp-sequence-number-cve-2004-0230.

For Red Hat Linux: There is no fix available.

Workaround:
The following BGP-specific workaround information has been provided.

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

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

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

SSL Certificate - Will Expire Soon — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**0** AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Temporal Score:	**0** E:U/RL:W/RC:UC
Severity:	**1**
QID:	38174
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-10-11 20:02:26.0

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

Please refer to the scan result for details on when the certificate is expiring (within a week or within a month).

IMPACT:
A certificate with a past end date cannot be trusted.

SOLUTION:
Please install a server certificate with valid start and end dates.

RESULT:
Certificate #0 CN=*.maximumsettings.com The certificate will expire within a month: Dec 3 18:52:46 2022 GMT

ICMP Timestamp Request

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

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

VULNERABILITY DETAILS

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

CVSS Temporal Score:	**0** E:F/RL:W/RC:C
Severity:	**1**
QID:	82003
Category:	TCP/IP
CVE ID:	CVE-1999-0524
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-04-29 03:59:17.0

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the *Ping of Death* or *Smurf* attacks.

However, you should never filter **ALL** ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:
Timestamp of host (network byte ordering): 19:24:24 GMT

Potential Vulnerabilities (8)

EOL/Obsolete Software: jQuery 1.x and 2.x Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

Automatic Failure: Unsupported software

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**10.0** AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Score:	**7.4** E:U/RL:OF/RC:C
Severity:	**5**
QID:	13477
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-01-05 13:33:31.0

THREAT:
jQuery is a JavaScript library designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animation, and Ajax. It is free, open-source software using the permissive MIT License.

jQuery 1.x and 2.x has ended. No further bug fixes, enhancements, security updates or technical support is available for this release.

QID Detection Logic(Unauthenticated):
It checks for vulnerable versions of jQuery from default web page.

IMPACT:
The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.

SOLUTION:
For additional information please refer to: jQuery 1.x and 2.x

Best Security practice is to remove the End of Life software and install a supported version of jQuery.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

jQuery 3.0

RESULT:
EOL Software:jQuery Version 1.x or 2.x Detected.

<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/jquery.js

EOL/Obsolete Software: jQuery 1.x and 2.x Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

Automatic Failure: Unsupported software

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**10.0** AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Score:	**7.4** E:U/RL:OF/RC:C
Severity:	**5**
QID:	13477
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-01-05 13:33:31.0

THREAT:
jQuery is a JavaScript library designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animation, and Ajax. It is free, open-source software using the permissive MIT License.

jQuery 1.x and 2.x has ended. No further bug fixes, enhancements, security updates or technical support is available for this release.

QID Detection Logic(Unauthenticated):
It checks for vulnerable versions of jQuery from default web page.

IMPACT:
The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.
SOLUTION:
For additional information please refer to: jQuery 1.x and 2.x

Best Security practice is to remove the End of Life software and install a supported version of jQuery.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

jQuery 3.0

RESULT:
EOL Software:jQuery Version 1.x or 2.x Detected.

<script type='text/javascript' src='https://orders.maximumsettings.com/assets/js/jquery.js

jQuery Prior to 3.5.0 Cross-Site Scripting Vulnerability — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — Automatic Failure: Cross-site Scripting (XSS) vulnerability

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**3.4** E:POC/RL:OF/RC:C
Severity:	**3**
QID:	13770
Category:	CGI
CVE ID:	CVE-2020-11022
Vendor Reference:	Jquery
Bugtraq ID:	-
Last Update:	2022-01-05 13:33:31.0

THREAT:
JQuery is prone to a cross-site-scripting vulnerability because it fails to sufficiently sanitize user-supplied input.

Affected Versions:
jQuery versions greater than or equal to 1.2 and before 3.5.0.

QID Detection Logic(Unauthenticated):
It checks for vulnerable versions of jQuery from default web page.
IMPACT:
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site.

SOLUTION:
Vendor has advised to Upgrade jquery to version 3.5.0

Patch:
Following are links for downloading patches to fix the vulnerabilities:

jQuery

RESULT:
jQuery Version Prior to 3.5.0 Detected.jquery.dataTables.min.css' type='text/css' media='all' />
<

jQuery Prior to 3.4.0 Cross-Site Scripting Vulnerability — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — Automatic Failure: Cross-site Scripting (XSS) vulnerability

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**3.2** E:U/RL:OF/RC:C
Severity:	**3**
QID:	13481
Category:	CGI
CVE ID:	CVE-2019-11358
Vendor Reference:	-
Bugtraq ID:	108023
Last Update:	2021-03-05 04:31:40.0

THREAT:
JQuery is prone to a cross-site-scripting vulnerability because it fails to sufficiently sanitize user-supplied input.

Affected Versions:
jQuery Versions prior to 3.4.0 are affected.

QID Detection Logic(Unauthenticated):
It checks for vulnerable versions of jQuery from default web page.

IMPACT:
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

SOLUTION:
Vendor has advised to Upgrade jquery to version 3.4.0

Patch:
Following are links for downloading patches to fix the vulnerabilities:

jQuery

RESULT:
jQuery Version Prior to 3.4.0 Detected.
<script type='text/javascript' src='https://orders.maximumsettings.com/assets/js/jquery.js

jQuery Prior to 3.5.0 Cross-Site Scripting Vulnerability — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Cross-site Scripting (XSS) vulnerability

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**3.4** E:POC/RL:OF/RC:C
Severity:	**3**
QID:	13770
Category:	CGI
CVE ID:	CVE-2020-11022
Vendor Reference:	Jquery
Bugtraq ID:	-
Last Update:	2022-01-05 13:33:31.0

THREAT:

JQuery is prone to a cross-site-scripting vulnerability because it fails to sufficiently sanitize user-supplied input.

Affected Versions:

jQuery versions greater than or equal to 1.2 and before 3.5.0.

QID Detection Logic(Unauthenticated):

It checks for vulnerable versions of jQuery from default web page.

IMPACT:

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site.

SOLUTION:

Vendor has advised to Upgrade jquery to version 3.5.0

Patch:

Following are links for downloading patches to fix the vulnerabilities:

jQuery

RESULT:

jQuery Version Prior to 3.5.0 Detected.jquery.dataTables.min.css' type='text/css' media='all' />
<

jQuery Cross-Site Scripting Vulnerability — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Cross-site Scripting (XSS) vulnerability

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**3.4** E:POC/RL:OF/RC:C
Severity:	**3**
QID:	13772

Category:	CGI
CVE ID:	CVE-2020-11023
Vendor Reference:	Jquery
Bugtraq ID:	-
Last Update:	2021-05-17 12:30:05.0

THREAT:
JQuery is prone to a cross-site-scripting vulnerability because it fails to sufficiently sanitize user-supplied input.

Affected Versions:
jQuery versions greater than or equal to 1.0.3 and before 3.5.0.

QID Detection Logic(Unauthenticated):
It checks for vulnerable versions of jQuery from default web page.

IMPACT:
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site.

SOLUTION:
Vendor has advised to Upgrade jquery to version 3.5.0

Patch:
Following are links for downloading patches to fix the vulnerabilities:

jQuery

RESULT:
jQuery Version Prior to 3.5.0 Detected.jquery.dataTables.min.css' type='text/css' media='all' />
<

jQuery Cross-Site Scripting Vulnerability — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — Automatic Failure: Cross-site Scripting (XSS) vulnerability

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**3.4** E:POC/RL:OF/RC:C
Severity:	**3**
QID:	13772
Category:	CGI
CVE ID:	CVE-2020-11023
Vendor Reference:	Jquery
Bugtraq ID:	-
Last Update:	2021-05-17 12:30:05.0

THREAT:
JQuery is prone to a cross-site-scripting vulnerability because it fails to sufficiently sanitize user-supplied input.

Affected Versions:
jQuery versions greater than or equal to 1.0.3 and before 3.5.0.

QID Detection Logic(Unauthenticated):
It checks for vulnerable versions of jQuery from default web page.

IMPACT:
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site.

SOLUTION:
Vendor has advised to Upgrade jquery to version 3.5.0

Patch:
Following are links for downloading patches to fix the vulnerabilities:

jQuery

RESULT:
jQuery Version Prior to 3.5.0 Detected.jquery.dataTables.min.css' type='text/css' media='all' />
<

jQuery Prior to 3.4.0 Cross-Site Scripting Vulnerability — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — Automatic Failure: Cross-site Scripting (XSS) vulnerability

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**3.2** E:U/RL:OF/RC:C
Severity:	**3**
QID:	13481
Category:	CGI
CVE ID:	CVE-2019-11358
Vendor Reference:	-
Bugtraq ID:	108023
Last Update:	2021-03-05 04:31:40.0

THREAT:
JQuery is prone to a cross-site-scripting vulnerability because it fails to sufficiently sanitize user-supplied input.

Affected Versions:
jQuery Versions prior to 3.4.0 are affected.

QID Detection Logic(Unauthenticated):
It checks for vulnerable versions of jQuery from default web page.

IMPACT:
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

SOLUTION:
Vendor has advised to Upgrade jquery to version 3.4.0

Patch:
Following are links for downloading patches to fix the vulnerabilities:

jQuery

RESULT:
jQuery Version Prior to 3.4.0 Detected.
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/jquery.js

Information Gathered (61)

Content-Security-Policy HTTP Security Header Not Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Content-Security-Policy HTTP Header missing on port 443.
GET / HTTP/1.0
Host: orders.maximumsettings.com

Content-Security-Policy HTTP Security Header Not Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3

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

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Content-Security-Policy HTTP Header missing on port 443.
GET / HTTP/1.0
Host: order.maximumsettings.com

DEFLATE Data Compression Algorithm Used for HTTPS

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**3**
QID:	42416
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2013-08-10 00:02:05.0

THREAT:
HTTP data is compressed before it is sent from the server. DEFLATE data compression algorithm uses the LZ77 algorithm which takes advantage of repeated strings to more efficiently compress output.

DEFLATE data compression algorithm is prone to be unsafe as described in the BREACH attack. If an attacker can inject a string into a HTTPS response intended to match another unknown string (the target secret), they can iteratively guess the secret value by monitoring the compressed size of the responses for different guesses. Note: The attacker needs the capability of reading responses received by the user's browser and the capability of cause the victim to send requests from their browser to perform BREACH attack.

This QID detects that the remote HTTP server is using a gzip or DEFLATE (zlib) compression format which is using DEFLATE data compression algorithm.

IMPACT:
N/A

SOLUTION:

N/A

RESULT:

HTTP/1.1 200 OK
Date: Fri, 25 Nov 2022 20:43:13 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
X-Content-Type-Options: nosniff
Set-Cookie: ci_session=t249kl338kle3kjnuct1h31kb251pq6r; expires=Fri, 25-Nov-2022 20:53:13 GMT; Max-Age=600; path=/; HttpOnly;HttpOnly;Secure;SameSite=Strict
Content-Length: 10560
Content-Type: text/html; charset=UTF-8

_1F_8B_08_00_00_00_00_00_00_03_ED}_DBv_DB_B6_D6_EE_FD_1A_E3_7F_07,
_B5_ABn_F7*u_F29_B1_D5_E18I_936>4v_DA4_FF_F8_87_06DB_12l_92`@P_B22_F6_ED~_92}_B5._F6S_F4_C5_F6_9C_00IQg_C9_B2c_B8_89_DA_18
_89_C371'&_E6_C4_81_FC_AF_7F_1C_FC_F3_F9_D9_F1_E5_9F_E7/HW_05~_E3_BF_FEq_80!q}
_1A_C7_87_A5P8Wq_89_F84_EC_1C_96XX_82_E7_04~_07]F_BD4_AE_AF[4f_A4+Y_FB_B0_D4U*_8A_9FT*;;_E5_AD_FDr}_BB^_AE_D5_F6+_A5b_EA_80)
J_11*_16_AA_C3_92_DB_A52f_EA0Qmgo$_9D_E2_CAg_8D_13z_C3_83$ _17L)_1Evb_F2_DD7{_F5Z_ED)
y_CE<_EER_C5<_F23_18_B9P_92_D1_00R_1CTL_C6_F1_1A_11_99_C3>&_BCwX:_A6n_979_C7_80A
_BF4_04_03_04_BB_F8_E8G_02_B1X _B1 _89_95#Y_8F_FA_DC_83_EAJ_A42_B7_E8sI;_01_9DR_E6_A2_8C/n".Y_C8Y_9D_96%
_04b_0FK=_CE_FA_91_90_AA_90_BA_CF=_D5=_F4X_8F_BB_CC_D1_17?_12_1Er_C5_A9_EF_C4._F5_D9a_AD_B4"_D3_D2_A4_C3Ly_E6_D8_95<RD"
_00_A3_D8_8D_AA_D1_1E5w_8B_B5_E0_AFG%_89_B9b_CDD_FA_E4_90_CC_AA_ED_E9d._84_B8z_AE_B8+_FA_CD_D8_88K3_12Q_12A_FE_8D_8Di)
_99_9BH_AE_06M`_8F{_8D_A9j_D3_92_F1_B6_84FO_81L-_88GM_EAy_F8tg_AB_BC_B9__DE_DF+_D7_B6G_CA:_A8_98_C6_81_B6)_DC_F4yxM$_F3_0F7_BC0v"
`_06Snw_C3_B0e_03I_06_8A_DB_C0_E1_B8_DC_11_A2_E33_1A_F1_B8_EC_8A_A0_B21*_1AK_15_14_97_FBe!;i_DE_A9_B9c5_F0Y_DCeLm_10_EE_C1_B5hc3:
_1A_83_E3_C6_F1_06I_CB_9C_81_0B_92_FC_D4_86~_E8_0F_0E_CF"_16_FE_AB_FE_EC_82_86_F1_BFv_8F_CFE_14q_88m_1EmU_AB_FF_AA_1Fo_EB_BF;
_FA_EF_AE_FE_BBW_AD~_F7Mus_EFi_9C_B4P#_F8_14_AA_86_FB:t@_C6_CC_D3_1E_93_87_B5ru_C3_08_DF_86_16>,
_00_85@_0F7_A8_EF_CFj_9C_D2_90_BC_D2_D1_07_ED_C7T_8C_C5V_A0_B82_84%_E8K_8AuPZ_A0_98._DD_DC_DBr_B6_AB_E2_D9_BBW
/_82^_F4_DB_BFk_FE_1F[_83_ED_DD_F3_CB_97A_F7_98_BE_8F_AA'o_B6_BD_9D_EAI_EDd7yU_FFw_F8_F1_1D_EF}z_CDZ_DD_D0;_FB_E5_D7_FA_1E
{m_E8_BCR_C4_B1_90_BC_C3_C3_C3_12E8_08D_12_97fpg_0E|_D7_0B_AF_80_01_BEH_BC_B6O%_D3_BC_A0W_F4_A6_E2_F3V_ACY_E5_D0>_8BE_C0*
[_E5_DDrU_D3V_BC]_06_DD_A9 _9D_DEr_D4WL_86Z_FF_99NO_A3_C8G_FD_CBEX_91q_FC_EF_9B_00_14_A9_D6_BC_87_A5I_9D-_E9_C7D<%
/_19_F32_E8<_F4_D8_8D_B7_BB_B7U_C6!_E7_A76<:_84_82_EA_A5Y_CC_BB_1B_08_C7"
_08@__C6_93X_E8_8EG_0BX_DC4_A13_0F_D4D_87_E9GN_CB_17_EE_B5_03_ED._A9_1C_8C_F4_99_85_C2_A6K+_EB,
_ABK_F7_1Dcqa_DC_13_C1r`>_03_9C_96_10*V_92F_99_A0_AE_DDD_CB_F2_A4_0F_A9a_F8_94_AA>_B3_EA;_AC_8D_F9_CC]_AF&lk_DDZ!_ED_DD_A2_8D!
_D7=4/(_A82_98O_F0__0BR_94C_A6*_B5r_ADZ_06_00X_F3_D5_C7_84_C9_81NqiR|f._9F_C1_B0_E2_D3_C1_05hd_DFo_81Iz_DB_CAo3_C6_A0]
_19q_F7_9AI3_D4_98.U(_BDhnm_8C_99[_1B$_96_EE_02
_AF_F2_16_BE_8A7_1A_B9-_82_A6]j_D2WR_9B>_BDl o_90y_01##_C2?_1D_87_9C_03_9D_82zL_82_D1M_A5"_8E3_96_E2_C0_E3_BD,w_CC_D0_1Cq_C0L-
A_C5_F0_A01_91_BCP_E0_8B_D0_8B'_CB#_AF_18>_1D_DE<_E57V^W_97_85_BD_A4_D4_85q_AF_94;;_CAA+_D51_CF_C7_8DX_C3_90{J
{_BC_A3G_9D_D1_92u2_E8=y_81_B4_07_82DL_E0x_ACM_13_e_97_B1_02~_0FH_D6_E3_08_14_06_8EB;_F1}_D2_A5_B1_D3_A2_EEuG_8A$_F4_C6_81_E8Z
_ED_8B_F6?_E5!"_1EO6_86_FBHI_DEJ_14_9BK_C0_B4*_A8R_D2A_90_90[_89p_1A_A2<[_E2O_85_91_FEfg_D4_99}>^%_8C_15_8E_08_D9_BC*_F3_DCt_AC_BB
|_04Eb,_81_D4!_D0V*X Tv_C0_C4_04_D9>_C3T_E4T_F4_0F*tA-_07`L-J2_9D_04_D5_17_B7"_C1_17`_19_CE_A7_00<_1D_BF]
j_BC_C1_94k_93pPI_FCY_02_A1_FB_EE_8Cg(d_D0ug_8B_D8_9C|F8M_0F_Y4_D3_DE4_BD_CF_8Ed2_B2_9BZ_8E_A9 _8F_95_A2D_07_99_12_C1Q
(_BD_C0_FE_E5_FB4_8A_F3_DBi_B3_7F_93_E6_01_131Y_C4_DA_83\&_DA_94_B4_A9_83_C3_0B*_C3_F9_9C0_18_E7%)
J_0B_08_CBT1A5_07_9A_04I_E4_E4_F2_A0_A3o_90X_D1_D0_A3_D23W)E`_9BM_D7:
#u#_E7R_1D_A63_CF_E4_D6_B0_11_82_8E_1E_A9f_0C_87_D9P_C5_03_DAa`_07_A1*_C6_92_9D_AD_F2U_D4)_11_B0_FE'_AD_FA_9C$_8DA'
_8F_F5_08_8E_A6}en_F3_CE_EA)K_C9_F9_0Ci_9D_93_EB_18A_B90_84w_1964A{!_FE_91_B4_85_0C _80_16'_02_1E_C9l:_07_1F_10-_82@_E6r]!
_13_D4_8C_8FC_C1_D52_B0_9C_B8_82_FE.t_8A_AC_A8B_14|_D5_AEJ_FB_02:_AD_DF_A4q_91`_A7X(6_A0_1E_11_C2p_80_C3_81_B3W_DD_CA_99_98_DF%
_C3_E7_D8__1D_E3_8A_14_EE_8A_D6_154fv_DFM_A4_846s_86_F9_D3;_CD_08d_A99V"_D6_D8X_A2_EF|3b_1D_18_B1*5^_C1M_14_9E%_C7_82qbw>;_B1;K_11
[_F9_89&_AA+_E4am_82_E27`_9C_C6`_F5_B0~_BC_06_E1_BB_9F_9D_F0_DD_E5_B8_1CI_EE_C2_C5_04_D9_E7_E6_FE_1A$_EF}v_92_F7_96#_B9M?
N_90_FB_92~_D4_13_EB_BBO_D7_E0r_AD_F6_B9I_86_1A_97#_99Q_95_98_D9_F51_BA_D3_07k_F0y_FF_B3_F3y_7F_8Ch_ED`_8B
HB_AE_06_D3_CD_C5Q_B2_87_D6c_CB_A7_E1u_A9q_9C_E5^_83_F9_D5_CF_CE_FC_EAr_CC_D7.
_92_AB&x_7F_91D_B8_86_B2_04_C9_0B_EDb=_C6W_CAcC_EF_F4_81{_9A_85qP_81_AC_D3\N_B46f_9B_19_C6mgr_DC_._D8
(_E39_C6\Gh_DCR_E3_1F_D3_9E_A4N_E5B_BB#_80_84_CD_CCl_01_0F_D7_81_DE_14_890_E6=F_A4_E8O)a_C4_80W_D8ZI_10_82_E5_E3;q_E0_D4_EA:

_E6w_1C_D1n_03_1B_9D_FCzo_EA_83_C0_CB_AEk_D9_F5_DE_12_A8sW_1F_ED+_9CQq_C0?_CB_8B_1E_FB_CD_F12d_E3_A0[o_1C_B9.
_F8_EE_8A_1CK_A6_F9_06|_AA_CF_C0_A4_85a_86_8C_CC_A8_EC_1F_0B_A93_ED>_1Bf1)_EB_F0_18_08w_FA_92F_D1L_8E/_FB_1B_B3HG9Z_CBYV_AB
/YO_B1_BCt_A8v(_B4_EA
0_A7_15_A1UI_81_EDD_80_E3#n_9C_80_87d_C5_16_C0)_8F_95_9B_AC0O_90A_CA|_D8_83_EEV_EE.n_82_86;?z_FD_9C_1C_1D_1F_9F_BD;
_BD_BC_00A_DAj_1C_C4_11_F34_FD_ADj_95_E8_B9_8E_A6)_A2_D9_85_C6%_DF_93_D7!_FAw_8A_1C_B9_8A_F7_8C_FA_F8_E1_A0_82y_8D_BA_9B-
_1FK_A0n_0B_A1_D6_16_96_95_EA_A6Y_D5-_05_C4s_E9_FA_8C@_D4_01_B7)`$_A2_DCkR_D3_ED_C6&uV'S_B7_CE_CA_B9
_D3wa+_8E_9E_EA_FC_B3_95_C4_F4*W_91_A2_19JcN_D2_C5SO_8B_8B_BC_FDC_DD_03_F5_BC8(_05_9FQ_F9_84_B4_C0_DD}_9A_CD_08_CF_CF_0C:
u_CE_C0_BCtK_CC_02_E4_F18_F2_E9_E0 E_C8_9E_E6F_82_16_A8L9_E6_E3_DB_9C_E1_AA_A8_DC]_13/p*w8_1C:_E8)_E7_9Bh_8AZ_89_86_CC'
_FA_AF_D3_F2_93_91_E9_CE_89t_D9_A8Uj_A4J_81_1C_BF}qt_F9_FA_ECt_DC_B0_98_CC_8A_D3_FA_133_DB_85TK_8D~_D9o_FE_BC4_B4T:
_A2_10_82J_AD_9E_8F
4_E2_8A_FA_FC_13#_ED_BE_B3_03_CA+h9_9BUL_84_A3_E4_9C_89_0E_B0_DA_18j_1E9_B4g_FB_91_DB_DE53_1C:_EA_B4w_AA
{N_B4_B3_BD_E5_88_FAp_E7_92_F3_EE_A2D<._0FK_BE_9A?MX_A0_80l)d3_88;M_B8_99_89_EA_9C_AC_08l_A8_1Ee_E0_B4h_CC]_12%
_D2_ED_E2F_96_88_BA_D7`_C6_EA9_1F_07|m_FE _AD,0_C6_03_06_AE7P_10_89X_19Z_DA2h&QG_82:/_110]Aw_EB_A9_16_B3_F9'-_C8_E1a
[8_BA9Va_DB_0E_8E_10_D4_DDD_96l.r_05_DA_9C_F9_1E_18`_B9i_A5XD"_C7w_80_B3_0E_98eUC_13_DE_AE-
D_BA_C4$_F9_A4_05_0BnB_EC_98N4_EC_96_E9`_D0_C4Vj_EA_85_E7e_A6_E0'k_D0_E5_ED,_9Bw<_BFf6_AE_E4D_AB_94_A0K_F1i_8B_F9EJ%
*_1As_D3_A0_DA,5NA"_9E_C0_80_83_B7W_AD`_92_CC_FDUA_EArx_18%
_C5_BD`_99_9C_E2_DF_12_91_B8_BFM2o_A4ERrH_D24_89z_14_D4_1E_E8_9F_B9_93_B6S+__D0+_D7N_FF_19yy_DE_85_11_88_D8_CA_CD_08_D1-
dg_9A_EA+?_81_9F/_C05_F6_AD_E5'Ct_0B_F9_99_A6_FA_CA_CFM_9C$_0B_DB_1C_C6x_BB_F9_EA_1A_94_CD%_F8k)__D3_C9_8F_BF_DF`}
_E4y_E0_C4_0F-9(-8_87_92
_0C5_A8_16_AA_82,_1D_18_85Y _9FIh_EC_E4_E61W_83_87f_E5L%_00_D8_162_D4$_FA_EC*_C0Rn_A2_B3
_1F_9C_A1f_FFg_AE_CA5_A6E_8C_8C_9Ai_C2_A6X_B9q_EE_E2w "=_BB_98_89_D2Q_BB_D3_A5!
_C7_D9G_D0y_C3_8B_83_8AI_F8_00_10gA_FD_EB_FF_F8z_B7_8B -_04x_E4_B7_A0_F5(_B4_A3_89X
_B1_C3_A4_81_A8#6B_0C_00_98KCrA_03_81HG_AEm_04_1CzBJDj"VB_EC_08_#_C4_D0N_80 _F7S_88:f%H0_A4_05_C2_880_B3_B8_9D@y'
_A1z_AB_DA3*[_89g_10_8F_DF_B4_11_BA_EC0_00_1A"_E0,j%_CC_80_19Uo"VBLZ_1A _046_C2K_F0_84_90_AF_DB0_8B_DA
3_07i'_C4OL_B6(_BF_D2_16_1E_B7_10_E83_DA_A5_01_05_A74_8D_D8 QR_1Ej_88_18_B1_12b_D8_F1_A9_C7_E2.
_A2_CC_E2V_02_05Q_F4_84_E6_B7_89_D9_08_92_F9T_E21_DE4b'
_C4_0EO_02_11#vB_E4_9F_98F_08_A1_95_00C_DD_AB1_B0_12_9E_0C_B4_91_96Fl_84_D8M_F4_1C_81 m_04(|_DE_C3_91:_8DX 1_A4\b?1_11+!
_C6`_CEj'_E1_15_93_9FXG_F4_B41>_FD_BE_95_04_A8_B8Od_13_B3_12d_D2c_8A_BC_8E_CD_8C_D6_C8_A5_8Dp%_FD_C4}_C0_A9C+_01r_C5_E3.
y_1Dz_9C_86_E4_CCe_F0_F7_92I_B8-_E4_00_81_CF{n1A_BFs_D9_E1a*_19_F1_90_90_D1_FBV_12_90_84_8C#`_0Cm_04_98_F8_1D_AA=_BB,f%
Hyj_96_BC_A4_B1@_A0_C3+;_C1&_D0_BF4N_8CX_08_F1_98_06-_E1!_D3_B3_98_9D _99_14xv?
_8BY_04_D2_ACy1|_DDT_1A_DB_18_E2_0E_A9_A7_9B_16C_8B0_0F_01F_8C_FC_CE_A4_C7_10d_16_B7_12_E8 _A0_05_AD?
zm#`_16_E2_0C_1E9j_9B_A5_9A_B7,JZ>w_01_FA_8C&apos;6_12_D1_A5`_8B_E1_+_C1q_1F_C5_16_03;
_E1_A1_C9_AD_03+_E1I_1E_AB_80_C6_B9_C9=~_C7F_D0_C2_151_F9_EF__19_C3_17_0B_FCOA_1DL_7F`% _BE_08Zz_BCMcV_82_0C_84_14_BA]
u_C4J_88_E2_BA_C8_FF_E1_95_95`cE_C9[_BDL:_8C_DB_08T
_AA_B4p_9A_88_8D_10_F5_1A_DE_B1_9DKx_C7_89_A4._15_88OGl_848_88_F4_EC_BE m_04_F8_89_B9_DD_A2_BD4rm!_E0_E7,_10_AE_84_EE_E2_E6
(_89h_EBw_E5_1C_8B_B0_03_D2_B0(_85_95D_85_01_95_D7_88]Gl_84x_C5["Q_E0^g1_1BA_8A_80_87Z_F1g1_8BA_16_DD_94_C9{_16_02_7FAcE.9_18)
_A5_C60n#P7_A1_9EFi"6B_EC_0C_F0_ED_E7:_B0_11_9EO._A8_DFK[qxa#_D4_8F UBrp_F2_7FNx_88_AF
{_98_B8e#l_C9_95~7E_1A_B1_11b_AC_84_DEd_96Fl_84_A8_BA\D_1Ac_1A_B3_10_E4K_EA__A3_B34_F4_A0_C6_EFX Z
VD_B8_B4_11._BF_02_D3_04_FFZ .4_B3>i_C4F_88_92_86._03_84:_B4_12 _0B_C13_01}_AE_17_D7G._ED_85{._FCA_C8b>D_9C_DF_B1_17_F4_05X_F7]
&_87+_D4_9C_C59_FEi_0F-$_E5g_DA_C2_15,_1DX _CFLK_9A_D0F_80L_C8_8EFh"
VB_94_01_07_08QGl_84_D8_D5_CAJ_076_C2_C3_8Fk_F8_8A_82_8D_9FGm_84)_19_C3_B1_C9_84_96_02LG_F8<j'L_B3B_9EFl_84_08_FE:_F3E_12!
_BB_F3_B8_9D@_03_D1_C6_ED_D0_00K_B1_80_E2q_B6<j%L_B0#b_86_1A<_8DY _D2_CC)X;_91`_809_CFx_1C_D3$_C3_99^Z
w`_C6D_1DZ_08_F0_15_E58_CB_AD_03_1B_E11*_B3y_03_BD_1D_FA_C4}.B_EA_17f_17_16&_B1_91,_11z_89_C4_C3YY_CCN_90_1D_F2_AB_C0_F7)
_E6Q_1Ba&a_87_E2_B6_E34b!_C4_D7.3_F6R_1A_B1_11b_A87j_EA_C0Nx"_9DY_C8_A36_C2_94xh_07_FF_DA
_EE_A3_06_F7_D1JpY_17_91_D6v_91_D8g_B8_B4~_A2y<_BC_B0_12_AA_A4_CCG_94_18_DA_08PQ_1FT_B6_0El_84_D7_13r@_8E_05_8D_15_80_1C^X_08_F5_

4fRRe_80_9A_B8_95@_A5p_8D`_EA_88_95_10?_E1.h3_86_E7q_1B_81_0E(_9E_CE%_FF_FD,_91_01_FD_1F@;z_C3B_C8_A74_E0z_A3y_1A_B1_12b"
_13_04_08_81_8D_F0XD}_80_87_81_95_F0_F04Fj_B0_17._AC_84_DA'_C7_D4_CF_E66F.-_85_FB_81Q_B3_07_A3pa#T_EERI; _B6j_16_B5_12f_07?
_03_AE_03[_E1i_C9_E4_B6~_9B_E6_94_E3 _89_7Fm_04'd[_F8_D7_F9+_AEF_AF_ED_04_AC_BA_E4W_A1_8Fa_17.l_85_8A_A7_EEN_F0M_A1!
_1DN_D2_CCzb'_11}:_D0_90!_B4_10_E0Y_80_0B_D0_F8_D7Bp_E7_F4:_FDLZ_16_B3_12_A4_8F_87_10t`'<_16+_1E2_D1D_AD_84_19_D2_80"
F_0C_AD_04_18%_94_A0Q_94_1D_8F_19_BFc%hm_18_10_AC_89_D9_08_92_A13_84_7Fm_04_D7_E5>_8F"_E0o_8C_ _CF/l_84_CA_95K_B9,
_BC_C4v_FC_8E_8D_A0_85_B1_9CLh%@_A9_92_0E_FA_C3Y_CCF_90
_93J_E0K_1F_05_E0_1C^X_08_F57_AA_0F__EB_C0Bx3^_B0_F7X_DE_AA_F7_F6_AF_FF$!_C7_FDfY_CCF_90"
0_AB_82i_C4F_88l_AC_D7_88Lh#_C0>_A8K_04_A8C_0B_01^P_1E*_FC_EA_A5_EA_FE_F5_1F_9F_05`_83L_DC_B2_16_F6+_E63<_B1
[_BC_B2_16_EC_AF_A9X_1Fz=e=_1Eg_A8_C7n
[_0B_FFM_E2_F2_BC_A9_F5_85_B5P_CDv_8B_0C_AB_B9_B2_16_EC9gR2s_18_1AW_97|_91#_9F_F2_C8Z2~_E7_A1_CB D_B08_F2_9A_17y_18{|Q

+_89_D2__D8_B6_F5_C3_DA_17_D4_CC_AA_85_021fq_1B_81_FE_F5_7F_05_B9_14_C1__FF_D1|?_97_7F_FD_BF_D0_E5_F8_0E_95YOl$_82&_1E'
G_92_B6_8C_06_1C^_D9_08_16w&_A0_1F_94F_AC_84(MK_EA_D0J_80_03_B7_CB|_+_AF<n#P_1C!
(y_C3_04N_1C_16_AF_AC_04_1Bvh$_A4F_9AF_ED_84_89F_03X,_D4H_F3+_1B_C1_FA_A2G_AFugJc_96_824_DF_84_CFb6_82_C4_CF_B0_88_C2_AC_DC_D8+!
_07_E63_F1i_C4J_88_89_EA_A6_9F_B8B_9C_C3+k_C1_A6_AF_95_CC_EDTs_17_AC,_AF_CF_DDnQ>_96Om-
_B1_E9_12s_E1_C2Z_A8_17_89>X__B8_B0_11jD_B5_E7_89_81_8D_F0$'ohx_8D,_CF_A26_C2LYm+_93_13_F0_B6h_80vL_1A_B3_11$_84-
|_DB_1Aj_A6__B4_8F8_D0_06_CD_D4_FB6_12_D0_C7O*_EBU_A7<j%L_E6_E9v_D5_A1_95_00_B9_FAd_F6^"
_CA_FC_C2F_A8_03_BD_CBM_07_16_C2_BB_A4_BC_8Fz_C9_84V_02_BC_E2_D9V_9Ca_DCJ_A0_E1'
_B3_B6_94_C5l_04_D9_A5_A9_FE_C9b6_82_14_B8_EE_89_7F_AD_04w_CD_F4_AE_AB4b%
_C4_B0_83b_88_81_8D_F0_C0_BE_E0_1E5_A3_F5_A5hQ_CD_ED_C9_9B6BOB_AE_17g_D3_88_95_10_E55_BEM_CC_84_96_02_0CX_98_A9_F4_C2_95_A5`_CD

_B8-_92_D0_CB_BF_C9_F5_86_B6$_F5_84_D4_E0_A7?_B2_93_10_D1_A3_E4_C2_15J_BF)cxa_13X_A3_E3_98w_B8_91_C56_86g_FCCE%_17_A5F_1A_B1
_F7_F0_08_A3_C4_A1_82_BC_F0_FA_C3/_B9_95_1A_D3_EEZ _FF_B7_84_B5_98
[j_98_D0J_88_174_BE_A6_CA_ED2_BD_D6_BC_B2_12_AE~_CBG_1F_0C_F7_D1orO_BDm'_01_E0_1B_F5_12_05_90M_C4J_90_7F&_D7x.
H_07_8F_CBd_D6Yy_18%_8A_A8A_04_A4(v_A3J_A9_95_A7n_D4Rf^!]_AC_06>_E4_F4x_1C_F9t_F0$_14!{Z_CA_9A_A9D*__B4E_7F.
_A0_95|_B0_E3<F*_E4_03_8Ft_F4_A1_FBY_DC_FF_C4_A3_A6_0B_F8_160?i_0E_13>_00_9F_97_CB_B3l_F9&_1D!
_F3S_1ET_DA_9C_F9^_CC_D4_12_10_0E_BA_9B_8D_83
_FCY_90,+2k_E4X_B1_88D_8E_EFTI_E0(_A7V-_11_EE_99_DB_F5_89~FLG
[_86_C2_11_B1_C17_A5B_8DI_ECD4_1C_CAj_AD_BE_AC$M_91_C2Zm_151_FC_AC_FD_8F_BA_D7_B4s_87_1Dn_B7_B4_92_AE_C9K_1A_F1_A5#_83_AA_C9_BI

_C31_F4_D0_E9_1D_1A_06_85_A5s_99>_BDcW_9F_B6X07_BF_C1_ACO_0E3_DB_BB_D5_EA_FB_CB_1Fw_D2`_0F_83_19B_B9mF_99_859_8C@_EE_FE_8D_05

v_BC_80$_EAH_EA_B1f[_82_DEw_B5_A9[_9C_94_D5_E9o_AFX_CD;!_EFA_B7_FE_D3qt=_B8_1D_C5T_E2_B4_12_A5D_A8_F7(Q_1E_1Ae_E7_AD_FA_9A_D2"
_11_8D_03_9A_D1_D1R!_81_7F_0E_B4_92_13'_AD_00|_BE_B4V_B7_CB_DCkHTTP/1.1 200 OK
Date: Fri, 25 Nov 2022 20:43:58 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
X-Content-Type-Options: nosniff
Set-Cookie: ci_session=ubecjbhqf2ierbks4qgm3k66v16kutt6; expires=Fri, 25-Nov-2022 20:53:59 GMT; Max-Age=600; path=/; HttpOnly;HttpOnly;Secure;SameSite=Strict
Content-Length: 10560
Content-Type: text/html; charset=UTF-8

_1F_8B_08_00_00_00_00_00_00_03_ED}_DBv_DB_B6_D6_EE_FD_1A_E3_7F_07,
_B5_ABn_F7*u_F0_D9_89_AD_0E_C7I_9A_B4_F1_A1_B1_D3C_FE_F1_0F_88_84D_D8$_C1_80_A0de_EC_DB_FD$_FBj]
_EC_A7_E8_8B_ED9_01_92_A2_CE_92e_C7HS_B51@_12_87obNL_CC_89_03_F9__FF8_FC_E7_F3_F3_93_AB?.^_10__85A_F3_BF_FEq_88!
q_03_9A$G_95H8_D7I_85_044_EA_1EUXT_81_E7_04~_87>_A3^_16_D7_D7m_9A0_E2K_D69_AA_F8J_C5_C9_93Zmw_B7_BA}
P_DD_DC_D9_AC6_1A_07_B5J9u_C8_14%_AE_88_14_8B_D4Q_C5_F5_A9L_98:JU_C7_D9_1FI_A7_B8
X_F3_94_DE_F20_C9%S_8AG_DD_84|_F3_D5_FEf_A3_F1_94<g_1Ew_A9b_1E_F9_91_86_8C*_C9h_08)_0Ek&_E3x_8D_88_CCa_1FR_DE;_AA_9CP_D7g_CE
`_90"_A8_0C_C1_00_C1.>_FA_9E@,QBB,L_13_E5H_D6_A3_01_F7_A0_BA
_A9_CD-_FAB_D2nH_A7_94_B9(_E3_8B_DB_98K_96_94r_D6_A7e_89_80_D8_A3J_8F_B3~,_A4*_A5_EEsO_F9G_1E_EBq_979_FA_E2{_C2#_AE8_9C_C4_A5_01;
jTVdZ_96t_98_A9_C8_9C_B8_92_C7_8A_A8A_0C`_14_BBU_B5k_DA_A3_E6n_B9_16_FC_F5_A8$
W_AC_95_CA_80_1C_91Y_B5=_9D_CC_85_10W_CF_95_F8_A2_DFJ_8C_B8_B4b_11_A71_E4_DF_D8_98_96_92_B9_A9_E4j_D0_02_F6_B87_98_AA1-
_19_EFHh_F4_0C_C8_D4_82x_DC_A2_9E_87Ow_B7_AB[_07_D5_83_FDjcg_A4_AC_C3_9Ai_1Ch_9B_D2_CD_80G7D_B2_E0h_C3_8B_12'
_06f0_E5_FA_1B_86-_1BH2P_DC_01_0E'_D5_AE_10_DD_80_D1_98'UW_84_B5_8DQ_D1X_AA_A0_A4_DA_AF
_D9_CD_F2N_CD_9D_A8A_C0_12_9F1_B5A_B8_07_D7_A2_83_CD_E8h_0C_8E_9B$_1B$+s_06.H_F2C_07_FAa08:_8FY_F4_AF_CDg_974J_FE_B5wr!
_E2_98Cl_EBx_BB^_FF_D7_E6_C9_8E_FE_BB_AB_FF_EE_E9_BF_FB_F5_FA7__D5_B7_F6_9F&i_1B5B@_A1j_B8_AFC_07d_CC<_ED1y_D4_A8_D67_8C_F0mh_E

_AA
_E6_13_FC_D7_86_14_D5_88_A9Z_A3_DA_A8W_01_00_D6|_FD!er_A0S_99_14_9F_98_CB_E70_AC_04tp
_1A9_08_DA`_92_DE_B5_F2_BB_8C1hW_C6_DC_BDa_D2_0C5_A6K_95J/_9B
[_1Bc_E6_D6_06I_A4_BB_80_C2_EB_A2_85_AF_93_8Dfa_8B_A0i_97_99_F4_B5_CC_A6_CF._DB_C2_1B_E4^_C0_C8_88_F0O_C7!
_17@_A7_A0_1E_93`tS_A9_88_E3_8C_A58_F4x/_CF_9D04G_1C0S+P1<hN$/_15_F8"
_F2_92_C9_F2_C8+_86O_877_8FV_F9_8D_95_E7_EB_B2_B0_97T|_18_F7*_85_B3_A3_1C_B4R_1D_F3|_DC_88_D50_0C_B9g_B4_C7_BBz_D4_19-Y'

_83_DES_14H{ H_C4_04_8E_C7:4T~_99(_E0_F7_80_E4=_8E@a_E0(t_D2 >M_9C6uo_BAR_A4_917_0ED_D7Rj__B4_FF)
_8F_10_F1x_B21_DC_C7J_F2v_AA_D8_02_A6UA_95_92_0E_82_84_DCJD_D3_10_15_D9_D2`*_8C_EC7;
_A3_CE_1C_F0_F1*a_ACpD_C4_E6UY_E4_A6c_DDMH_E0#(_12c d_0E_81_B6R_C1J_A0_B2_0B&&_C8_F69_A6"
g_A2_7FX_A3_0Bj9_04cjQ_92_E9$_A8_BE_B8_13 _81_00_CBp>_05_E0_E9_04_9DJ_F3_A6_9B_84_C3Z_1A_CC_12_08_DDwg<C!_83_AE;
[_C4_E6_E43_C2iz_F8_CA_A2_99_F5_A6_E9}v$_93_91_DD_CCr_CC_04y_AC_14%_BA_E0_CAT_08_8EB_D9_05_F6_AF _A0qR_DC_CE_9A_FD_AB,
_0F_98_88_E9"_D6_1E_162_D1_A1_A4C_1D_1C^P_19_CE_E7_84_C18/IYZ@X_A6_8A _AA9_D0l H_A2 _97_87]}_83$_8AF_1E_95_9E_B9_CA
(_02_DBl_BA_D6_19_A9_1B9_97_E90_9Dy&_B7_86_8D_10v_F5H5c8_CC_87*_1E_D2._03;_08U1_96_EClW_AF_E3n_85_80_F5?i_D5_17$i_0C:
y_A2Gp4_EDks_9BwVOYJ_CEgH_EB_9C\&_08_CA_85!_DCg_D8_D0_04_ED_85_E4
{_D2_112_84_00Z_9C_08x$_F3_E9_1C|@_B4_08_02_99_CBu_85\Ps>_0E_05W_CB_C0r_E2
_FA_BB_D4)_F2_A2JQ_F0U}_95_F5_05tZ_BF_CA_E2"_C5N_B1Pl@="_1A_84_E1_00_87Cg_BF_BE]0_B1_B8K_86_CF_B1_BF:_C6_15)
_DD_15_EDkh_CC_FC_BE_9BJ m_E6_0C_F3gwZ1_C8Rk_ACD_AC_B1_B9D_DF_F9j_C4:0bUi_BE_82_9B(<K_8E_05_E3_C4_EE~rbw_97"_B6_F6_03M_95
/_E4Qc_82_E27`_9C&`_F5_B0~_B2_06_E1{_9F_9C_F0_BD_E5_B8_1CK_EE_C2_C5_04_D9_17_E6_FE_1A$_EF_7Fr_92_F7_97#_B9C?L_90_FB_92~_D0_13_EB
{O_D7_E0r_A3_F1_A9l_86_1A_97#_99Q_95_9A_D9_F51_BA_B3_07k_F0_F9_E0_93_F3_F9`_8Ch_ED`_8B0L#_AE_06_D3_CD_C5Q_B2_87_D6c;
_A0_D1M_A5y_92_E7^_83_F9_F5O_CE_FC_FAr_CC_D7._92_AB&x_7F_99_C6_B8_86_B2_04_C9_0B_EDb=_C6_D7_AAcC_EF_F4_81
{_9A_85qX_83_AC_D3\N_B46f_9B_19_C6mgr_DC_._D9(_E39_C6\Gh_DCJ_F3_1F_D3_9EdN_E5B_BB#_84_84_AD_DCl_01_0F_D7_81_DE_14_8B(_E1=F_A4_E8O)
a_C4_80W_D8Zi_18_81_E5_138l_E846u,_E8:_A2_D3_016:_C5_F5_FE_D4_07_A1_97_7_F2_EB_FD%
P_17_AE>_DAW8_A3_E2_B8_80_7F_96_17=_F6_9B_E3e_C8_E6_A1_BF_D9<v]_F0_DD_159_91L_F3_F8_B49_03_93_16_86_1922_A3_B2_7F,
_A4_CE_B4_FBl_98_E5_A4_AC_CB_13 _DC_E9K_1A_C739_BE_ECo_CC"_1D_E5h_A3`Ycs_C9z_CA_E5eC_B5C_A1UW_809_AD_08_ADJJl'
_02_1C_1Fq_EB_84<"
+_B6_00Ny_AC_DCd_A5y_82_1CR_EE_C3_1E_FA_DB_85_BB_B8_05_1A_EE_E2_F8_F5sr|rr_FE_EE_EC_EA_12_04i_BBy_98_C44*_D2_F4_B7_EBu_A2_E7:
Z_A6_88_96_0F_8DK_BE%_AF#_F4_EF_149v_15_EF_19_F5_F1_DDa_F3_1Au7[>_96@_DD_11B_AD-,+_D5M_F3_AA_DB
_88_E7_D2_18_81_A8_03nS_C8HL_B9_D7_A2_A6_DB_8DM_EA_ACN_A6n_9D_95sA_A6o_A2v_12?_D5_F9g+_89_E9U_AE"
E3_94_C6_9C_A4_8B_A7_9E_16_17y_F7_87_BA_07_EAyqP
_01_A3_F2 i_83_BB_FB4_9F_11_9E_9F_19t_EA_9C_81y_E9_96_98_05_C8_E3l_1C_D0_C1_13_12_89_88=-_8C_04-P_B9r,
_C6_B79_C3UY_B9A_BA_16^_E0T_EEp8t_D0S.
6_D1_94_B5_12_8DX@_F4__A7_1D_A4#_D3_9D_13_E9_F2Q_AB_D2_CC_94_029y_FB_E2_F8_EA_F5_F9_D9_B8a1_99_15_A7_F5'
f_B6K_A9_96_1A_FD_F2_DF_FCyih_A9lD!_04_95_DAf1*_D0_98+_1A_F0_8F_8Ct_FA_CE.(_AF_B0_EDl_D51_11_8E_92s&:
_C0jc_A8y_E4_D0_9E_ED_C7ng_CF_CCp_E8_A8_D3_D9_AD_EF;_F1_EE_CE_B6#6_87;_97_9Cw_97_15_E2qyT _D4_FCi_C2_12_05LJ!
[a_D2m_C1_CD\T_E7dE`C_F5(C_A7M_13_EE_928_95_AE_8F_1BYb_EA_DE_80_19_AB_E7|_1C_F0_B5_F9G_B4_B2_C0_18_0F_19_B8_DE@A,
_12eh_E9_C8_B0_95_C6] _EA_BCB_C0t_05_DD_AD_A7Z_CC_E6_9F_AC _87G_1D_E1_E8_E6X_85ms98B_90_BF_85,_D9Z_E4
t8_0B<0_C0
_D3J_B1_98_C4N_E0_00g_1D0_CB_EA_86&_BC_DDX_88t_89I_F2I_0B_16_DC_84_C41_9Dh_D8-_B3_C1_A0_85_AD_D4_D2_0B_CF_CBL_C1O_D6_A0_CB_DB]
6_EFx~_CDl_C9_89W)A_97_12_D06_0B_CA_94JT4_E6_A6A_B5Ui_9E_81D<_81_01_07o_AFZ_C1$_99_07_AB_82_D4_E5_F0(N_CB{_C1r9_C5_BF_15"
q_7F_9Bd_DEH_8Bd_E4_90_B4e_12_F5(_A8=_D0?s'm_A7V_BE_A0W_AE_9D_FE_13_F2_F2_C2_87_11_88_D8_CA_CD_18_D1-dg_96_EAo~_02?
__80k_1CX_CBO_86_E8_16_F23K_F57?_B7p_92,_EAp_18_E3_ED_E6_ABkP_B6_96_E0_AF_A5|_CD&?
_FEz_83_F5_B1_E7_817_90<_B6_E4_A0_B4_E0_1CJ&0_D4_A0Z_A8
_F2t`_14_E6%|"_A1_B1_93_9B&apos;\_1E_9B_953_95_00`[_C8P_93_E8_93_AB_00K_B9_89_CE_82|t_86_9A_FD_9F_85*_D7_98_1612ne
[b_E5_C6_B9_8F_DF_A1_88_F5_ECb.J_C7_9D_AEO#_8E_B3_8F_A0_F3_86_17_875_93_F0_11 _CE_82_FA_E7_FF
_F4n_17_13Z_08_F08hC_EBQhG_13_B1_12b_97I_03QGl_84_18_020_97F_E4_92_86_02_91_8E_DB_088_F2_84_94_88_D4D_AC_84_D8_15_81F_88_A1_9D_00S_

_84_11a_E6q;_81_F2nJ_F5V_B5gT_B6S_CF _1E_BFi#t_D9e_004B_C0y_D4J_98!3_AA_DED_AC_84_98_B65@_08l_84_97_E2
_A1@_B7a_1E_B5_15f_01_D2N_88_1F_99lS~_AD-_B8"n!_D0g_D4_A7!_05_A74_8B_D8 QR_1Ei_88_18_B1_12b_D4_A8_C7_12_1FQ_E6q+_81_82
(zB_F3_DB_C4l_04_C9_02*_F1_18o_16_B1_13b_97_A7_A1_86_88_11;!_F2_8FL#_84_D0J_80_91_EE_D5_18X O_86_DAH_CB"
6B_F4S=G`B_1B_01_8A_80_F7p_A4_CE"VB_8C(_97_D8OL_C4J_88 _98_B3_DAIx_C5_E4G_D6_15=m_8CO_BFo%_01*_E9S_03_D9_C4_AC_04_99_F6_98"
_AF_133_A35ri#\l?_F2_00p_EA_D0J_80_F1_C4'_AF#_8F_D3_88_9C_BB_0C_FE^1 _B7_85_1C _F0y_CF-&_E8W.
_BB<_CA$#_19_122z_DFJ_02_D2_88q_04_8C_A1_8D_00_D3_A0K_B5g_97_C7_AC_04)o@_CD_92_974_11_08txe'_D8_14_FA_97_C6_89_11_0B!
_9E_D0_B0-<dz_1E_B3_13$_93_02_CF_EE_E71_8B@_9A5/_86_AF_9B_CAb_1BC_DC_11_F5t_D3bh_11_E6!
_C0_98_91__99_F4_18_82_CC_E3V_02_1D_84_B4_A4_F5G_AFm_04_CC"_9C_C1#_C7_1D_B3T_F3_96_C5i;_E0.@_9F_F1_C4F"|
_B6_18_FE_B5_12_1C_0FPl1_B0_13_1E_9A_DC:_B0_12_9E_E4_89
iR_98_DC_E3wl_04-_91_90_FF_FE_991|_B1_C0_FF_94_D4_C1_F4_07V_92_10_88_B0_AD_C7_DB,f%_C8PH_A1_DBUG_AC_84(n_CA_FC_1F^Y
6Q_94_BC_D5_CB_A4_C3_B8_8D@_A5_A0J_0B_A7_89_D8_08Q_AF_E1_9D_D8_B9_84w_92J_EAR_81_F8t_C4F_88_83X_CF_EE_9B_D0F_80_1F_99_EB_97_ED_

_A9_BCA_EC:b#_C4k_DE_16_A9_02_F7:_8F_D9_08R_84<_D2_8A?_8FY_0C_B2_EC_A6L_DE_B3_10_F8_0B_9A(r_C5_C1H_A94_87q_1B_81_BA)
_F54J_13_B1_11bw_80o?_D7_81_8D_F0_02rI_83^_D6_8A_C3_0B_1B_A1~H_A9_12_92_83_93_FFc_CA#|_DD_C3_C4-_1BaK_AE_F4_BB)_B2_88_8D_10_13%
_F4&_B3,b#D_E5s_11k_8CY_CCB_90/ip_83_CE_D2_D0_83_1A_BFc%h)X_19q_E9_D2F_B8_FC_1AL_13_FCk%_B8_C8_CC_FAd_11_1B!
J_1A_B9_0C_10_EA_D0J_80,_02_CF_04_F4_B9^_1F_B9_B4_17_EE_85_08_06_11K_F8_10qq_C7^_D0_97`_DD_FBL_0EW_A89K

_FC_D3_1EZH_CA_8F_B4_8D+X:_B0_12_9E_99_964_A1_8D_00_99_90]_8D_D0D_AC_84
(C_1A_10_A2_8E_D8_08_D1_D7_CAJ_076_C2_C3_8Fk_04_8A_82_8D_Dm_84)_19_C3_B1_C9_84_96_02_CCF_F8"j'L_B3B_9EEl_84_08_FE:
_0BD_1A#_BB_8B_B8_9D@C_D1_C6_ED_D0_00K_B1_90_E2q_B6"j%L_B0#_12_86_1A<_8BY _D2_CC)X;_91`_809_CFx_92_D04_C7_99]Z
w`_C6D_1DZ_08_F0_15_E58_CB_AD_03_1B_E11*_F3y_03_BD_1D_FA_D4}."_1A_94f_17_16&_B1_91,_11y_A9_C4_C3Yy_CCN_90]_F2_B3_C0_F7)
_16Q_1Ba_A6Q_97_E2_B6_E3,b!_C4_D7.3_F6R_16_B1_11b_A47j_EA_C0Nx"_9BY(_A26_C2_94xh_07_FF_DA
_EE_83_06_F7_C1Jpy_17_91_D6v_91$`_B8_B4~_AAy<_BC_B0_12_AA_A4,@_94_18_DA_08P_D1_00T_B6_0El_84_D7_13r@N_04M_14_80_1C^X_08_F5'
_1AR_BD_07 _8BX 1_C6._A3_03_1B_E11_A9_DD2_13_DA_08PHO7_A0_0E-_04_F83_FDHo|_F3V_ABa_DCF_A0,
_1A@W_D1_81_8D_F0_B8_E4m_8A_FEX_1E_B3_11_A4HDO_00D_1D_DA_080_ED_837_0B_00uh#_C0_81_EC_0E>f_DD_A5_88
[_08_F4_C5_8D_DA_F8_D7JpJ_1F@7_A1_8D_00Y_1B?_0F_08M_C4J_88_89P_BE@_88:b#D_DE6_EF_D0_CB"vB_1C_18_80V_8E*o8s}
_C5_A2D1|+_C7_C8_A5_95p_95_9F_9A7;_16Q_1Ba_A6_B7,l_8BTv_01g_11_B7_10_E8_A995pj_E9_99_01_C0_C5<_B3_F1_AE_88Z _D3_A3]_9A_B8_B8z<_8C[
4_A0}_8E 1_B4_14_E0 1_FC61;Az_BC_87_1B_81_F2_98_9D _A3-e_B32<Vv2X&>_82_E1:_D2_F8_1D;A+_1E_F1_0F_F8_1D_ACa_DCJ_A0_A9_E4_8AfZ=_8F
[_0B_94_A7I_8E_93[yn_ED_94_0E_84R_9A_EB:b#Dv_CB]_B43th#@_EE_CA|i_18_B7_11_A8_08<_D1C_94&b%_C4_88jf_EB_D0N_80]_A1_w_9B_C7_EC_04
~_18_EBJ_D3_92Y_DCR_A0 _93_92*_03_D4_C4_AD_04*_85k_04SG_AC_84_F8_11wA_9B1_BC_88_DB_08t@_F1t.
_F9_EFg_A9_0C_E9_FF_00_DA_D1_1B_16B>_A3!_D7_1B_CD_B3_88_95_10S_99"@_08l_84_C7b_1A_00<_0C_AC_84_87_A712_83_BDta%_D4>9_A1A>_B71ri)
_DC_F7_8C_9A=_18_A5_0B_1B_A1r_97J_DAM_B1U_F3_A8_950_BB_F8_19p_1D_D8
OK&_B7_F5_DB4g_1C_07I_FCk#8!;"_B8)^q5zm'`_E5_93_9F_85>_86]_BA_B0_15*_9E_BA;_C57_85Ft8I3_EB_89_9DD_F4_E9@C_86_D0B_80_E7!.
@_E3__0B_C1]
_D0_9B_EC3iy_CCJ_90_01_1EB_D0_81_9D_F0X_A2x_C44D_13_B5_12fDC_8A_181_B4_12`_9CR_82FQ~<f_FC_8E_95_A0_B5a4@_B0&f#H_86_CE_10_FE_B5_11

_C09_BC_B0_10_EA/T_1F_BE_D6_81_85_F0f_BC`_EFsy_AB_DE_DB?_FF_93F_1C_F7_9B_E51_1BA_8A_D0_AC
f_11_1B!_A6_89^'#2_A1_8D_00_FB_A0._11_A0_0E-_04xIy_A4_F0_AB_97_CA_FF_F3?_01_0B_C1_06_99_B8e-_ECW,`xb_B7|e-
_D8_9F_B9R_89>_F4z_C6z<_C9Q_8F_DD_B6_16_FE_9B_D4_E5ES_EB_0Bk_A1_9A_ED_169Vse-_D8_0B_CE_A4d_E604_AE.
_05_A2@>_E5_91_B5d_FC_CA#_97A_88`q_E45/_F20_F6_F8_A2_14V_12_A5_BF_B0m_EB_87_B5/_A9_99U_8B_04b_CC_E36_02_FD_F3_FF
r%_C2?_FF_A3_F9~!_FF_FC_7F_91_CB_F1_1D*_B3_9E_D8H_04M=N_8E%m_1B8_BC_B2_11,_EEL@?(_8BX Q_9A_96_D4_A1_95_00_07_AE_CF_82@+_AF"
n#P_1C!(y_C3_04N_1C_96_AF_AC_04_1Bui,_A4F_9AE_ED_84_89F_03X,
_D2H_8B+_1B_C1_06_A2Gotg_CAb_96_824_DF_84_CFc6_82_C4_CF_B0_88_D2_AC_DC_D8+!_87_E63_F1Y_C4J_88_A9_F2_B3O\!
_CE_E1_95_B5`_B3_D7J_16v_AA_B9_0BV_96_D7_E7_AE__96_8F_E5S[Kl_B6_C4\_BA_B0_16_EAe_AA_0F_D6_97.l_84_1AS_EDyb`#<_C9_C9_1B_1A_DD
_CB_F3_A8_8D03V_DB_CA_E4_14_BC-_1A_A2_1D_93_C5l_04 a_1B_DF_B6_86_9A_E9'_ED#_0E_B4A3_F5_BE_8D_04_F4_F1_93_CAz_D5_A9_88Z
_93y_BA]uh%@_AE>_9A_BD_97_88_B2_B8_B0_11_EA@_EFr_D3_81_85_F0_AE(_EF_A3^2_A1_95_00_AFy_BE_15g_18_B7_12h_F4_D1_AC-_E51_1BA_FA4_D3?
y_CCF_90_02_D7=_F1_AF_95_E0n_98_DEu_95E_AC_84_18uQ_0C1_B0_11_1E_D8_17_DC_A3f_B4_BE_12m_AA_B9=y_D3F_E8i_C4_F5_E2l_16_B1_12_A2_BC_C

_0F_08^R_9FJ_C4<rm!_E0?X_88s_BD:_B0_10_DE_FB_EC_DB}_EFm_FDv_DF{_1E_B6i_BB_0Ffi_1E{$_90_87_B5_84_05_CCU+V
{X_F3xo_85<y_FA_15r@_06_E2_064l_8E*_1D!C_A7+E_1AWV_C5_19_D06_0B_F2r_11))_02'_BB
_B1$t_B6*Mm_FC_D5_C8_85_14=_DC_9B_F9_E4_B0_A6S_ACZW qV_F6_C1_AAxu9_86#_04_D7_D3_8E*"n%_08_AFB$_FB_90r _B6j_B9U2_92H_9E,
_B9K_8D_EB_FE
_E9._E4_FB8h3_89_AF_D2_CB"6u_C1_02_E43|uZ_E2_93_13_11_A4F__8C_DF_B1_12_F6)_05_97E_B4_F5
[_EAL_CCJ_98x_D0_F4_99L_A3_A4_CF_DD_1B_F3z_8E_E2_D2V_C0_1D_91F^_F1M_AE7_B4-_A9'_A4_06?_FD_91_9D_84_88_1E%
_97_AEP_FAM_19_C3_0B_9B_C0_1A_1D_C7_BC_A3_8D<_B61<_E3_1F)*_B9_A84_B3_88M_B8_87G_18%
_0E_15_E4_85_D7_1F~_C9_AD_D2_9Cv_D7J_F8_BF_A4_AC_CD_DCJ_D3_84VB_BC_A4_C9U_AE_CF_F4Zs_F9_CAJ_B8_FA-_1F}
0_DCG_BF_C9=_F5_B6_9D_04_80o_D4K_15@6_11+A_FE_91_DE_E0_B9 _1D|^&_B3_CE_CA_A38UDb E_B1[U_C9_AC<u_AB_962_F3J_E9_125_08
_A7_C7_938_A0_83'_91_88_D8_D3J_DEL_15R_FB_A2-
_FA_0B_01_AD_14_80_1D_E71R#_EFy_AC_A3_8Fm_D8_CF_E2_FEG_1E_B7_C0_B7_80_F9ik_98_F0_11_F8_BC_9Ee_CB7_E9_08_99_9F_F2_B0_D6_E1,
_F0_12_A6_96_80p_E8o5_0Fk_F0gA_B2_BC_C8_BC_91_13_C5b_12;_81S'_A1_A3_9CF_BDB_B8gnoN_F43b:_DA2_14_8E_88_BE)_15jL_13'
_A6_D1PV_1B_9B_CBJ_D2_14)l4V_11_C3O_DA_FF_A8{C_BB_F7_D8_E1_F6*+_E9_9A_A2_A4_11_:
6_A8Z_DC_9B_DF_D3_0C_FF_D3_B8U_CA_F0Hn_B5_E6_11_D1_8DxT_B9_E2L_92_95x_FE_18_BF_FBAW_0C_FD_1EU_D4_89_91!
_8D_EDJve_D8y|_FA_9C_BC_A5_1E_83To_7F'_DB_FB_F5_DA_CE~_9D_EC_FF_F8_8C|_FB_86G_E9-n_00P_DF_15_BArk_B7_D2\._0B_F9_96|]
_AFn_ED_C0_D0_E1_93_EF,_B0_83_96_F9=_B3_EF_8F6_FB_15_18_B3P=y_BBn_83Df_F7_B0_E16_EB_F5j_BDnU_D3i_18_BA'=_B2-;
_D9_9B_97V_FF_8F_F5{8_B1_DA_19_15_AB_B3__?_7F}L~|_F1_F2_FC_ED_C9_0B_F2_E3_D5_EF_A4Q_DF_AB_C3p_0C=tz_87_86Aa_E9_A6O_EF_DA_D5_A7-
_16_CC_AD/W07'_87_99_9D_BDz_FD_F7_AB_EFw_B3`_1F_83_19B_B9cF_99_859_8C@_EE_FD_85_05_F2_0E_E6_DA_A7]
_8D_BA_F7_B4e_07_CF_E7_1E_9E_87_C9_EDKv_CB_F1]_96_DD_C2_A6t_83$_F7_FF&_9E_A1_81_BA_92_87w'
ojn_D2_FB_F7_A5_B6f_FAR_F3i_B3_C1_D3Z_C9_DF?_FC_A7_E3,_9BvY_1C4`R_11_FD_D7_89%_0F_A9_1C_10_D7m_F5%_8Dc&g_CD_06_81
/_C3_B2_BC_8F_A1_CE_FF_17y}zq_FE_F6_EA_F8_EC_EA _D9_02FD sS_C5{_8Ct(_0F_C0_F9_A2J_B10V _E9_F3 _00_9F,
I_03ExD_A8_EB_8A_14_B8_98_A4I_CC_A2_04_14c_95_9C_A4_89_12!_0CMz_FF4_B8n_1C_B8_8C_D3_EC<B_E7_8Dj=_1EB"_D2fP_9E_F2_A1_1C<_89_CCn)
x_80 _F44B=_0F_EAH_AA_9Fz_C2_10;_A7_E3X_EB_AB_0FB_EC1W_A0_B6_EE_CFa_DFY_7F_E9;6_C0Z_A8O_17L_8D_95_93_1A_CDzGq_CF_ED_81_FB6
/_A2_F3_B5w_0E_8F_95_0C_88_F5W+.tx_BFe_BB_BAs_B4_B0sT_9AYO9_81_8B{_A6@_8AP_98_E9_C8_E6_05_C6_F5_1C_EB_1Au|_16{Q_86T
/P_BEkt_A1_BB_F7x]_D2R_BD_FE_05_0C_93_92_0C_F9v_C7_9E?_0E}_9D_DE_AF_CB_9A5G^_92_B6_05_AA`_C8 _AD_08_EE<S_AE_E1_AC([w_C9_B3_9E<.

4_02,_97_C33_1C_97E_C7_8C_E4_BE_08<&m_17E_84_DA_12QK_BF_FA`_D1_92_CDhb_EB_85Q_E7_F9_C4"P_1A_A1tk_DB_C2_FF_11cD_F3q
K$_E3_B8N_B9_86_C9=6_D6_FE_CA_13_DC_1C_0E_7F_EFa_A2`_AC_ECS_8A_9B_8DO_B4_B10_8C_AFk+_AC_B1H_FE_D7_16s_AD_E8_A24l_DB_AC_E8_F4_F

K_1AK_E6=_10_1E_E7*kcDem<_88_CA_FA&j'_F1_D3G_D6X_B3F7-c_AD_A5TX9_A9_D9_93
-_E72_B3_D9_F1_A8r_9C_95Q_AC_CB_AD_BAw_FDn_1BNWm_89_D1_DF*_87_A7_D6_ABi_D9_FA_86u_ADp_08jn_C2_B5_8F@_CF>m?_FC{$H_92_86x,
_A8_D5_0E_04_BEpm_F5_B3N_E53FI_EA_BA,I_CCnj_C7_A3_83$_DF_EBC|_8E;_FE_CF_84b_E4 Q>_BE[5;
_AD_A3_0F_F1_D0T_89P_BFo7_08_06x_14G1_19_F2_88_E2[_B6_F1T_0E_18_01_80|t;=_96_DFr_A1_13@_83_E3_D3&_C1;
_84w_A0_95H_C4_FA_A4_93F_1E_D4#_F5_11_1E
(hx_BE_87*_02_A0_B8_F0_AA_AB_1D_D5+_D1_9D7_1A_B7_EE_B0_9Fi_DA|_F5_CA&_1CHYq_BC_E9u_D4_11K_C8_DD<_1C_9Fj_E3_F6_FD_BA wz_A9_8E.
_AB,Q_C8M_B3_DB:_17_A6_BF_B7_A0_16G_BD|P:_D62-
_F6_F5_D7_9B_FF_E6_DA_F8Q_9D_90_F2_C0Z_AE1D_F77_D7&_1Dns_D6_D4Z_BEega_1F_85s_AB_D64_E5_B7_BA_B9_BB_FC;_CCt_AE{_1A_D6_B37a}
_16_A3_FAN_F1_E2_AE{_16_DB_95[_AE(K_8B_ED_E8
(a_10~_0E_1AG_B3_DF_1C_AE~_CE_14_A8_C9_CFB_00_D6>>_0E_FB~_84`T_064_C8G_92_81_BB30m_19_7F_E7^_E7_7F_C7+)I_C9_9DO_C1/'
*_FA_F0_F0_9A~_C08_FAu_85E_977)0_BA_D9_D7_F4
t_D1_8F_B0_1C_B5R_9E_11i_CB^_04_F0_D7_10_B7_FB=)
<N_C6_C3_C8_DD_C8_E9_DF_CFG_F2t_BE_C7_E0_F1=_1E_05_1E_A7_E1_01_19l_0E_FB_FE_CD_DD%_B9{?'`_C7_A9x
_FE_E6GW_FFf_EFB_F6_DE_FB!_D6qJ_1E_8A_C5_1AmKo_07_FE_9B_CD_8B{_F1_FA_FBO_C6_B1?_0Cc_B3_DD%_8F_CB_D2Ok_F2e_8B_8C_7F_83o_AD-
+_D3_90?_8C_98ek_C0_9F_8F_E6XW_C8_14_BD_FD_8BH_D8_15_BD%_DFNr_14 _8CKc_FEw_C4z!_04_C8_9F_91_04_EA|_8F_C1_F0_C3v_F3J_E0_97A
_DD_D2nZ_CFZ_04_FC_D7_D72_0F_F6R_DEI_06-_FF*_D8_F1_02_D2_B8+_A9_C7Z_1D
z_DF_D5_A6nyRV_A7_BF_BBb5_EF_84|_00_DD_FAO_C7_D1_F5_E0v_14S_89_D3N_95_12_91_DE_A3Dyd_94_9D_B7_EAkJ_CBD4_0FiNG
[E_04_FE9_D0JN_92_B6C_F0_F9_B2Z]_9F_B97"

Missing header: Permissions-Policy — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	150248
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-05-31 16:57:02.0

THREAT:

The Permissions-Policy response header is not present.

IMPACT:

Permissions-Policy allows web developers to selectively enable, disable, or modify the behavior of some of the browser features and APIs within their application.

A user agent has a set of supported features(Policy Controlled Features), which is the set of features which it allows to be controlled through policies.

Not defining policy for unused and risky policy controlled features may leave application vulnerable.

SOLUTION:

It is recommended to define policy for policy controlled features to make application more secure.

References:

Permissions-Policy W3C Working Draft

Policy Controlled Features

RESULT:
Permissions-Policy: Header missing
Response headers on link: GET https://order.maximumsettings.com/ response code: 200
Date: Fri, 25 Nov 2022 19:25:20 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Set-Cookie: ci_session=6t7ju6kdld0hqba8ddr2p0am2q2a1ok0; expires=Fri, 25-Nov-2022 19:35:20 GMT; Max-Age=600; path=/; HttpOnly;HttpOnly;Secure; SameSite=Strict
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://order.maximumsettings.com/ response code: 200
GET https://order.maximumsettings.com/assets/css/all.css response code: 200
GET https://order.maximumsettings.com/indexd784.html?feed=rss2 response code: 404
GET https://order.maximumsettings.com/indexa6da.html?feed=comments-rss2 response code: 404
GET https://order.maximumsettings.com/assets/css/style.css response code: 200
GET https://order.maximumsettings.com/assets/css/custom.css response code: 200
GET https://order.maximumsettings.com/assets/css/bootstrap.min.css response code: 200
GET https://order.maximumsettings.com/assets/css/sweetalert2.min.css response code: 200
GET https://order.maximumsettings.com/assets/css/select2.min.css response code: 200
GET https://order.maximumsettings.com/assets/css/bootsnav.css response code: 200
GET https://order.maximumsettings.com/assets/css/OverlayScrollbars.css response code: 200
GET https://order.maximumsettings.com/assets/css/datepicker.css response code: 200
GET https://order.maximumsettings.com/assets/js/jquery.js response code: 200
GET https://order.maximumsettings.com/assets/js/bootstrap.min.js response code: 200
GET https://order.maximumsettings.com/assets/js/datatables/datatables.min.js response code: 200
GET https://order.maximumsettings.com/assets/js/bootstrap-datepicker.js response code: 200
GET https://order.maximumsettings.com/assets/js/jquery.steps.js response code: 200
GET https://order.maximumsettings.com/assets/js/jquery.validate.js response code: 200
GET https://order.maximumsettings.com/assets/js/sweetalert2.min.js response code: 200
GET https://order.maximumsettings.com/assets/js/form.min.js response code: 200
GET https://order.maximumsettings.com/assets/js/bootsnav.js response code: 200
GET https://order.maximumsettings.com/assets/js/order.js?t=638116a089bcb response code: 200
GET https://order.maximumsettings.com/assets/js/trial.js?t=638116a089bd3 response code: 200
GET https://order.maximumsettings.com/assets/js/select2.min.js response code: 200
GET https://order.maximumsettings.com/assets/js/jquery.overlayScrollbars.js response code: 200
GET https://order.maximumsettings.com/js/bootstrap-datetimepicker.js response code: 404
GET https://order.maximumsettings.com/assets/js/order.js?t=638116a0f18f8 response code: 200
GET https://order.maximumsettings.com/assets/js/trial.js?t=638116a0f1900 response code: 200

Host Uptime Based on TCP TimeStamp Option

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2007-05-29 18:56:36.0

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Based on TCP timestamps obtained via port 443, the host's uptime is 37 days, 2 hours, and 48 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-11-15 18:49:15.0

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

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

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

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

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

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

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

RESULT:

Operating System Technique ID
Ubuntu/Linux TCP/IP Fingerprint U7254:
443

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:	2017-04-24 10:47:04.0

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

IMPACT:
N/A

SOLUTION:
N/A

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

PII Fields Found — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	150375
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-02-03 22:15:06.0

THREAT:
Personally Identifiable Information(PII) is found on the form(s) on the Web Application.

IMPACT:
Improper handling of the PII can lead to loss of reputation for the organization and the individuals whose personal information is stored. Attackers can use this information for more focused attacks in the future.

SOLUTION:
Please review all the PII fields below in the report and if required, PII should be obtained by lawful and fair means.

RESULT:
Parent URI: https://orders.maximumsettings.com/

PII fields Found:
Address
Credit Card Number
Credit Card Type
Credit Card Expiry Month
City
Country
Email
Phone
State/Province
Zip Code

PII Fields Found — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	150375
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-02-03 22:15:06.0

THREAT:
Personally Identifiable Information(PII) is found on the form(s) on the Web Application.

IMPACT:
Improper handling of the PII can lead to loss of reputation for the organization and the individuals whose personal information is stored. Attackers can use this information for more focused attacks in the future.

SOLUTION:
Please review all the PII fields below in the report and if required, PII should be obtained by lawful and fair means.

RESULT:
Parent URI: https://order.maximumsettings.com/

PII fields Found:
Address
Credit Card Number
Credit Card Type
Credit Card Expiry Month
City
Country
Email
Phone
State/Province
Zip Code

Missing header: Permissions-Policy — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	150248
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-05-31 16:57:02.0

THREAT:
The Permissions-Policy response header is not present.

IMPACT:

Permissions-Policy allows web developers to selectively enable, disable, or modify the behavior of some of the browser features and APIs within their application.

A user agent has a set of supported features(Policy Controlled Features), which is the set of features which it allows to be controlled through policies.

Not defining policy for unused and risky policy controlled features may leave application vulnerable.

SOLUTION:

It is recommended to define policy for policy controlled features to make application more secure.

References:

Permissions-Policy W3C Working Draft

Policy Controlled Features

RESULT:

Permissions-Policy: Header missing

Response headers on link: GET https://orders.maximumsettings.com/ response code: 200

Date: Fri, 25 Nov 2022 19:25:57 GMT

Server: Apache

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

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

Pragma: no-cache

Vary: Accept-Encoding

X-Content-Type-Options: nosniff

Set-Cookie: ci_session=aevqoh5bev8av1l56nl2anurkemkg72k; expires=Fri, 25-Nov-2022 19:35:58 GMT; Max-Age=600; path=/; HttpOnly;HttpOnly;Secure; SameSite=Strict

Transfer-Encoding: chunked

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

Header missing on the following link(s):

(Only first 50 such pages are listed)

GET https://orders.maximumsettings.com/ response code: 200

GET https://orders.maximumsettings.com/assets/css/all.css response code: 200

GET https://orders.maximumsettings.com/indexd784.html?feed=rss2 response code: 404

GET https://orders.maximumsettings.com/indexa6da.html?feed=comments-rss2 response code: 404

GET https://orders.maximumsettings.com/assets/css/style.css response code: 200

GET https://orders.maximumsettings.com/assets/css/custom.css response code: 200

GET https://orders.maximumsettings.com/assets/css/bootstrap.min.css response code: 200

GET https://orders.maximumsettings.com/assets/css/sweetalert2.min.css response code: 200

GET https://orders.maximumsettings.com/assets/css/select2.min.css response code: 200

GET https://orders.maximumsettings.com/assets/css/bootsnav.css response code: 200

GET https://orders.maximumsettings.com/assets/css/OverlayScrollbars.css response code: 200

GET https://orders.maximumsettings.com/assets/css/datepicker.css response code: 200

GET https://orders.maximumsettings.com/assets/js/jquery.js response code: 200

GET https://orders.maximumsettings.com/assets/js/bootstrap.min.js response code: 200

GET https://orders.maximumsettings.com/assets/js/datatables/datatables.min.js response code: 200

GET https://orders.maximumsettings.com/assets/js/bootstrap-datepicker.js response code: 200

GET https://orders.maximumsettings.com/assets/js/jquery.steps.js response code: 200

GET https://orders.maximumsettings.com/assets/js/jquery.validate.js response code: 200

GET https://orders.maximumsettings.com/assets/js/sweetalert2.min.js response code: 200

GET https://orders.maximumsettings.com/assets/js/form.min.js response code: 200

GET https://orders.maximumsettings.com/assets/js/bootsnav.js response code: 200

GET https://orders.maximumsettings.com/assets/js/order.js?t=638116c596227 response code: 200

GET https://orders.maximumsettings.com/assets/js/trial.js?t=638116c59622f response code: 200

GET https://orders.maximumsettings.com/assets/js/select2.min.js response code: 200

GET https://orders.maximumsettings.com/assets/js/jquery.overlayScrollbars.js response code: 200

GET https://orders.maximumsettings.com/js/bootstrap-datetimepicker.js response code: 404
GET https://orders.maximumsettings.com/assets/js/order.js?t=638116c6097bb response code: 200
GET https://orders.maximumsettings.com/assets/js/trial.js?t=638116c6097c2 response code: 200

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:	2017-04-24 10:47:04.0

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

IMPACT:
N/A

SOLUTION:
N/A

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

First Link Crawled Response Code Information — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150546
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-10-05 18:04:13.0

THREAT:
The Web server returned the following information from where the Web application scanning engine initiated. Information reported includes First Link Crawled, response Code, response Header, and response Body (first 500 characters). The first link crawled is the "Web Application URL (or Swagger file URL)" set in the Web Application profile.

IMPACT:
An erroneous response might be indicative of a problem in the Web server, or the scan configuration.

SOLUTION:
Review the information to check if this is in line with the expected scan configuration. Refer to the output of QIDs 150009, 150019, 150021, 150042 and 150528 (if present) for additional details.

RESULT:
Base URI: https://order.maximumsettings.com/
Response Code: 200
Response Header:
Date: Fri, 25 Nov 2022 19:25:20 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Set-Cookie: ci_session=6t7ju6kdld0hqba8ddr2p0am2q2a1ok0; expires=Fri, 25-Nov-2022 19:35:20 GMT; Max-Age=600; path=/; HttpOnly;HttpOnly;Secure; SameSite=Strict
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

Response Body:

<!DOCTYPE html>
<html class="no-js" lang="en">
<head>
<base href="https://order.maximumsettings.com/">
<meta content="charset=utf-8">
<title>Maximum Settings – Dedicated Game Streaming</title>
<meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<meta name="viewport" content="width=device-width, initial
...

External Links Discovered — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150010

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

THREAT:

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

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 18
https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css
https://www.paypal.com/sdk/js?client-id=AXCYoBHG6D0aLrR8_-C8M5J6CT1rvQPPb7H16kP0h994jDOGITw1ufMaqLNZiCTmEkwFWSBPXoDBHzeN&currency=CAD
https://www.paypal.com/sdk/js?client-id=AdxTCDDviKQ4NfGkev7ZHmb6dpcARIMXdWiLdkFWAYpwUnNmWbs6HIFQYla0yrYi227svx1cN4J3HkBF&currency=USD
https://www.paypalobjects.com/api/checkout.js
https://cdn.datatables.net/1.10.19/css/jquery.dataTables.min.css
https://code.highcharts.com/highcharts.js
https://code.highcharts.com/modules/export-data.js
https://code.highcharts.com/modules/exporting.js
https://code.highcharts.com/modules/series-label.js
https://community.maximumsettings.com/
https://discord.gg/A9jp5Cn
https://canvasjs.com/assets/script/jquery-1.11.1.min.js
https://canvasjs.com/assets/script/jquery.canvasjs.min.js
https://login.maximumsettings.com/
http://fonts.googleapis.com/
http://maximumsettings.com/
http://maximumsettings.com/?author=1
http://s.w.org/

SSL Server Information Retrieval — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

THREAT:

The following is a list of supported SSL ciphers.

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

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

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

SSLv2 PROTOCOL IS DISABLED
SSLv3 PROTOCOL IS DISABLED
TLSv1 PROTOCOL IS DISABLED
TLSv1.1 PROTOCOL IS DISABLED
TLSv1.2 PROTOCOL IS ENABLED
TLSv1.2 COMPRESSION METHOD None
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
CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM
DHE-RSA-CAMELLIA128-SHA DH RSA SHA1 Camellia(128) MEDIUM
DHE-RSA-AES128-SHA256 DH RSA SHA256 AES(128) MEDIUM
DHE-RSA-AES256-SHA256 DH RSA SHA256 AES(256) HIGH
CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH
DHE-RSA-CAMELLIA256-SHA DH RSA SHA1 Camellia(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
CAMELLIA128-SHA256 RSA RSA SHA256 Camellia(128) MEDIUM
DHE-RSA-CAMELLIA128-SHA256 DH RSA SHA256 Camellia(128) MEDIUM
CAMELLIA256-SHA256 RSA RSA SHA256 Camellia(256) HIGH
DHE-RSA-CAMELLIA256-SHA256 DH RSA SHA256 Camellia(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
ARIA128-GCM-SHA256 RSA RSA AEAD ARIAGCM(128) MEDIUM
ARIA256-GCM-SHA384 RSA RSA AEAD ARIAGCM(256) HIGH
DHE-RSA-ARIA128-GCM-SHA256 DH RSA AEAD ARIAGCM(128) MEDIUM
DHE-RSA-ARIA256-GCM-SHA384 DH RSA AEAD ARIAGCM(256) HIGH
ECDHE-RSA-ARIA128-GCM-SHA256 ECDH RSA AEAD ARIAGCM(128) MEDIUM
ECDHE-RSA-ARIA256-GCM-SHA384 ECDH RSA AEAD ARIAGCM(256) HIGH
ECDHE-RSA-CAMELLIA128-SHA256 ECDH RSA SHA256 Camellia(128) MEDIUM
ECDHE-RSA-CAMELLIA256-SHA384 ECDH RSA SHA384 Camellia(256) HIGH
AES128-CCM RSA RSA AEAD AESCCM(128) MEDIUM
AES256-CCM RSA RSA AEAD AESCCM(256) HIGH
DHE-RSA-AES128-CCM DH RSA AEAD AESCCM(128) MEDIUM
DHE-RSA-AES256-CCM DH RSA AEAD AESCCM(256) HIGH

AES128-CCM-8 RSA RSA AEAD AESCCM8(128) MEDIUM
AES256-CCM-8 RSA RSA AEAD AESCCM8(256) HIGH
DHE-RSA-AES128-CCM-8 DH RSA AEAD AESCCM8(128) MEDIUM
DHE-RSA-AES256-CCM-8 DH RSA AEAD AESCCM8(256) HIGH
ECDHE-RSA-CHACHA20-POLY1305 ECDH RSA AEAD CHACHA20/POLY1305(256) HIGH
DHE-RSA-CHACHA20-POLY1305 DH RSA AEAD CHACHA20/POLY1305(256) HIGH
AES128-SHA256 RSA RSA SHA256 AES(128) MEDIUM
AES256-SHA256 RSA RSA SHA256 AES(256) HIGH
TLSv1.3 PROTOCOL IS ENABLED
TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM
TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH
TLS13-CHACHA20-POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256) HIGH

Secure Sockets Layer (SSL) Certificate Transparency Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Source Validated Name URL ID Time
Certificate #0 CN=*.maximumsettings.com
Certificate yes Comodo 'Mammoth' CT log mammoth.ct.comodo.com/ 6f5376ac31f03119d89900a45115ff77151c11d902c10029068db2089a37d913 Sun 04 Sep 2022 07:52:47 PM GMT
Certificate yes Google 'Xenon2022' log ct.googleapis.com/logs/xenon2022/ 46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47 Sun 04 Sep 2022 07:52:47 PM GMT

Certificate #0 CN=*.maximumsettings.com
Certificate yes Comodo 'Mammoth' CT log mammoth.ct.comodo.com/ 6f5376ac31f03119d89900a45115ff77151c11d902c10029068db2089a37d913 Sun 04 Sep 2022 07:52:47 PM GMT
Certificate yes Google 'Xenon2022' log ct.googleapis.com/logs/xenon2022/ 46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47 Sun 04 Sep 2022 07:52:47 PM GMT

Default Web Page (Follow HTTP Redirection) — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

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

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:

nas-201911-01

RESULT:
GET / HTTP/1.0
Host: order.maximumsettings.com

<!DOCTYPE html>
<html class="no-js" lang="en">
<head>
<base href="https://order.maximumsettings.com/">
<meta content="charset=utf-8">
<title>Maximum Settings – Dedicated Game Streaming</title>
<meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />

<meta name="viewport" content="width=device-width, initial-scale=1">
<base href="https://order.maximumsettings.com/">
<script type="text/javascript">
var site_url = "https://order.maximumsettings.com/";
var base_url = "https://order.maximumsettings.com/";
var show_setting_popup = '';
var security_check = '1';
var iframe_url = '';
var ip_add = '64.39.98.151';
</script>

<link rel='dns-prefetch' href='http://fonts.googleapis.com/' />
<link rel='dns-prefetch' href='http://s.w.org/' />

<link rel='stylesheet' id='softing-fonts-css' href='//fonts.googleapis.com/css?family=Open%2BSans%7CPoppins%3A400%2C500%2C600%2C700%2C800&subset=latin%2Clatin-ext&ver=1.0' type='text/css' media='all' />
<link rel="stylesheet" href="https://order.maximumsettings.com/assets/css/all.css" integrity="sha384-50oBUHEmvpQ+1lW4y57PTFmhCaXp0ML5d60M1M7uH2+nqUivzIebhndOJK28anvf" crossorigin="anonymous">

<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
<link rel="alternate" type="application/rss+xml" title="Maximum Settings » Feed" href="indexd784.html?feed=rss2" />
<link rel="alternate" type="application/rss+xml" title="Maximum Settings » Comments Feed" href="indexa6da.html?feed=comments-rss2" />
<link rel='stylesheet' id='wp-block-library-css' href='https://order.maximumsettings.com/assets/css/style.css' type='text/css' media='all' />
<link rel='stylesheet' id='wp-block-library-css' href='https://order.maximumsettings.com/assets/css/custom.css' type='text/css' media='all' />

<link rel='stylesheet' id='wp-block-library-css' href='https://order.maximumsettings.com/assets/css/bootstrap.min.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://order.maximumsettings.com/assets/css/sweetalert2.min.css' type='text/css'/>
<link rel='stylesheet' href='https://order.maximumsettings.com/assets/css/select2.min.css' type='text/css'/>
<link rel='stylesheet' id='bootsnav-css' href='https://order.maximumsettings.com/assets/css/bootsnav.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://cdn.datatables.net/1.10.19/css/jquery.dataTables.min.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://order.maximumsettings.com/assets/css/OverlayScrollbars.css' type='text/css' media='all' />
<link rel="stylesheet" href="https://order.maximumsettings.com/assets/css/datepicker.css" />

<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/jquery.js'></script>

</head>

<body class="">
<!-- Preloader Start -->
<!--<div class="se-pre-con"></div>-->
<!-- Preloader Ends -->
<!-- Header
== -->
<header id="home" class="nt-site-header">
<!-- Start Navigation -->
<nav class="navbar navbar-default navbar-sticky bootsnav on no-full has-background">
 <!-- Start Atribute Navigation -->


```
<li class="attr-nav-li-one">
<a href="https://orders.maximumsettings.com" target="">Order Now</a>
</li>
<li class="attr-nav-li-two">
<a href="https://login.maximumsettings.com" target="_self">Login</a>
</li>
</ul>
</div>
<!-- End Atribute Navigation -->

<!-- Start Header Navigation -->
<div class="navbar-header">
<button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#navbar-menu">
<i class="fa fa-bars"></i>
</button>
<a href="http://maximumsettings.com" id="nt-logo" class="img-logo standard-logo navbar-brand">
<!-- sticky logo -->
<img src="https://order.maximumsettings.com//assets/images/site-logo-4.jpg" alt="Maximum Settings" class="logo logo-scrolled" />
</a>
</div>
<!-- End Header Navigation -->

<!-- Collect the nav links, forms, and other content for toggling -->
<div class="collapse navbar-collapse" id="navbar-menu">
<ul class="nav navbar-nav navbar-right" data-in="#" data-out="#">
<li id="menu-item-804" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-804"><a href="
http://maximumsettings.com#home" class="scroll">Home</a></li>
<li id="menu-item-806" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-806"><a href="
http://maximumsettings.com/?author=1" class="scroll">Latest News</a></li>
<li id="menu-item-807" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-807"><a href="
http://maximumsettings.com#pricing" class="scroll">Pricing</a></li>
<li id="menu-item-808" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-808"><a href="
http://maximumsettings.com#faq" class="scroll">Faq&#8217;s</a></li>
<li id="menu-item-811" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-811"><a href="
http://maximumsettings.com#features" class="scroll">Features</a></li>
<li id="menu-item-809" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-809"><a href="
https://community.maximumsettings.com" class="scroll" target="_blank">Community</a></li>
<li id="menu-item-810" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-810"><a href="
http://maximumsettings.com#contact" class="scroll">Support</a></li>
</ul>
</div><!-- /.navbar-collapse -->
</div>
</nav>
<!-- End Navigation -->

</header>
<!-- End Header -->

<div class="content">
<div class="container">
<div class="main_content ult-responsive row">
<div class="nt-column col-sm-12 col-lg-offset-2 col-lg-8 col-lg-offset-2 col-md-offset-1 col-md-8">
<div class="site-heading text-center">
<br><h2>Account Creation</h2>
</div>
</div>
```

```
<div class="row">

<div class="register-wrapper">
<div class="col-sm-12 col-lg-12 col-md-12">
<div class="pricing-area">
<div class="pricing-item text-center or-box-min ">
<ul>
<li class="pricing-header"><h4 class="f30">PAID ACCOUNTS</h4><span class="fw400 order_header_h2"> ( Instant Activation )</span></li>

<li class="footer">
<a class="btn circle btn-theme paid_account">Order Now</a>
</li>
<li> </li>
</ul>
</div>
</div>

</div>


<div style="clear: both;"></div>
<br>
</div>
<div style="display: none;" class="paid_register_content nt-column col-sm-12 col-lg-12 col-md-12 nt_col-has-responsive-data">
<div class="panel panel-blue">
<div class="panel-heading">ACCOUNT CREATION</div>
<div class="panel-body">
<div class="">
<div class="nt-wrapper "><h2 class="capitalize fw-600 mb-30 "></h2>
<div role="form" class="wpcf7" id="wpcf7-f608-p654-o2" lang="en-US" dir="ltr">
<div class="error_msg_div"></div>
<form class="form-basic purchase_package form-horizontal" method="post" id="frm_upgrade" action="#" name="package-info-form">
<h3></h3>
<fieldset class="step p-l-0 m-t-10" id="step1">
<div class="content cus-panel col-sm-12 account_info_block">
<div class="col-sm-6">
<div class="form-group">
<label class="control-label col-sm-3">Name:</label>
<div class="col-sm-9">
<input type="text" name="name" required class="form-control u_name" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Phone :</label>
<div class="col-sm-9">
<input type="text" name="phone" required class="form-control u_phone" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Email :</label>
<div class="col-sm-9">
<input type="text" name="email" required class="form-control u_email" value="" />
</div>
</div>
```

```
<div class="form-group">
<label class="control-label col-sm-3">Confirm Email :</label>
<div class="col-sm-9">
<input type="text" name="confirm_email" required class="form-control" value="" />
</div>
</div>
</div>
<div class="col-sm-6">
<div class="form-group">
<label class="control-label col-sm-3">Address:</label>
<div class="col-sm-9">
<textarea name="address" required class="form-control u_address"></textarea>
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3">City:</label>
<div class="col-sm-9">
<input type="text" name="city" required class="form-control u_city" value="" />
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3">Country:</label>
<div class="col-sm-9">
<select name="country" required class="form-control up_country_op">
<option value="Afghanistan">Afghanistan</option>
<option value="land">land</option>
<option value="Albania">Albania</option>
<option value="Algeria">Algeria</option>
<option value="American Samoa">American Samoa</option>
<option value="Andorra">Andorra</option>
<option value="Angola">Angola</option>
<option value="Anguilla">Anguilla</option>
<option value="Antarctica">Antarctica</option>
<option value="Antigua and Barbuda">Antigua and Barbuda</option>
<option value="Argentina">Argentina</option>
<option value="Armenia">Armenia</option>
<option value="Aruba">Aruba</option>
<option value="Australia">Australia</option>
<option value="Austria">Austria</option>
<option value="Azerbaijan">Azerbaijan</option>
<option value="Bahamas">Bahamas</option>
<option value="Bahrain">Bahrain</option>
<option value="Bangladesh">Bangladesh</option>
<option value="Barbados">Barbados</option>
<option value="Belarus">Belarus</option>
<option value="Belgium">Belgium</option>
<option value="Belize">Belize</option>
<option value="Benin">Benin</option>
<option value="Bermuda">Bermuda</option>
<option value="Bhutan">Bhutan</option>
<option value="Bolivia">Bolivia</option>
<option value="Bonaire">Bonaire</option>
<option value="Bosnia and Herzegovina">Bosnia and Herzegovina</option>
<option value="Botswana">Botswana</option>
```

<option value="Bouvet Island">Bouvet Island</option>
<option value="Brazil">Brazil</option>
<option value="British Indian Ocean Territory">British Indian Ocean Territory</option>
<option value="British Virgin Islands">British Virgin Islands</option>
<option value="Brunei">Brunei</option>
<option value="Bulgaria">Bulgaria</option>
<option value="Burkina Faso">Burkina Faso</option>
<option value="Burundi">Burundi</option>
<option value="Cambodia">Cambodia</option>
<option value="Cameroon">Cameroon</option>
<option selected='selected' value="Canada">Canada</option>
<option value="Cape Verde">Cape Verde</option>
<option value="Cayman Islands">Cayman Islands</option>
<option value="Central African Republic">Central African Republic</option>
<option value="Chad">Chad</option>
<option value="Chile">Chile</option>
<option value="China">China</option>
<option value="Christmas Island">Christmas Island</option>
<option value="Cocos [Keeling] Islands">Cocos [Keeling] Islands</option>
<option value="Colombia">Colombia</option>
<option value="Comoros">Comoros</option>
<option value="Cook Islands">Cook Islands</option>
<option value="Costa Rica">Costa Rica</option>
<option value="Croatia">Croatia</option>
<option value="Cuba">Cuba</option>
<option value="Curacao">Curacao</option>
<option value="Cyprus">Cyprus</option>
<option value="Czech Republic">Czech Republic</option>
<option value="Democratic Republic of the Congo">Democratic Republic of the Congo</option>
<option value="Denmark">Denmark</option>
<option value="Djibouti">Djibouti</option>
<option value="Dominica">Dominica</option>
<option value="Dominican Republic">Dominican Republic</option>
<option value="East Timor">East Timor</option>
<option value="Ecuador">Ecuador</option>
<option value="Egypt">Egypt</option>
<option value="El Salvador">El Salvador</option>
<option value="Equatorial Guinea">Equatorial Guinea</option>
<option value="Eritrea">Eritrea</option>
<option value="Estonia">Estonia</option>
<option value="Ethiopia">Ethiopia</option>
<option value="Falkland Islands">Falkland Islands</option>
<option value="Faroe Islands">Faroe Islands</option>
<option value="Fiji">Fiji</option>
<option value="Finland">Finland</option>
<option value="France">France</option>
<option value="French Guiana">French Guiana</option>
<option value="French Polynesia">French Polynesia</option>
<option value="French Southern Territories">French Southern Territories</option>
<option value="Gabon">Gabon</option>
<option value="Gambia">Gambia</option>
<option value="Georgia">Georgia</option>
<option value="Germany">Germany</option>
<option value="Ghana">Ghana</option>
<option value="Gibraltar">Gibraltar</option>
<option value="Greece">Greece</option>

<option value="Greenland">Greenland</option>
<option value="Grenada">Grenada</option>
<option value="Guadeloupe">Guadeloupe</option>
<option value="Guam">Guam</option>
<option value="Guatemala">Guatemala</option>
<option value="Guernsey">Guernsey</option>
<option value="Guinea">Guinea</option>
<option value="Guinea-Bissau">Guinea-Bissau</option>
<option value="Guyana">Guyana</option>
<option value="Haiti">Haiti</option>
<option value="Heard Island and McDonald Islands">Heard Island and McDonald Islands</option>
<option value="Honduras">Honduras</option>
<option value="Hong Kong">Hong Kong</option>
<option value="Hungary">Hungary</option>
<option value="Iceland">Iceland</option>
<option value="India">India</option>
<option value="Indonesia">Indonesia</option>
<option value="Iran">Iran</option>
<option value="Iraq">Iraq</option>
<option value="Ireland">Ireland</option>
<option value="Isle of Man">Isle of Man</option>
<option value="Israel">Israel</option>
<option value="Italy">Italy</option>
<option value="Ivory Coast">Ivory Coast</option>
<option value="Jamaica">Jamaica</option>
<option value="Japan">Japan</option>
<option value="Jersey">Jersey</option>
<option value="Jordan">Jordan</option>
<option value="Kazakhstan">Kazakhstan</option>
<option value="Kenya">Kenya</option>
<option value="Kiribati">Kiribati</option>
<option value="Kosovo">Kosovo</option>
<option value="Kuwait">Kuwait</option>
<option value="Kyrgyzstan">Kyrgyzstan</option>
<option value="Laos">Laos</option>
<option value="Latvia">Latvia</option>
<option value="Lebanon">Lebanon</option>
<option value="Lesotho">Lesotho</option>
<option value="Liberia">Liberia</option>
<option value="Libya">Libya</option>
<option value="Liechtenstein">Liechtenstein</option>
<option value="Lithuania">Lithuania</option>
<option value="Luxembourg">Luxembourg</option>
<option value="Macao">Macao</option>
<option value="Macedonia">Macedonia</option>
<option value="Madagascar">Madagascar</option>
<option value="Malawi">Malawi</option>
<option value="Malaysia">Malaysia</option>
<option value="Maldives">Maldives</option>
<option value="Mali">Mali</option>
<option value="Malta">Malta</option>
<option value="Marshall Islands">Marshall Islands</option>
<option value="Martinique">Martinique</option>
<option value="Mauritania">Mauritania</option>
<option value="Mauritius">Mauritius</option>
<option value="Mayotte">Mayotte</option>

<option value="Mexico">Mexico</option>
<option value="Micronesia">Micronesia</option>
<option value="Moldova">Moldova</option>
<option value="Monaco">Monaco</option>
<option value="Mongolia">Mongolia</option>
<option value="Montenegro">Montenegro</option>
<option value="Montserrat">Montserrat</option>
<option value="Morocco">Morocco</option>
<option value="Mozambique">Mozambique</option>
<option value="Myanmar [Burma]">Myanmar [Burma]</option>
<option value="Namibia">Namibia</option>
<option value="Nauru">Nauru</option>
<option value="Nepal">Nepal</option>
<option value="Netherlands">Netherlands</option>
<option value="New Caledonia">New Caledonia</option>
<option value="New Zealand">New Zealand</option>
<option value="Nicaragua">Nicaragua</option>
<option value="Niger">Niger</option>
<option value="Nigeria">Nigeria</option>
<option value="Niue">Niue</option>
<option value="Norfolk Island">Norfolk Island</option>
<option value="North Korea">North Korea</option>
<option value="Northern Mariana Islands">Northern Mariana Islands</option>
<option value="Norway">Norway</option>
<option value="Oman">Oman</option>
<option value="Pakistan">Pakistan</option>
<option value="Palau">Palau</option>
<option value="Palestine">Palestine</option>
<option value="Panama">Panama</option>
<option value="Papua New Guinea">Papua New Guinea</option>
<option value="Paraguay">Paraguay</option>
<option value="Peru">Peru</option>
<option value="Philippines">Philippines</option>
<option value="Pitcairn Islands">Pitcairn Islands</option>
<option value="Poland">Poland</option>
<option value="Portugal">Portugal</option>
<option value="Puerto Rico">Puerto Rico</option>
<option value="Qatar">Qatar</option>
<option value="Republic of the Congo">Republic of the Congo</option>
<option value="Runion">Runion</option>
<option value="Romania">Romania</option>
<option value="Russia">Russia</option>
<option value="Rwanda">Rwanda</option>
<option value="Saint Barthlemy">Saint Barthlemy</option>
<option value="Saint Helena">Saint Helena</option>
<option value="Saint Kitts and Nevis">Saint Kitts and Nevis</option>
<option value="Saint Lucia">Saint Lucia</option>
<option value="Saint Martin">Saint Martin</option>
<option value="Saint Pierre and Miquelon">Saint Pierre and Miquelon</option>
<option value="Saint Vincent and the Grenadines">Saint Vincent and the Grenadines</option>
<option value="Samoa">Samoa</option>
<option value="San Marino">San Marino</option>
<option value="So Tom and Prncipe">So Tom and Prncipe</option>
<option value="Saudi Arabia">Saudi Arabia</option>
<option value="Senegal">Senegal</option>
<option value="Serbia">Serbia</option>

<option value="Seychelles">Seychelles</option>
<option value="Sierra Leone">Sierra Leone</option>
<option value="Singapore">Singapore</option>
<option value="Sint Maarten">Sint Maarten</option>
<option value="Slovakia">Slovakia</option>
<option value="Slovenia">Slovenia</option>
<option value="Solomon Islands">Solomon Islands</option>
<option value="Somalia">Somalia</option>
<option value="South Africa">South Africa</option>
<option value="South Georgia and the South Sandwich Islands">South Georgia and the South Sandwich Islands</option>
<option value="South Korea">South Korea</option>
<option value="South Sudan">South Sudan</option>
<option value="Spain">Spain</option>
<option value="Sri Lanka">Sri Lanka</option>
<option value="Sudan">Sudan</option>
<option value="Suriname">Suriname</option>
<option value="Svalbard and Jan Mayen">Svalbard and Jan Mayen</option>
<option value="Swaziland">Swaziland</option>
<option value="Sweden">Sweden</option>
<option value="Switzerland">Switzerland</option>
<option value="Syria">Syria</option>
<option value="Taiwan">Taiwan</option>
<option value="Tajikistan">Tajikistan</option>
<option value="Tanzania">Tanzania</option>
<option value="Thailand">Thailand</option>
<option value="Togo">Togo</option>
<option value="Tokelau">Tokelau</option>
<option value="Tonga">Tonga</option>
<option value="Trinidad and Tobago">Trinidad and Tobago</option>
<option value="Tunisia">Tunisia</option>
<option value="Turkey">Turkey</option>
<option value="Turkmenistan">Turkmenistan</option>
<option value="Turks and Caicos Islands">Turks and Caicos Islands</option>
<option value="Tuvalu">Tuvalu</option>
<option value="U.S. Minor Outlying Islands">U.S. Minor Outlying Islands</option>
<option value="U.S. Virgin Islands">U.S. Virgin Islands</option>
<option value="Uganda">Uganda</option>
<option value="Ukraine">Ukraine</option>
<option value="United Arab Emirates">United Arab Emirates</option>
<option value="United Kingdom">United Kingdom</option>
<option value="United States">United States</option>
<option value="Uruguay">Uruguay</option>
<option value="USA">USA</option>
<option value="USA / Canada">USA / Canada</option>
<option value="Uzbekistan">Uzbekistan</option>
<option value="Vanuatu">Vanuatu</option>
<option value="Vatican City">Vatican City</option>
<option value="Venezuela">Venezuela</option>
<option value="Vietnam">Vietnam</option>
<option value="Wallis and Futuna">Wallis and Futuna</option>
<option value="Western Sahara">Western Sahara</option>
<option value="Yemen">Yemen</option>
<option value="Zambia">Zambia</option>
<option value="Zimbabwe">Zimbabwe</option>
</select>

```
</div>

<div class="form-group">
<label class="control-label col-sm-3">State/ Province:</label>
<div class="col-sm-9">
<select name="op_state" required class="form-control op_states">
<option value="Alberta">Alberta</option>
<option value="British Columbia">British Columbia</option>
<option value="Manitoba">Manitoba</option>
<option value="New Brunswick">New Brunswick</option>
<option value="Newfoundland and Labrador">Newfoundland and Labrador</option>
<option value="Nova Scotia">Nova Scotia</option>
<option selected=&apos;selected&apos; value="Ontario">Ontario</option>
<option value="Prince Edward Island">Prince Edward Island</option>
<option value="Quebec">Quebec</option>
<option value="Saskatchewan">Saskatchewan</option>
<option value="Northwest Territories">Northwest Territories</option>
<option value="Nunavut">Nunavut</option>
<option value="Yukon">Yukon</option>
</select>
<input type="text" name="txt_state" required class="form-control txt_state" style="display:none;" value="" />
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3">Postal Code / Zip Code:</label>
<div class="col-sm-9">
<input type="text" name="zip_code" required class="form-control u_zip_code" value="" />
</div>
</div>


</div>
</div>
</fieldset>


<h3></h3>
<fieldset class="step p-l-0 m-t-10" id="step2" style="display: none;">
<div class="content cus-panel col-sm-12">
<div class="col-sm-11">
<div class="form-group">
<label class="control-label col-sm-3">Package:</label>
<div class="col-sm-7">

<select name="package_id" required class="form-control" id="up_package_id">
<optgroup label="Tier 1">

<option data-pid="14" data-pname="AMD Radeon RX 480/580 8GB (Linux Mint)" value="36">AMD Radeon RX 480/580 8GB (Linux Mint) ( $0.35 / h )</option>

<option data-pid="18" data-pname="Test111" value="41">Test111 ( $200.00 / h )</option>
</optgroup>
<optgroup label="Tier 2">

<option data-pid="15" data-pname="NVIDIA GEFORCE GTX 1070-1080 (Linux Mint)" value="37">NVIDIA GEFORCE GTX 1070-1080 (Linux Mint) ( $0.65 / h )</option>
</optgroup>
```

<optgroup label="Tier 3">

<option data-pid="12" data-pname="AMD 5700XT,6700XT,6800XT (Linux Mint)" value="35">AMD 5700XT,6700XT,6800XT (Linux Mint) ($0.75 / h)</option>
</optgroup>

</select>

<input type="hidden" class="existing_package_cls" name="existing_package_id" value="" />

</fieldset>

<h3></h3>
<fieldset class="step p-l-0 m-t-10" id="step3" style="display: none;">

<!--
* IMPORTANT: 3 consecutive failed attempts will result in account suspension. Customer and Credit card information must be within the exact same address.
-->

<label class="control-label col-sm-3">Payment Type:</label>

<select name="payment_type" required class="form-control payment_type_cls" >
<option value="">Select One</option>
<option value="paypal">Paypal</option>
<option value="credit_card">Credit Card</option>
<option value="promo_code">Promo Code</option>
</select>

<label class="control-label col-sm-3">Enter Promo Code:</label>

<input type="text" name="promo_code" required class="form-control promo_code_cls" value="" />

<label class="control-label col-sm-3">Name of card holder:</label>

<input type="text" name="card_on_name" required class="form-control u_card_on_name" value="" />

<label class="control-label col-sm-3">Credit Card type:</label>

<select name="card_type" required class="form-control u_card_type">
<option value="Visa">Visa</option>
<option value="MasterCard">MasterCard</option>
</select>

```
</div>
<div class="form-group">
<label class="control-label col-sm-3">Credit card number:</label>
<div class="col-sm-5">
<input type="text" id="u_ccnumber" name="ccnumber" maxlength="16" required class="form-control u_ccnumber" value="" />
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3" >Expiration month /year:</label>
<div class="col-sm-5">
<div class="controls cc-ym-wrapper">
<div class="col-sm-6 p-l-0">
<select name="ccmonth" required class="form-control u_ccmonth">
<option value="">Month </option>
<option value="1">1</option>
<option value="2">2</option>
<option value="3">3</option>
<option value="4">4</option>
<option value="5">5</option>
<option value="6">6</option>
<option value="7">7</option>
<option value="8">8</option>
<option value="9">9</option>
<option value="10">10</option>
<option value="11">11</option>
<option value="12">12</option>

</select>
</div>
<div class="col-sm-6 p-r-0">
<select name="ccyear" required class="form-control u_ccyear col-sm-4">
<option value="">Year</option>
<option value="2022">2022</option>
<option value="2023">2023</option>
<option value="2024">2024</option>
<option value="2025">2025</option>
<option value="2026">2026</option>
<option value="2027">2027</option>
<option value="2028">2028</option>
<option value="2029">2029</option>
<option value="2030">2030</option>
<option value="2031">2031</option>
<option value="2032">2032</option>
<option value="2033">2033</option>
</select>
</div>

</div>
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3">CVC code:</label>
<div class="col-sm-5">
<input type="text" name="ccvc" required class="form-control u_ccvc" value="" />
```

```
</div>
</div>

</div>
<div class="form-group amt_wrapper" style="display:none;">
<label class="control-label col-sm-3">Amount:</label>
<div class="col-sm-5">
<select name="amount" required class="form-control cc_amount_opt">
<option value="20">$20</option>
<option value="30">$30</option>
<option value="50">$50</option>
<option value="other">Other ( Min $5 )</option>
</select>
</div>

</div>

<div class="form-group r_amount_div" style=&apos;display:none;&apos;>
<label class="control-label col-sm-3"> </label>
<div class="col-sm-5">
<input type="text" name="other_amount" required class="form-control other_amount_cls" placeholder="Amount" value="5" >
</div>
</div>
</div>
</div>
</fieldset>
<h3></h3>
<fieldset class="step p-l-0" id="step4" style="display: none;">
<div class="content cus-panel col-sm-12 summary_block">
<div class="alert alert-success promo-days-wrapper hide">Note : this account will automatically be terminated with <span class="promo_days_cnt"></span> days if no new funds are added within that period. </div>
<div class="summary_up_wrapper">
<div class="col-sm-6">
<h3>Customer Info</h3>
<div class="form-group">
<label class="control-label col-sm-3">Name:</label>
<div class="col-sm-9">
<span class="summ_name"></span>
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Phone:</label>
<div class="col-sm-9">
<span class="summ_phone"></span>
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Email:</label>
<div class="col-sm-9">
<span class="summ_email"></span>
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Address:</label>
<div class="col-sm-9">
<span class="summ_address"></span>
```

```
</div>
</div>
</div>


<div class="col-sm-6">
<h3>Package Info</h3>
<div class="form-group">
<label class="control-label col-sm-5">Packages:</label>
<div class="col-sm-6">
<span class="summ_package"></span>
</div>
</div>
<h3>Payment Detail</h3>
<div class="form-group">
<label class="control-label col-sm-5">Payment Type:</label>
<div class="col-sm-6">
<span class="summ_payment"></span>
</div>
</div>

<div class="u_promo_wrapper" style="display:none;">
<div class="form-group" >
<label class="control-label col-sm-5">Promo Name:</label>
<div class="col-sm-6">
<span class="summ_promo_name"></span>
</div>
</div>
</div>
<div class="u_credit_wrapper" style="display:none;">
<div class="form-group" >
<label class="control-label col-sm-5">Name of card holder:</label>
<div class="col-sm-6">
<span class="summ_card_on_name"></span>
</div>
</div>
<div class="form-group" >
<label class="control-label col-sm-5">Credit Card type:</label>
<div class="col-sm-6">
<span class="summ_card_type"></span>
</div>
</div>
<div class="form-group" >
<label class="control-label col-sm-5">Credit card number:</label>
<div class="col-sm-6">
<span class="summ_ccnumber"></span>
</div>
</div>
<div class="form-group" >
<label class="control-label col-sm-5">Expiration month /year:</label>
<div class="col-sm-6">
<span class="summ_ccmonth_year"></span>
</div>
</div>
<div class="form-group" >
<label class="control-label col-sm-5">CVC code:</label>
```

```
<div class="col-sm-6">
<span class="summ_u_ccvc"></span>
</div>
</div>

</div>
<div class="amount_wrapper" style="display:none;">
<div class="form-group" >
<label class="control-label col-sm-5">Amount:</label>
<div class="col-sm-6">
<span class="summ_amount"></span>
</div>
</div>
</div>
<div class="tax_wrapper" style="display:none;">
<div class="form-group" >
<label class="control-label col-sm-5">Tax (<span class="summ_tax_per"></span>) :</label>
<div class="col-sm-6">
<span class="summ_tax"></span>
</div>
</div>
<div class="form-group" >
<label class="control-label col-sm-5"><b>Total Amount:</b></label>
<div class="col-sm-6">
<span class="summ_total_amount"></span>
</div>
</div>
</div>
</div>
</div>
<div class="col-sm-12">
<div class="upgrade_frm_action form-group">
<div class="paypal_wrapper" style="display:none;">
<!--<div id="paypal-button-container"></div>-->
<div><a class="btn btn-frm-submit paypal-checkout" href=&apos;javascript:void(0)&apos;> <img style="height: 38px;margin-top: -10px;" src="https://order.
maximumsettings.com/assets/images/paypal.png" /> </a></div>
<div><a href="javascript:void(0);" onclick="location.reload();" class="btn btn-default btn-cancel">Cancel</a></div>
</div>
<div class="cc_pay_wrapper" style="display:none;">
<div><button type="submit" id="upgrade_btn" class="btn btn-theme btn-frm-submit">Pay Now</button></div>
<div><a href="javascript:void(0);" onclick="location.reload();" class="btn btn-default btn-cancel">Cancel</a></div>
</div>
<div class="promo_wrapper" style="display:none;">
<div><button type="submit" id="promo_btn" class="btn btn-theme btn-frm-submit">Place Order</button></div>
<div><a href="javascript:void(0);" onclick="location.reload();" class="btn btn-default btn-cancel">Cancel</a></div>
</div>
</div>
</div>
</fieldset>
</form>
</div>
</div>
</div>
</div>
</div>
</div> </div>
```

```
</div>
<div class="nt-column col-sm-12 col-lg-12 col-md-12">
<div class="nt-column-inner">
<div class="nt-wrapper ">
<h2 class="nt_ch_1541650940591 poppins capitalize fw-300 mb-5 vc_custom_heading">Need Help ?</h2>
</div>
</div>
</div>
<div class="nt-column col-sm-12 col-lg-offset-2 col-lg-8 col-md-offset-2 col-md-8">
<div class="nt-column-inner">
<div class="nt-wrapper ">
<div class="site-heading text-center sec_title_1541352243086">
<h2>Join Us On Discord</h2>
<p>
<a href="https://discord.gg/A9jp5Cn"><img class="discord_logo" src="https://order.maximumsettings.com//assets/images/discord-logo.jpg"/></a>
</p>
</div>
</div>
</div>
</div>



</div>

</div>

<div class="modal fade" id="not_available_modal" tabindex="-1" role="dialog" aria-labelledby="not_available_modal_label" aria-hidden="true" data-backdrop="static" data-keyboard="false">
<div class="modal-dialog" role="document">
<div class="modal-content">
<div class="modal-header">
<h5 class="modal-title text-center blue_background" id="otp_modal_label">PAID ACCOUNTS</h5>
</div>
<div class="modal-body">
<div class="modal-body-content">
<center><h2>Not Yet Available. <br>Please try again later.</h2></center>
</div>
</div>
<div class="modal-footer">
<button type="button" class="btn btn-secondary close_button" data-dismiss="modal">Close</button>
</div>
</div>
</div>
</div> <div class="modal fade" id="otp_modal" tabindex="-1" role="dialog" aria-labelledby="otp_modal_label" aria-hidden="true" data-backdrop="static" data-keyboard="false">
<div class="modal-dialog" role="document">
<div class="modal-content">
<div class="modal-header">
<h5 class="modal-title text-center blue_background" id="otp_modal_label">Code Sent via SMS</h5>
<button type="button" class="close close_button" data-dismiss="modal" aria-label="Close" onClick=&apos;location.reload();&apos;>
<span aria-hidden="true">&times;</span>
</button>
</div>
<div class="modal-body">
<div class="modal-body-content">
<div class="row">
```

<input type="hidden" id="verification_step" value="1">

<label>Enter Code : </label>

<input type="text" name="otp" id="otp_input_val" value='' size="40" class="form-control" placeholder="Enter the code" maxlength="6">

<!-- Not Received? Click here -->

<!--<button type="button" class="btn btn-secondary close_button" data-dismiss="modal" onClick='location.reload();'>Close</button>-->
<button type="button" class="btn btn-secondary close_button" data-dismiss="modal">Close</button>
<input type="button" name='sub' id='otp_submit' value="Next" class="submit-btn btn btn-primary">

<h3 class="modal-title">Trial Accounts</h3>

<h4>IMPORTANT</h4>

Dear Potential Customer,
This trial service is only available in the United States and Canada. Furthermore, you will require a physical address to obtain a trial activation code. We will be sending a valid code through your local post office such as Canada Post/ Fedex / DHL/ etc. Only accounts with valid phone numbers are valid. Services like Text NOW or similar voip services will be rejected and address details automatically banned.

<h4>Note: Trial activation code will <u>NOT</u> be sent by Email.</h4>

Paid accounts can be started for as little as $5 and are available in most parts of the world. If you are not located within Canada and the United states, you can still use Maximumsettings via the regular paid process. If you wish to continue with a Trial activation please click continue otherwise, you can click " Paid Account Please " and get started within just a few minutes.
<u>Limited Time Offer:</u>
Paid accounts will automatically get an additional $35 credit with any purchase
Thank you
Maximum Settings.

<button type="button" class="btn circle btn-theme btn-sm paid_account">Paid Account Please</button>
<button type="button" class="btn circle btn-theme border btn-sm continue_trial">Continue To Trial</button>

<footer class="bg-light">

 Copyright 2022. All Rights Reserved by Maximum Settings

<li id="menu-item-511" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-511">Terms of user
<li id="menu-item-512" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-512">License
<li id="menu-item-513" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-513">Support

</footer>
<script src="https://canvasjs.com/assets/script/jquery-1.11.1.min.js"></script>
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/bootstrap.min.js'></script>

<script type="text/javascript" src="https://order.maximumsettings.com/assets/js/datatables/datatables.min.js"></script>

<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/bootstrap-datepicker.js'></script>

<script type='text/javascript' src="https://order.maximumsettings.com/assets/js/jquery.steps.js"></script>
<script type='text/javascript' src="https://order.maximumsettings.com/assets/js/jquery.validate.js"></script>
<script type='text/javascript' src="https://order.maximumsettings.com/assets/js/sweetalert2.min.js"></script>
<script type='text/javascript' src="https://order.maximumsettings.com/assets/js/form.min.js"></script>

<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/bootsnav.js'></script>
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/order.js?t=63811d3253f4e'></script>
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/trial.js?t=63811d3253f57'></script>

<script src="https://canvasjs.com/assets/script/jquery.canvasjs.min.js"></script>
<script src="https://code.highcharts.com/highcharts.js"></script>
<script src="https://code.highcharts.com/modules/series-label.js"></script>
<script src="https://code.highcharts.com/modules/exporting.js"></script>
<script src="https://code.highcharts.com/modules/export-data.js"></script>
<script src="https://canvasjs.com/assets/script/jquery.canvasjs.min.js"></script>

<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/select2.min.js'></script>
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/jquery.overlayScrollbars.js'></script>
<!--<script type='text/javascript' src='js/bootstrap-datetimepicker.js'></script>-->
<!--<script src="https://www.paypal.com/sdk/js?client-
id=AdxTCDDviKQ4NfGkev7ZHmb6dpcARIMXdWiLdkFWAYpwUnNmWbs6HIFQYla0yrYi227svx1cN4J3HkBF&currency=USD"></script>-->

<script src="//www.paypalobjects.com/api/checkout.js"></script>
<script src="https://www.paypal.com/sdk/js?client-id=AXCYoBHG6D0aLrR8_-
C8M5J6CT1rvQPPb7H16kP0h994jDOGITw1ufMaqLNZiCTmEkwFWSBPXoDBHzeN&currency=CAD" data-namespace="paypal_sdk"></script>

<script>var env = 'production';</script> <!-- // sandbox | production -->
<script>var client_sandbox = 'AXCYoBHG6D0aLrR8_-C8M5J6CT1rvQPPb7H16kP0h994jDOGITw1ufMaqLNZiCTmEkwFWSBPXoDBHzeN';</script>
<script>var client_production = 'AbVx2eNpll12ZAblvXX9lzPUhkceBr43Z2j3pl280MyQ_THe9FZomXD9lbmEQ8LtWqcN2ObbZPaoJx1d';</script>
<script>var canada_quebec_rate = '14.795';</script>
<script>var canada_wide_rate = '13';</script>

</body>
</html>
GET / HTTP/1.0
Host: orders.maximumsettings.com

<!DOCTYPE html>
<html class="no-js" lang="en">
<head>
<base href="https://orders.maximumsettings.com/">
<meta content="charset=utf-8">
<title>Maximum Settings – Dedicated Game Streaming</title>
<meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<meta name="viewport" content="width=device-width, initial-scale=1">
<base href="https://orders.maximumsettings.com/">
<script type="text/javascript">
var site_url = "https://orders.maximumsettings.com/";
var base_url = "https://orders.maximumsettings.com/";
var show_setting_popup = '';
var security_check = '1';
var iframe_url = '';
var ip_add = '64.39.98.151';
</script>

<link rel='dns-prefetch' href='http://fonts.googleapis.com/' />
<link rel='dns-prefetch' href='http://s.w.org/' />

<link rel='stylesheet' id='softing-fonts-css' href='//fonts.googleapis.com/css?family=Open%2BSans%7CPoppins%3A400%2C500%2C600%2C700%2C800&subset=latin%2Clatin-ext&ver=1.0' type='text/css' media='all' />
<link rel="stylesheet" href="https://orders.maximumsettings.com/assets/css/all.css" integrity="sha384-50oBUHEmvpQ+1lW4y57PTFmhCaXp0ML5d60M1M7uH2+nqUivzIebhndOJK28anvf" crossorigin="anonymous">

<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
<link rel="alternate" type="application/rss+xml" title="Maximum Settings » Feed" href="indexd784.html?feed=rss2" />
<link rel="alternate" type="application/rss+xml" title="Maximum Settings » Comments Feed" href="indexa6da.html?feed=comments-rss2" />
<link rel='stylesheet' id='wp-block-library-css' href='https://orders.maximumsettings.com/assets/css/style.css' type='text/css' media='all' />
<link rel='stylesheet' id='wp-block-library-css' href='https://orders.maximumsettings.com/assets/css/custom.css' type='text/css' media='all' />

<link rel='stylesheet' id='wp-block-library-css' href='https://orders.maximumsettings.com/assets/css/bootstrap.min.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://orders.maximumsettings.com/assets/css/sweetalert2.min.css' type='text/css'/>
<link rel='stylesheet' href='https://orders.maximumsettings.com/assets/css/select2.min.css' type='text/css'/>
<link rel='stylesheet' id='bootsnav-css' href='https://orders.maximumsettings.com/assets/css/bootsnav.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://cdn.datatables.net/1.10.19/css/jquery.dataTables.min.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://orders.maximumsettings.com/assets/css/OverlayScrollbars.css' type='text/css' media='

all' />
<link rel="stylesheet" href="https://orders.maximumsettings.com/assets/css/datepicker.css" />

<script type='text/javascript' src='https://orders.maximumsettings.com/assets/js/jquery.js'></script>

</head>

<body class="">
<!-- Preloader Start -->
<!--<div class="se-pre-con"></div>-->
<!-- Preloader Ends -->
<!-- Header
== -->
<header id="home" class="nt-site-header">
<!-- Start Navigation -->
<nav class="navbar navbar-default navbar-sticky bootsnav on no-full has-background">
 <!-- Start Atribute Navigation -->

<li class="attr-nav-li-one">
Order Now

<li class="attr-nav-li-two">
Login

<!-- End Atribute Navigation -->

<!-- Start Header Navigation -->

<button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#navbar-menu">

</button>

<!-- sticky logo -->

<!-- End Header Navigation -->

<!-- Collect the nav links, forms, and other content for toggling -->

<ul class="nav navbar-nav navbar-right" data-in="#" data-out="#">
<li id="menu-item-804" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-804"><a href="
http://maximumsettings.com#home" class="scroll">Home
<li id="menu-item-806" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-806"><a href="
http://maximumsettings.com/?author=1" class="scroll">Latest News
<li id="menu-item-807" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-807"><a href="
http://maximumsettings.com#pricing" class="scroll">Pricing
<li id="menu-item-808" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-808"><a href="
http://maximumsettings.com#faq" class="scroll">Faq’s
<li id="menu-item-811" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-811"><a href="
http://maximumsettings.com#features" class="scroll">Features
<li id="menu-item-809" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-809"><a href="

https://community.maximumsettings.com" class="scroll" target="_blank">Community
<li id="menu-item-810" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-810"><a href="
http://maximumsettings.com#contact" class="scroll">Support

<!-- /.navbar-collapse -->

</nav>
<!-- End Navigation -->

</header>
<!-- End Header -->

<h2>Account Creation</h2>

<li class="pricing-header"><h4 class="f30">PAID ACCOUNTS</h4> (Instant Activation)

<li class="footer">
Order Now

ACCOUNT CREATION

<h2 class="capitalize fw-600 mb-30 "></h2>

<form class="form-basic purchase_package form-horizontal" method="post" id="frm_upgrade" action="#" name="package-info-form">
<h3></h3>
<fieldset class="step p-l-0 m-t-10" id="step1">

```
<div class="content cus-panel col-sm-12 account_info_block">
<div class="col-sm-6">
<div class="form-group">
<label class="control-label col-sm-3">Name:</label>
<div class="col-sm-9">
<input type="text" name="name" required class="form-control u_name" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Phone :</label>
<div class="col-sm-9">
<input type="text" name="phone" required class="form-control u_phone" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Email :</label>
<div class="col-sm-9">
<input type="text" name="email" required class="form-control u_email" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Confirm Email :</label>
<div class="col-sm-9">
<input type="text" name="confirm_email" required class="form-control" value="" />
</div>
</div>
</div>
<div class="col-sm-6">
<div class="form-group">
<label class="control-label col-sm-3">Address:</label>
<div class="col-sm-9">
<textarea name="address" required class="form-control u_address"></textarea>
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3">City:</label>
<div class="col-sm-9">
<input type="text" name="city" required class="form-control u_city" value="" />
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3">Country:</label>
<div class="col-sm-9">
<select name="country" required class="form-control up_country_op">
<option value="Afghanistan">Afghanistan</option>
<option value="land">land</option>
<option value="Albania">Albania</option>
<option value="Algeria">Algeria</option>
<option value="American Samoa">American Samoa</option>
<option value="Andorra">Andorra</option>
<option value="Angola">Angola</option>
<option value="Anguilla">Anguilla</option>
<option value="Antarctica">Antarctica</option>
<option value="Antigua and Barbuda">Antigua and Barbuda</option>
```

<option value="Argentina">Argentina</option>
<option value="Armenia">Armenia</option>
<option value="Aruba">Aruba</option>
<option value="Australia">Australia</option>
<option value="Austria">Austria</option>
<option value="Azerbaijan">Azerbaijan</option>
<option value="Bahamas">Bahamas</option>
<option value="Bahrain">Bahrain</option>
<option value="Bangladesh">Bangladesh</option>
<option value="Barbados">Barbados</option>
<option value="Belarus">Belarus</option>
<option value="Belgium">Belgium</option>
<option value="Belize">Belize</option>
<option value="Benin">Benin</option>
<option value="Bermuda">Bermuda</option>
<option value="Bhutan">Bhutan</option>
<option value="Bolivia">Bolivia</option>
<option value="Bonaire">Bonaire</option>
<option value="Bosnia and Herzegovina">Bosnia and Herzegovina</option>
<option value="Botswana">Botswana</option>
<option value="Bouvet Island">Bouvet Island</option>
<option value="Brazil">Brazil</option>
<option value="British Indian Ocean Territory">British Indian Ocean Territory</option>
<option value="British Virgin Islands">British Virgin Islands</option>
<option value="Brunei">Brunei</option>
<option value="Bulgaria">Bulgaria</option>
<option value="Burkina Faso">Burkina Faso</option>
<option value="Burundi">Burundi</option>
<option value="Cambodia">Cambodia</option>
<option value="Cameroon">Cameroon</option>
<option selected='selected' value="Canada">Canada</option>
<option value="Cape Verde">Cape Verde</option>
<option value="Cayman Islands">Cayman Islands</option>
<option value="Central African Republic">Central African Republic</option>
<option value="Chad">Chad</option>
<option value="Chile">Chile</option>
<option value="China">China</option>
<option value="Christmas Island">Christmas Island</option>
<option value="Cocos [Keeling] Islands">Cocos [Keeling] Islands</option>
<option value="Colombia">Colombia</option>
<option value="Comoros">Comoros</option>
<option value="Cook Islands">Cook Islands</option>
<option value="Costa Rica">Costa Rica</option>
<option value="Croatia">Croatia</option>
<option value="Cuba">Cuba</option>
<option value="Curacao">Curacao</option>
<option value="Cyprus">Cyprus</option>
<option value="Czech Republic">Czech Republic</option>
<option value="Democratic Republic of the Congo">Democratic Republic of the Congo</option>
<option value="Denmark">Denmark</option>
<option value="Djibouti">Djibouti</option>
<option value="Dominica">Dominica</option>
<option value="Dominican Republic">Dominican Republic</option>
<option value="East Timor">East Timor</option>
<option value="Ecuador">Ecuador</option>
<option value="Egypt">Egypt</option>

<option value="El Salvador">El Salvador</option>
<option value="Equatorial Guinea">Equatorial Guinea</option>
<option value="Eritrea">Eritrea</option>
<option value="Estonia">Estonia</option>
<option value="Ethiopia">Ethiopia</option>
<option value="Falkland Islands">Falkland Islands</option>
<option value="Faroe Islands">Faroe Islands</option>
<option value="Fiji">Fiji</option>
<option value="Finland">Finland</option>
<option value="France">France</option>
<option value="French Guiana">French Guiana</option>
<option value="French Polynesia">French Polynesia</option>
<option value="French Southern Territories">French Southern Territories</option>
<option value="Gabon">Gabon</option>
<option value="Gambia">Gambia</option>
<option value="Georgia">Georgia</option>
<option value="Germany">Germany</option>
<option value="Ghana">Ghana</option>
<option value="Gibraltar">Gibraltar</option>
<option value="Greece">Greece</option>
<option value="Greenland">Greenland</option>
<option value="Grenada">Grenada</option>
<option value="Guadeloupe">Guadeloupe</option>
<option value="Guam">Guam</option>
<option value="Guatemala">Guatemala</option>
<option value="Guernsey">Guernsey</option>
<option value="Guinea">Guinea</option>
<option value="Guinea-Bissau">Guinea-Bissau</option>
<option value="Guyana">Guyana</option>
<option value="Haiti">Haiti</option>
<option value="Heard Island and McDonald Islands">Heard Island and McDonald Islands</option>
<option value="Honduras">Honduras</option>
<option value="Hong Kong">Hong Kong</option>
<option value="Hungary">Hungary</option>
<option value="Iceland">Iceland</option>
<option value="India">India</option>
<option value="Indonesia">Indonesia</option>
<option value="Iran">Iran</option>
<option value="Iraq">Iraq</option>
<option value="Ireland">Ireland</option>
<option value="Isle of Man">Isle of Man</option>
<option value="Israel">Israel</option>
<option value="Italy">Italy</option>
<option value="Ivory Coast">Ivory Coast</option>
<option value="Jamaica">Jamaica</option>
<option value="Japan">Japan</option>
<option value="Jersey">Jersey</option>
<option value="Jordan">Jordan</option>
<option value="Kazakhstan">Kazakhstan</option>
<option value="Kenya">Kenya</option>
<option value="Kiribati">Kiribati</option>
<option value="Kosovo">Kosovo</option>
<option value="Kuwait">Kuwait</option>

Results were truncated

Scan Activity per Port

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-06-24 12:42:21.0

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Protocol Port
Time
TCP 443 13:21:56

SSL Certificate - Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-

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

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME VALUE

(0)CERTIFICATE 0
(0)Version 3 (0x2)
(0)Serial Number 03:9b:ff:79:71:df:f3:0d:0f:71:f8:0f:35:59:a1:e0:5b:0f
(0)Signature Algorithm sha256WithRSAEncryption
(0)ISSUER NAME
countryName US
organizationName Let's Encrypt
commonName R3
(0)SUBJECT NAME
commonName *.maximumsettings.com
(0)Valid From Sep 4 18:52:47 2022 GMT
(0)Valid Till Dec 3 18:52:46 2022 GMT
(0)Public Key Algorithm rsaEncryption
(0)RSA Public Key (2048 bit)
(0) RSA Public-Key: (2048 bit)
(0) Modulus:
(0) 00:b3:60:e9:fb:9e:e9:bd:42:31:d5:30:20:46:9e:
(0) dc:82:e3:13:62:50:2a:33:ca:58:1b:89:c4:fa:6d:
(0) fa:06:94:6d:17:89:ef:13:33:fe:c6:51:cc:e8:1b:
(0) b3:ba:cb:e6:64:b8:b2:8f:39:a9:f4:bc:6a:df:bd:
(0) 79:47:ab:31:81:d5:1c:31:4e:5b:33:e2:9a:e5:91:
(0) f4:cd:6b:15:ae:71:0a:73:5f:0a:9a:e0:46:76:8b:
(0) 29:e3:14:fa:64:f7:17:96:ce:fd:61:66:28:61:e4:
(0) ee:e5:24:f7:e6:26:4b:81:3d:47:65:c5:55:a5:d9:
(0) 96:01:2f:50:83:d2:9e:b8:34:96:fd:6a:b1:1b:58:
(0) 1c:11:1d:8d:10:32:34:d4:ee:83:74:db:83:ac:02:
(0) 27:58:fb:f5:77:81:bd:25:83:bd:58:62:3d:b6:b9:
(0) 74:95:f7:07:45:92:41:b9:b4:32:f4:6b:fb:d9:6a:
(0) d6:38:83:93:d6:73:95:54:34:4a:15:1a:6d:ea:9c:
(0) d2:16:f4:af:6e:4f:db:37:a8:bd:0a:2b:e6:48:81:
(0) e8:2f:b4:da:b2:9e:4b:1a:af:94:73:2a:72:93:4d:
(0) d4:97:a1:77:8a:e1:15:d5:ea:99:c6:58:a7:19:9d:
(0) 51:78:cf:b6:83:3e:f8:d1:40:8e:cd:d2:cf:fa:1a:
(0) 75:bf
(0) Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS
(0)X509v3 Key Usage critical
(0) Digital Signature, Key Encipherment
(0)X509v3 Extended Key Usage TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints critical
(0) CA:FALSE
(0)X509v3 Subject Key Identifier 00:82:C3:D4:58:77:CD:C2:E9:D2:DD:8E:C7:68:BF:22:2A:A7:C6:E1
(0)X509v3 Authority Key Identifier keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:

C6
(0)Authority Information Access OCSP - URI:http://r3.o.lencr.org
(0) CA Issuers - URI:http://r3.i.lencr.org/
(0)X509v3 Subject Alternative Name DNS:*.maximumsettings.com
(0)X509v3 Certificate Policies Policy: 2.23.140.1.2.1
(0) Policy: 1.3.6.1.4.1.44947.1.1.1
(0) CPS: http://cps.letsencrypt.org
(0)CT Precertificate SCTs Signed Certificate Timestamp:
(0) Version : v1 (0x0)
(0) Log ID : 6F:53:76:AC:31:F0:31:19:D8:99:00:A4:51:15:FF:77:
(0) 15:1C:11:D9:02:C1:00:29:06:8D:B2:08:9A:37:D9:13
(0) Timestamp : Sep 4 19:52:47.304 2022 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:45:02:20:29:39:25:22:3B:F8:0C:E0:29:8B:03:CA:
(0) 88:0B:C5:41:E0:7F:31:8A:7B:29:04:D8:67:34:A8:18:
(0) 9F:D4:1D:34:02:21:00:B8:7D:1A:62:28:32:39:01:C9:
(0) CD:88:75:8A:1C:EF:01:8A:F7:EC:C4:EF:34:1A:B3:D1:
(0) 98:7F:03:12:36:24:C9
(0) Signed Certificate Timestamp:
(0) Version : v1 (0x0)
(0) Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0) 11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0) Timestamp : Sep 4 19:52:47.325 2022 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:45:02:21:00:BB:2C:D0:A6:C2:4C:FB:65:D8:50:84:
(0) 40:28:4F:0A:A1:69:AE:50:AB:80:AB:79:60:15:E9:68:
(0) 81:D9:F1:38:9E:02:20:4E:54:0F:45:82:05:AD:5F:54:
(0) 36:94:88:E1:F9:AC:B4:A5:9C:D8:EE:17:AF:52:50:29:
(0) C9:F5:65:60:E1:A3:AE
(0)Signature (256 octets)
(0) 56:a2:d0:5c:10:93:be:a5:c6:52:b5:1a:1e:bd:df:d8
(0) 8e:a2:d5:42:0e:82:63:f6:1f:bc:7b:c6:23:b9:52:91
(0) 20:9e:a6:1f:88:cb:29:45:20:a5:9f:2a:1f:a7:71:fe
(0) 2b:c4:40:2e:0a:c7:27:b7:6b:b4:c1:5c:0d:e9:da:b4
(0) 82:8b:05:ab:19:19:00:75:9c:1f:af:7e:33:61:aa:89
(0) d6:f0:b9:4d:69:b4:1c:5c:3c:83:a6:20:a7:c8:dc:75
(0) 3f:49:e3:68:37:9d:cd:b0:cf:50:d5:03:ef:fa:85:db
(0) 33:21:5f:5d:06:a3:2d:e6:93:49:81:48:08:de:d3:3a
(0) f9:17:25:5c:36:e3:09:40:3b:30:a8:a6:f8:0c:31:f9
(0) b5:52:c2:14:63:b8:18:a3:fb:c7:f2:d6:c0:d4:f5:ca
(0) b3:b9:4e:ee:9c:12:65:6b:db:1e:87:51:e2:78:6d:68
(0) 15:d1:ef:86:33:80:ce:7a:ec:c7:e8:28:8b:44:9b:f2
(0) 38:d0:d0:42:ce:24:0a:ad:72:10:f7:92:34:8b:62:fc
(0) 32:80:6c:e8:1c:1a:3e:9c:d7:94:19:4f:44:24:88:b2
(0) 7c:c0:0b:09:e4:e7:cb:79:9e:81:ca:2c:f5:52:d9:bd
(0) 87:6d:61:02:f5:51:da:26:69:f7:50:df:bc:29:b9:8a
(1)CERTIFICATE 1
(1)Version 3 (0x2)
(1)Serial Number 91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a
(1)Signature Algorithm sha256WithRSAEncryption
(1)ISSUER NAME
countryName US
organizationName Internet Security Research Group
commonName ISRG Root X1

(1)SUBJECT NAME
countryName US
organizationName Let's Encrypt
commonName R3
(1)Valid From Sep 4 00:00:00 2020 GMT
(1)Valid Till Sep 15 16:00:00 2025 GMT
(1)Public Key Algorithm rsaEncryption
(1)RSA Public Key (2048 bit)
(1) RSA Public-Key: (2048 bit)
(1) Modulus:
(1) 00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:
(1) 92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:
(1) 2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47:
(1) 94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:
(1) a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:
(1) e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:
(1) 37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:
(1) 45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:
(1) 60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:
(1) d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:
(1) 30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:
(1) c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:
(1) e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:
(1) a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:
(1) 09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:
(1) 63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:
(1) a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:
(1) db:15
(1) Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS
(1)X509v3 Key Usage critical
(1) Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Extended Key Usage TLS Web Client Authentication, TLS Web Server Authentication
(1)X509v3 Basic Constraints critical
(1) CA:TRUE, pathlen:0
(1)X509v3 Subject Key Identifier 14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
(1)X509v3 Authority Key Identifier keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
(1)Authority Information Access CA Issuers - URI:http://x1.i.lencr.org/
(1)X509v3 CRL Distribution Points
(1) Full Name:
(1) URI:http://x1.c.lencr.org/
(1)X509v3 Certificate Policies Policy: 2.23.140.1.2.1
(1) Policy: 1.3.6.1.4.1.44947.1.1.1
(1)Signature (512 octets)
(1) 85:ca:4e:47:3e:a3:f7:85:44:85:bc:d5:67:78:b2:98
(1) 63:ad:75:4d:1e:96:3d:33:65:72:54:2d:81:a0:ea:c3
(1) ed:f8:20:bf:5f:cc:b7:70:00:b7:6e:3b:f6:5e:94:de
(1) e4:20:9f:a6:ef:8b:b2:03:e7:a2:b5:16:3c:91:ce:b4
(1) ed:39:02:e7:7c:25:8a:47:e6:65:6e:3f:46:f4:d9:f0
(1) ce:94:2b:ee:54:ce:12:bc:8c:27:4b:b8:c1:98:2f:a2
(1) af:cd:71:91:4a:08:b7:c8:b8:23:7b:04:2d:08:f9:08
(1) 57:3e:83:d9:04:33:0a:47:21:78:09:82:27:c3:2a:c8
(1) 9b:b9:ce:5c:f2:64:c8:c0:be:79:c0:4f:8e:6d:44:0c
(1) 5e:92:bb:2e:f7:8b:10:e1:e8:1d:44:29:db:59:20:ed
(1) 63:b9:21:f8:12:26:94:93:57:a0:1d:65:04:c1:0a:22
(1) ae:10:0d:43:97:a1:18:1f:7e:e0:e0:86:37:b5:5a:b1

(1) bd:30:bf:87:6e:2b:2a:ff:21:4e:1b:05:c3:f5:18:97
(1) f0:5e:ac:c3:a5:b8:6a:f0:2e:bc:3b:33:b9:ee:4b:de
(1) cc:fc:e4:af:84:0b:86:3f:c0:55:43:36:f6:68:e1:36
(1) 17:6a:8e:99:d1:ff:a5:40:a7:34:b7:c0:d0:63:39:35
(1) 39:75:6e:f2:ba:76:c8:93:02:e9:a9:4b:6c:17:ce:0c
(1) 02:d9:bd:81:fb:9f:b7:68:d4:06:65:b3:82:3d:77:53
(1) f8:8e:79:03:ad:0a:31:07:75:2a:43:d8:55:97:72:c4
(1) 29:0e:f7:c4:5d:4e:c8:ae:46:84:30:d7:f2:85:5f:18
(1) a1:79:bb:e7:5e:70:8b:07:e1:86:93:c3:b9:8f:dc:61
(1) 71:25:2a:af:df:ed:25:50:52:68:8b:92:dc:e5:d6:b5
(1) e3:da:7d:d0:87:6c:84:21:31:ae:82:f5:fb:b9:ab:c8
(1) 89:17:3d:e1:4c:e5:38:0e:f6:bd:2b:bd:96:81:14:eb
(1) d5:db:3d:20:a7:7e:59:d3:e2:f8:58:f9:5b:b8:48:cd
(1) fe:5c:4f:16:29:fe:1e:55:23:af:c8:11:b0:8d:ea:7c
(1) 93:90:17:2f:fd:ac:a2:09:47:46:3f:f0:e9:b0:b7:ff
(1) 28:4d:68:32:d6:67:5e:1e:69:a3:93:b8:f5:9d:8b:2f
(1) 0b:d2:52:43:a6:6f:32:57:65:4d:32:81:df:38:53:85
(1) 5d:7e:5d:66:29:ea:b8:dd:e4:95:b5:cd:b5:56:12:42
(1) cd:c4:4e:c6:25:38:44:50:6d:ec:ce:00:55:18:fe:e9
(1) 49:64:d4:4e:ca:97:9c:b4:5b:c0:73:a8:ab:b8:47:c2
(2)CERTIFICATE 2
(2)Version 3 (0x2)
(2)Serial Number 40:01:77:21:37:d4:e9:42:b8:ee:76:aa:3c:64:0a:b7
(2)Signature Algorithm sha256WithRSAEncryption
(2)ISSUER NAME
organizationName Digital Signature Trust Co.
commonName DST Root CA X3
(2)SUBJECT NAME
countryName US
organizationName Internet Security Research Group
commonName ISRG Root X1
(2)Valid From Jan 20 19:14:03 2021 GMT
(2)Valid Till Sep 30 18:14:03 2024 GMT
(2)Public Key Algorithm rsaEncryption
(2)RSA Public Key (4096 bit)
(2) RSA Public-Key: (4096 bit)
(2) Modulus:
(2) 00:ad:e8:24:73:f4:14:37:f3:9b:9e:2b:57:28:1c:
(2) 87:be:dc:b7:df:38:90:8c:6e:3c:e6:57:a0:78:f7:
(2) 75:c2:a2:fe:f5:6a:6e:f6:00:4f:28:db:de:68:86:
(2) 6c:44:93:b6:b1:63:fd:14:12:6b:bf:1f:d2:ea:31:
(2) 9b:21:7e:d1:33:3c:ba:48:f5:dd:79:df:b3:b8:ff:
(2) 12:f1:21:9a:4b:c1:8a:86:71:69:4a:66:66:6c:8f:
(2) 7e:3c:70:bf:ad:29:22:06:f3:e4:c0:e6:80:ae:e2:
(2) 4b:8f:b7:99:7e:94:03:9f:d3:47:97:7c:99:48:23:
(2) 53:e8:38:ae:4f:0a:6f:83:2e:d1:49:57:8c:80:74:
(2) b6:da:2f:d0:38:8d:7b:03:70:21:1b:75:f2:30:3c:
(2) fa:8f:ae:dd:da:63:ab:eb:16:4f:c2:8e:11:4b:7e:
(2) cf:0b:e8:ff:b5:77:2e:f4:b2:7b:4a:e0:4c:12:25:
(2) 0c:70:8d:03:29:a0:e1:53:24:ec:13:d9:ee:19:bf:
(2) 10:b3:4a:8c:3f:89:a3:61:51:de:ac:87:07:94:f4:
(2) 63:71:ec:2e:e2:6f:5b:98:81:e1:89:5c:34:79:6c:
(2) 76:ef:3b:90:62:79:e6:db:a4:9a:2f:26:c5:d0:10:
(2) e1:0e:de:d9:10:8e:16:fb:b7:f7:a8:f7:c7:e5:02:
(2) 07:98:8f:36:08:95:e7:e2:37:96:0d:36:75:9e:fb:
(2) 0e:72:b1:1d:9b:bc:03:f9:49:05:d8:81:dd:05:b4:

(2) 2a:d6:41:e9:ac:01:76:95:0a:0f:d8:df:d5:bd:12:
(2) 1f:35:2f:28:17:6c:d2:98:c1:a8:09:64:77:6e:47:
(2) 37:ba:ce:ac:59:5e:68:9d:7f:72:d6:89:c5:06:41:
(2) 29:3e:59:3e:dd:26:f5:24:c9:11:a7:5a:a3:4c:40:
(2) 1f:46:a1:99:b5:a7:3a:51:6e:86:3b:9e:7d:72:a7:
(2) 12:05:78:59:ed:3e:51:78:15:0b:03:8f:8d:d0:2f:
(2) 05:b2:3e:7b:4a:1c:4b:73:05:12:fc:c6:ea:e0:50:
(2) 13:7c:43:93:74:b3:ca:74:e7:8e:1f:01:08:d0:30:
(2) d4:5b:71:36:b4:07:ba:c1:30:30:5c:48:b7:82:3b:
(2) 98:a6:7d:60:8a:a2:a3:29:82:cc:ba:bd:83:04:1b:
(2) a2:83:03:41:a1:d6:05:f1:1b:c2:b6:f0:a8:7c:86:
(2) 3b:46:a8:48:2a:88:dc:76:9a:76:bf:1f:6a:a5:3d:
(2) 19:8f:eb:38:f3:64:de:c8:2b:0d:0a:28:ff:f7:db:
(2) e2:15:42:d4:22:d0:27:5d:e1:79:fe:18:e7:70:88:
(2) ad:4e:e6:d9:8b:3a:c6:dd:27:51:6e:ff:bc:64:f5:
(2) 33:43:4f
(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)Authority Information Access CA Issuers - URI:http://apps.identrust.com/roots/dstrootcax3.p7c
(2)X509v3 Authority Key Identifier keyid:C4:A7:B1:A4:7B:2C:71:FA:DB:E1:4B:90:75:FF:C4:15:60:85:89:
10
(2)X509v3 Certificate Policies Policy: 2.23.140.1.2.1
(2) Policy: 1.3.6.1.4.1.44947.1.1.1
(2) CPS: http://cps.root-x1.letsencrypt.org
(2)X509v3 CRL Distribution Points
(2) Full Name:
(2) URI:http://crl.identrust.com/DSTROOTCAX3CRL.crl
(2)X509v3 Subject Key Identifier 79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
(2)Signature (256 octets)
(2) 0a:73:00:6c:96:6e:ff:0e:52:d0:ae:dd:8c:e7:5a:06
(2) ad:2f:a8:e3:8f:bf:c9:0a:03:15:50:c2:e5:6c:42:bb
(2) 6f:9b:f4:b4:4f:c2:44:88:08:75:cc:eb:07:9b:14:62
(2) 6e:78:de:ec:27:ba:39:5c:f5:a2:a1:6e:56:94:70:10
(2) 53:b1:bb:e4:af:d0:a2:c3:2b:01:d4:96:f4:c5:20:35
(2) 33:f9:d8:61:36:e0:71:8d:b4:b8:b5:aa:82:45:95:c0
(2) f2:a9:23:28:e7:d6:a1:cb:67:08:da:a0:43:2c:aa:1b
(2) 93:1f:c9:de:f5:ab:69:5d:13:f5:5b:86:58:22:ca:4d
(2) 55:e4:70:67:6d:c2:57:c5:46:39:41:cf:8a:58:83:58
(2) 6d:99:fe:57:e8:36:0e:f0:0e:23:aa:fd:88:97:d0:e3
(2) 5c:0e:94:49:b5:b5:17:35:d2:2e:bf:4e:85:ef:18:e0
(2) 85:92:eb:06:3b:6c:29:23:09:60:dc:45:02:4c:12:18
(2) 3b:e9:fb:0e:de:dc:44:f8:58:98:ae:ea:bd:45:45:a1
(2) 88:5d:66:ca:fe:10:e9:6f:82:c8:11:42:0d:fb:e9:ec
(2) e3:86:00:de:9d:10:e3:38:fa:a4:7d:b1:d8:e8:49:82
(2) 84:06:9b:2b:e8:6b:4f:01:0c:38:77:2e:f9:dd:e7:39

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2018-01-04 17:39:37.0

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

IP address Host name
66.49.252.119 order.maximumsettings.
com

Form Contains Credit Card Information — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150043
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-30 21:20:25.0

THREAT:
The links listed below have forms that accept credit card information. This information is provided to help you identify areas of the web application that may need careful review due to the sensitive data being handled.

IMPACT:
N/A

SOLUTION:
If possible, review of the source code responsible for handling these form inputs.

RESULT:
https://order.maximumsettings.com/

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

IMPACT:
Items include:

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

SOLUTION:
N/A

RESULT:

NAME STATUS
TLSv1.2
Extended Master Secret yes

Encrypt Then MAC yes
Heartbeat no
Truncated HMAC no
Cipher priority controlled by client
OCSP stapling no
SCT extension no
TLSv1.3
Heartbeat no
Cipher priority controlled by client
OCSP stapling no
SCT extension no

External Links Discovered — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Number of links: 19
https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css
https://www.paypal.com/sdk/js?client-id=AXCYoBHG6D0aLrR8_-C8M5J6CT1rvQPPb7H16kP0h994jDOGITw1ufMaqLNZiCTmEkwFWSBPXoDBHzeN&currency=CAD
https://www.paypal.com/sdk/js?client-id=AdxTCDDviKQ4NfGkev7ZHmb6dpcARIMXdWiLdkFWAYpwUnNmWbs6HIFQYla0yrYi227svx1cN4J3HkBF&currency=USD
https://www.paypalobjects.com/api/checkout.js
https://cdn.datatables.net/1.10.19/css/jquery.dataTables.min.css
https://code.highcharts.com/highcharts.js
https://code.highcharts.com/modules/export-data.js
https://code.highcharts.com/modules/exporting.js
https://code.highcharts.com/modules/series-label.js

https://community.maximumsettings.com/
https://orders.maximumsettings.com/
https://discord.gg/A9jp5Cn
https://canvasjs.com/assets/script/jquery-1.11.1.min.js
https://canvasjs.com/assets/script/jquery.canvasjs.min.js
https://login.maximumsettings.com/
http://fonts.googleapis.com/
http://maximumsettings.com/
http://maximumsettings.com/?author=1
http://s.w.org/

Web Server and Technologies Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150247
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-04-27 20:40:50.0

THREAT:
Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.
IMPACT:
An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

SOLUTION:
Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:
RESULT:
Number of technologies detected: 2
Technology name: Apache
Matched Components:
header match:
Server:Apache
Matched links: reporting only first 3 links
https://order.maximumsettings.com/
https://order.maximumsettings.com/indexa6da.html?feed=comments-rss2
https://order.maximumsettings.com/indexd784.html?feed=rss2

Technology name: Bootstrap
Matched Components:

html response match:
='text/css' media='all' />
<link rel='stylesheet' id='wp-block-library-css' href='https://order.maximumsettings.com/assets/css/custom.css' type='text/css' media='all' />

<link rel='stylesheet' id='wp-block-library-css' href='https://order.maximumsettings.com/assets/css/bootstrap.min.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://order.maximumsettings.com/assets/css/sweetalert2.min.css' type='text/css'/>
<link rel='stylesheet' href
script tag match:
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/bootstrap-datepicker.js'></script>
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/bootstrap.min.js'></script>
<script type='text/javascript' src='js/bootstrap-datetimepicker.js'></script>
Matched links: reporting only first 3 links
https://order.maximumsettings.com/

Scan Diagnostics — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

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

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

SOLUTION:
No action is required.

RESULT:
Target web application page https://order.maximumsettings.com/ fetched. Status code:200, Content-Type:text/html, load time:409 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 4 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.

Collected 28 links overall in 0 hours 0 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 3) + files:(0 x 4) + directories:(9 x 6) + paths:(0 x 10) = total (54)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 10 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 36 requests, 0 seconds. Completed 36 requests of 54 estimated requests (66.6667%). All tests completed.
WSEnumeration no tests enabled.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (95 tests, 1 inputs)
Batch #1 URI parameter manipulation (no auth): 95 vulnsigs tests, completed 83 requests, 2 seconds. Completed 83 requests of 95 estimated requests (87.3684%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 1 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 16 requests, 0 seconds. Completed 16 requests of 24 estimated requests (66.6667%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 1 inputs)
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 14 requests, 1 seconds. Completed 14 requests of 14 estimated requests (100%). All tests completed.
Time based tests for Apache Struts Vulnerabilities - no tests enabled.
Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (95 tests, 1 inputs)
Batch #2 URI parameter manipulation (no auth): 95 vulnsigs tests, completed 83 requests, 1 seconds. Completed 83 requests of 95 estimated requests (87.3684%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 1 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 16 requests, 1 seconds. Completed 16 requests of 24 estimated requests (66.6667%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 1 inputs)
Batch #2 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 14 requests, 0 seconds. Completed 14 requests of 14 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 1 minute (107 tests, 1 inputs)
Batch #4 WebCgiOob: 107 vulnsigs tests, completed 54 requests, 1 seconds. Completed 54 requests of 1190 estimated requests (4.53782%). All tests completed.
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, 4 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 4 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 1 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 72 requests, 2 seconds. Completed 72 requests of 72 estimated requests (100%). XSS optimization removed 116 links. All tests completed.
Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 4 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 252 requests, 4 seconds. Completed 252 requests of 520 estimated requests (48.4615%). XSS optimization removed 116 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 4 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 4 requests, 1 seconds. Completed 4 requests of 4 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.
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 3) + files:(0 x 4) + directories:(4 x 6) + paths:(11 x 10) = total (134)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 10 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 92 requests, 2 seconds. Completed 92 requests of 134 estimated requests (68.6567%). 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 3) + files:(10 x 4) + directories:(95 x 6) + paths:(9 x 10) = total (709)
Batch #5 Path manipulation: estimated time < 1 minute (117 tests, 10 inputs)
Batch #5 Path manipulation: 117 vulnsigs tests, completed 474 requests, 5 seconds. Completed 474 requests of 709 estimated requests (66.8547%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 minute (247 tests, 1 inputs)
Batch #5 WebCgiGeneric: 247 vulnsigs tests, completed 468 requests, 8 seconds. Completed 468 requests of 3130 estimated requests (14.9521%). All tests completed.
Duration of Crawl Time: 9.00 (seconds)
Duration of Test Phase: 29.00 (seconds)
Total Scan Time: 38.00 (seconds)

Total requests made: 1755
Average server response time: 0.10 seconds

Average browser load time: 0.11 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Web Server Version — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
Apache

Referrer-Policy HTTP Security Header Not Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:26.0

THREAT:

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

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

QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

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

SOLUTION:

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

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

RESULT:

Referrer-Policy HTTP Header missing on 443 port.

Web Server and Technologies Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150247
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-04-27 20:40:50.0

THREAT:
Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

IMPACT:
An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

SOLUTION:
Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:

RESULT:
Number of technologies detected: 2
Technology name: Apache
Matched Components:
header match:
Server:Apache
Matched links: reporting only first 3 links
https://orders.maximumsettings.com/
https://orders.maximumsettings.com/indexa6da.html?feed=comments-rss2
https://orders.maximumsettings.com/indexd784.html?feed=rss2

Technology name: Bootstrap
Matched Components:
html response match:
text/css' media='all' />
<link rel='stylesheet' id='wp-block-library-css' href='https://orders.maximumsettings.com/assets/css/custom.css' type='text/css' media='all' />

<link rel='stylesheet' id='wp-block-library-css' href='https://orders.maximumsettings.com/assets/css/bootstrap.min.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://orders.maximumsettings.com/assets/css/sweetalert2.min.css' type='text/css'/>
<link rel='stylesheet' hre
script tag match:
<script type='text/javascript' src='https://orders.maximumsettings.com/assets/js/bootstrap-datepicker.js'></script>
<script type='text/javascript' src='https://orders.maximumsettings.com/assets/js/bootstrap.min.js'></script>
<script type='text/javascript' src='js/bootstrap-datetimepicker.js'></script>
Matched links: reporting only first 3 links
https://orders.maximumsettings.com/

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

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:

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

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH

TLSv1.2
RSA 2048 no 110 low
DHE 2048 yes 110 low
ECDHE x448 448 yes 224 low
ECDHE x25519 256 yes 128 low
ECDHE secp384r1 384 yes 192 low
ECDHE secp256r1 256 yes 128 low
ECDHE secp521r1 521 yes 260 low
TLSv1.3
ECDHE x25519 256 yes 128 low
ECDHE secp256r1 256 yes 128 low
ECDHE x448 448 yes 224 low
ECDHE secp521r1 521 yes 260 low
ECDHE secp384r1 384 yes 192 low

HTTP Public-Key-Pins Security Header Not Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**

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

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

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

IMPACT:
N/A
SOLUTION:
N/A

RESULT:
HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.0
Host: order.maximumsettings.com

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

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

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

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

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

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

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

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:
https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css
https://www.paypal.com/sdk/js?client-id=AXCYoBHG6D0aLrR8_-C8M5J6CT1rvQPPb7H16kP0h994jDOGITw1ufMaqLNZiCTmEkwFWSBPXoDBHzeN&currency=CAD
https://www.paypal.com/sdk/js?client-id=AdxTCDDviKQ4NfGkev7ZHmb6dpcARIMXdWiLdkFWAYpwUnNmWbs6HIFQYla0yrYi227svx1cN4J3HkBF&currency=USD
https://www.paypalobjects.com/api/checkout.js
https://cdn.datatables.net/1.10.19/css/jquery.dataTables.min.css
https://code.highcharts.com/highcharts.js
https://code.highcharts.com/modules/export-data.js
https://code.highcharts.com/modules/exporting.js
https://code.highcharts.com/modules/series-label.js
https://community.maximumsettings.com/

IP based excluded links:

First Link Crawled Response Code Information — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150546
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-10-05 18:04:13.0

THREAT:
The Web server returned the following information from where the Web application scanning engine initiated. Information reported includes First Link Crawled, response Code, response Header, and response Body (first 500 characters). The first link crawled is the "Web Application URL (or Swagger file URL)" set in the Web Application profile.

IMPACT:
An erroneous response might be indicative of a problem in the Web server, or the scan configuration.

SOLUTION:
Review the information to check if this is in line with the expected scan configuration. Refer to the output of QIDs 150009, 150019, 150021, 150042 and 150528 (if present) for additional details.

RESULT:
Base URI: https://orders.maximumsettings.com/
Response Code: 200
Response Header:

Date: Fri, 25 Nov 2022 19:25:57 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Set-Cookie: ci_session=aevqoh5bev8av1l56nl2anurkemkg72k; expires=Fri, 25-Nov-2022 19:35:58 GMT; Max-Age=600; path=/; HttpOnly;HttpOnly;Secure; SameSite=Strict
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

Response Body:

<!DOCTYPE html>
<html class="no-js" lang="en">
<head>
<base href="https://orders.maximumsettings.com/">
<meta content="charset=utf-8">
<title>Maximum Settings – Dedicated Game Streaming</title>
<meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<meta name="viewport" content="width=device-width, initia
...

Default Web Page — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.0
Host: order.maximumsettings.com

<!DOCTYPE html>
<html class="no-js" lang="en">
<head>
<base href="https://order.maximumsettings.com/">
<meta content="charset=utf-8">
<title>Maximum Settings – Dedicated Game Streaming</title>
<meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<meta name="viewport" content="width=device-width, initial-scale=1">
<base href="https://order.maximumsettings.com/">
<script type="text/javascript">
var site_url = "https://order.maximumsettings.com/";
var base_url = "https://order.maximumsettings.com/";
var show_setting_popup = '';
var security_check = '1';
var iframe_url = '';
var ip_add = '64.39.98.151';
</script>

<link rel='dns-prefetch' href='http://fonts.googleapis.com/' />
<link rel='dns-prefetch' href='http://s.w.org/' />

<link rel='stylesheet' id='softing-fonts-css' href='//fonts.googleapis.com/css?family=Open%2BSans%7CPoppins%3A400%2C500%2C600%2C700%2C800&subset=latin%2Clatin-ext&ver=1.0' type='text/css' media='all' />
<link rel="stylesheet" href="https://order.maximumsettings.com/assets/css/all.css" integrity="sha384-50oBUHEmvpQ+1lW4y57PTFmhCaXp0ML5d60M1M7uH2+nqUivzIebhndOJK28anvf" crossorigin="anonymous">

<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
<link rel="alternate" type="application/rss+xml" title="Maximum Settings » Feed" href="indexd784.html?feed=rss2" />
<link rel="alternate" type="application/rss+xml" title="Maximum Settings » Comments Feed" href="indexa6da.html?feed=comments-rss2" />
<link rel='stylesheet' id='wp-block-library-css' href='https://order.maximumsettings.com/assets/css/style.css' type='text/css' media='all' />
<link rel='stylesheet' id='wp-block-library-css' href='https://order.maximumsettings.com/assets/css/custom.css' type='text/css' media='all' />

<link rel='stylesheet' id='wp-block-library-css' href='https://order.maximumsettings.com/assets/css/bootstrap.min.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://order.maximumsettings.com/assets/css/sweetalert2.min.css' type='text/css'/>
<link rel='stylesheet' href='https://order.maximumsettings.com/assets/css/select2.min.css' type='text/css'/>
<link rel='stylesheet' id='bootsnav-css' href='https://order.maximumsettings.com/assets/css/bootsnav.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://cdn.datatables.net/1.10.19/css/jquery.dataTables.min.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://order.maximumsettings.com/assets/css/OverlayScrollbars.css' type='text/css' media='all' />
<link rel="stylesheet" href="https://order.maximumsettings.com/assets/css/datepicker.css" />

<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/jquery.js'></script>

</head>

<body class="">
<!-- Preloader Start -->
<!--<div class="se-pre-con"></div>-->
<!-- Preloader Ends -->
<!-- Header
== -->
<header id="home" class="nt-site-header">
<!-- Start Navigation -->
<nav class="navbar navbar-default navbar-sticky bootsnav on no-full has-background">
 <!-- Start Atribute Navigation -->

<li class="attr-nav-li-one">
Order Now

<li class="attr-nav-li-two">
Login

<!-- End Atribute Navigation -->

<!-- Start Header Navigation -->

<button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#navbar-menu">

</button>

<!-- sticky logo -->

<!-- End Header Navigation -->

<!-- Collect the nav links, forms, and other content for toggling -->

<ul class="nav navbar-nav navbar-right" data-in="#" data-out="#">
<li id="menu-item-804" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-804"><a href="
http://maximumsettings.com#home" class="scroll">Home
<li id="menu-item-806" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-806"><a href="
http://maximumsettings.com/?author=1" class="scroll">Latest News
<li id="menu-item-807" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-807"><a href="
http://maximumsettings.com#pricing" class="scroll">Pricing
<li id="menu-item-808" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-808"><a href="
http://maximumsettings.com#faq" class="scroll">Faq’s
<li id="menu-item-811" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-811"><a href="
http://maximumsettings.com#features" class="scroll">Features
<li id="menu-item-809" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-809"><a href="
https://community.maximumsettings.com" class="scroll" target="_blank">Community
<li id="menu-item-810" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-810"><a href="
http://maximumsettings.com#contact" class="scroll">Support


```
</div><!-- /.navbar-collapse -->
</div>
</nav>
<!-- End Navigation -->

</header>
<!-- End Header -->

<div class="content">
<div class="container">
<div class="main_content ult-responsive row">
<div class="nt-column col-sm-12 col-lg-offset-2 col-lg-8 col-lg-offset-2 col-md-offset-1 col-md-8">
<div class="site-heading text-center">
<br><h2>Account Creation</h2>
</div>
</div>


<div class="row">

<div class="register-wrapper">
<div class="col-sm-12 col-lg-12 col-md-12">
<div class="pricing-area">
<div class="pricing-item text-center or-box-min ">
<ul>
<li class="pricing-header"><h4 class="f30">PAID ACCOUNTS</h4><span class="fw400 order_header_h2"> ( Instant Activation )</span></li>

<li class="footer">
<a class="btn circle btn-theme paid_account">Order Now</a>
</li>
<li> </li>
</ul>
</div>
</div>

</div>


<div style="clear: both;"></div>
<br>
</div>
<div style="display: none;" class="paid_register_content nt-column col-sm-12 col-lg-12 col-md-12 nt_col-has-responsive-data">
<div class="panel panel-blue">
<div class="panel-heading">ACCOUNT CREATION</div>
<div class="panel-body">
<div class="">
<div class="nt-wrapper "><h2 class="capitalize fw-600 mb-30 "></h2>
<div role="form" class="wpcf7" id="wpcf7-f608-p654-o2" lang="en-US" dir="ltr">
<div class="error_msg_div"></div>
<form class="form-basic purchase_package form-horizontal" method="post" id="frm_upgrade" action="#" name="package-info-form">
<h3></h3>
<fieldset class="step p-l-0 m-t-10" id="step1">
<div class="content cus-panel col-sm-12 account_info_block">
<div class="col-sm-6">
<div class="form-group">
<label class="control-label col-sm-3">Name:</label>
```

```
<div class="col-sm-9">
<input type="text" name="name" required class="form-control u_name" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Phone :</label>
<div class="col-sm-9">
<input type="text" name="phone" required class="form-control u_phone" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Email :</label>
<div class="col-sm-9">
<input type="text" name="email" required class="form-control u_email" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Confirm Email :</label>
<div class="col-sm-9">
<input type="text" name="confirm_email" required class="form-control" value="" />
</div>
</div>
</div>
<div class="col-sm-6">
<div class="form-group">
<label class="control-label col-sm-3">Address:</label>
<div class="col-sm-9">
<textarea name="address" required class="form-control u_address"></textarea>
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3">City:</label>
<div class="col-sm-9">
<input type="text" name="city" required class="form-control u_city" value="" />
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3">Country:</label>
<div class="col-sm-9">
<select name="country" required class="form-control up_country_op">
<option value="Afghanistan">Afghanistan</option>
<option value="land">land</option>
<option value="Albania">Albania</option>
<option value="Algeria">Algeria</option>
<option value="American Samoa">American Samoa</option>
<option value="Andorra">Andorra</option>
<option value="Angola">Angola</option>
<option value="Anguilla">Anguilla</option>
<option value="Antarctica">Antarctica</option>
<option value="Antigua and Barbuda">Antigua and Barbuda</option>
<option value="Argentina">Argentina</option>
<option value="Armenia">Armenia</option>
<option value="Aruba">Aruba</option>
<option value="Australia">Australia</option>
```

<option value="Austria">Austria</option>
<option value="Azerbaijan">Azerbaijan</option>
<option value="Bahamas">Bahamas</option>
<option value="Bahrain">Bahrain</option>
<option value="Bangladesh">Bangladesh</option>
<option value="Barbados">Barbados</option>
<option value="Belarus">Belarus</option>
<option value="Belgium">Belgium</option>
<option value="Belize">Belize</option>
<option value="Benin">Benin</option>
<option value="Bermuda">Bermuda</option>
<option value="Bhutan">Bhutan</option>
<option value="Bolivia">Bolivia</option>
<option value="Bonaire">Bonaire</option>
<option value="Bosnia and Herzegovina">Bosnia and Herzegovina</option>
<option value="Botswana">Botswana</option>
<option value="Bouvet Island">Bouvet Island</option>
<option value="Brazil">Brazil</option>
<option value="British Indian Ocean Territory">British Indian Ocean Territory</option>
<option value="British Virgin Islands">British Virgin Islands</option>
<option value="Brunei">Brunei</option>
<option value="Bulgaria">Bulgaria</option>
<option value="Burkina Faso">Burkina Faso</option>
<option value="Burundi">Burundi</option>
<option value="Cambodia">Cambodia</option>
<option value="Cameroon">Cameroon</option>
<option selected='selected' value="Canada">Canada</option>
<option value="Cape Verde">Cape Verde</option>
<option value="Cayman Islands">Cayman Islands</option>
<option value="Central African Republic">Central African Republic</option>
<option value="Chad">Chad</option>
<option value="Chile">Chile</option>
<option value="China">China</option>
<option value="Christmas Island">Christmas Island</option>
<option value="Cocos [Keeling] Islands">Cocos [Keeling] Islands</option>
<option value="Colombia">Colombia</option>
<option value="Comoros">Comoros</option>
<option value="Cook Islands">Cook Islands</option>
<option value="Costa Rica">Costa Rica</option>
<option value="Croatia">Croatia</option>
<option value="Cuba">Cuba</option>
<option value="Curacao">Curacao</option>
<option value="Cyprus">Cyprus</option>
<option value="Czech Republic">Czech Republic</option>
<option value="Democratic Republic of the Congo">Democratic Republic of the Congo</option>
<option value="Denmark">Denmark</option>
<option value="Djibouti">Djibouti</option>
<option value="Dominica">Dominica</option>
<option value="Dominican Republic">Dominican Republic</option>
<option value="East Timor">East Timor</option>
<option value="Ecuador">Ecuador</option>
<option value="Egypt">Egypt</option>
<option value="El Salvador">El Salvador</option>
<option value="Equatorial Guinea">Equatorial Guinea</option>
<option value="Eritrea">Eritrea</option>
<option value="Estonia">Estonia</option>

<option value="Ethiopia">Ethiopia</option>
<option value="Falkland Islands">Falkland Islands</option>
<option value="Faroe Islands">Faroe Islands</option>
<option value="Fiji">Fiji</option>
<option value="Finland">Finland</option>
<option value="France">France</option>
<option value="French Guiana">French Guiana</option>
<option value="French Polynesia">French Polynesia</option>
<option value="French Southern Territories">French Southern Territories</option>
<option value="Gabon">Gabon</option>
<option value="Gambia">Gambia</option>
<option value="Georgia">Georgia</option>
<option value="Germany">Germany</option>
<option value="Ghana">Ghana</option>
<option value="Gibraltar">Gibraltar</option>
<option value="Greece">Greece</option>
<option value="Greenland">Greenland</option>
<option value="Grenada">Grenada</option>
<option value="Guadeloupe">Guadeloupe</option>
<option value="Guam">Guam</option>
<option value="Guatemala">Guatemala</option>
<option value="Guernsey">Guernsey</option>
<option value="Guinea">Guinea</option>
<option value="Guinea-Bissau">Guinea-Bissau</option>
<option value="Guyana">Guyana</option>
<option value="Haiti">Haiti</option>
<option value="Heard Island and McDonald Islands">Heard Island and McDonald Islands</option>
<option value="Honduras">Honduras</option>
<option value="Hong Kong">Hong Kong</option>
<option value="Hungary">Hungary</option>
<option value="Iceland">Iceland</option>
<option value="India">India</option>
<option value="Indonesia">Indonesia</option>
<option value="Iran">Iran</option>
<option value="Iraq">Iraq</option>
<option value="Ireland">Ireland</option>
<option value="Isle of Man">Isle of Man</option>
<option value="Israel">Israel</option>
<option value="Italy">Italy</option>
<option value="Ivory Coast">Ivory Coast</option>
<option value="Jamaica">Jamaica</option>
<option value="Japan">Japan</option>
<option value="Jersey">Jersey</option>
<option value="Jordan">Jordan</option>
<option value="Kazakhstan">Kazakhstan</option>
<option value="Kenya">Kenya</option>
<option value="Kiribati">Kiribati</option>
<option value="Kosovo">Kosovo</option>
<option value="Kuwait">Kuwait</option>
<option value="Kyrgyzstan">Kyrgyzstan</option>
<option value="Laos">Laos</option>
<option value="Latvia">Latvia</option>
<option value="Lebanon">Lebanon</option>
<option value="Lesotho">Lesotho</option>
<option value="Liberia">Liberia</option>
<option value="Libya">Libya</option>

<option value="Liechtenstein">Liechtenstein</option>
<option value="Lithuania">Lithuania</option>
<option value="Luxembourg">Luxembourg</option>
<option value="Macao">Macao</option>
<option value="Macedonia">Macedonia</option>
<option value="Madagascar">Madagascar</option>
<option value="Malawi">Malawi</option>
<option value="Malaysia">Malaysia</option>
<option value="Maldives">Maldives</option>
<option value="Mali">Mali</option>
<option value="Malta">Malta</option>
<option value="Marshall Islands">Marshall Islands</option>
<option value="Martinique">Martinique</option>
<option value="Mauritania">Mauritania</option>
<option value="Mauritius">Mauritius</option>
<option value="Mayotte">Mayotte</option>
<option value="Mexico">Mexico</option>
<option value="Micronesia">Micronesia</option>
<option value="Moldova">Moldova</option>
<option value="Monaco">Monaco</option>
<option value="Mongolia">Mongolia</option>
<option value="Montenegro">Montenegro</option>
<option value="Montserrat">Montserrat</option>
<option value="Morocco">Morocco</option>
<option value="Mozambique">Mozambique</option>
<option value="Myanmar [Burma]">Myanmar [Burma]</option>
<option value="Namibia">Namibia</option>
<option value="Nauru">Nauru</option>
<option value="Nepal">Nepal</option>
<option value="Netherlands">Netherlands</option>
<option value="New Caledonia">New Caledonia</option>
<option value="New Zealand">New Zealand</option>
<option value="Nicaragua">Nicaragua</option>
<option value="Niger">Niger</option>
<option value="Nigeria">Nigeria</option>
<option value="Niue">Niue</option>
<option value="Norfolk Island">Norfolk Island</option>
<option value="North Korea">North Korea</option>
<option value="Northern Mariana Islands">Northern Mariana Islands</option>
<option value="Norway">Norway</option>
<option value="Oman">Oman</option>
<option value="Pakistan">Pakistan</option>
<option value="Palau">Palau</option>
<option value="Palestine">Palestine</option>
<option value="Panama">Panama</option>
<option value="Papua New Guinea">Papua New Guinea</option>
<option value="Paraguay">Paraguay</option>
<option value="Peru">Peru</option>
<option value="Philippines">Philippines</option>
<option value="Pitcairn Islands">Pitcairn Islands</option>
<option value="Poland">Poland</option>
<option value="Portugal">Portugal</option>
<option value="Puerto Rico">Puerto Rico</option>
<option value="Qatar">Qatar</option>
<option value="Republic of the Congo">Republic of the Congo</option>
<option value="Runion">Runion</option>

<option value="Romania">Romania</option>
<option value="Russia">Russia</option>
<option value="Rwanda">Rwanda</option>
<option value="Saint Barthlemy">Saint Barthlemy</option>
<option value="Saint Helena">Saint Helena</option>
<option value="Saint Kitts and Nevis">Saint Kitts and Nevis</option>
<option value="Saint Lucia">Saint Lucia</option>
<option value="Saint Martin">Saint Martin</option>
<option value="Saint Pierre and Miquelon">Saint Pierre and Miquelon</option>
<option value="Saint Vincent and the Grenadines">Saint Vincent and the Grenadines</option>
<option value="Samoa">Samoa</option>
<option value="San Marino">San Marino</option>
<option value="So Tom and Prncipe">So Tom and Prncipe</option>
<option value="Saudi Arabia">Saudi Arabia</option>
<option value="Senegal">Senegal</option>
<option value="Serbia">Serbia</option>
<option value="Seychelles">Seychelles</option>
<option value="Sierra Leone">Sierra Leone</option>
<option value="Singapore">Singapore</option>
<option value="Sint Maarten">Sint Maarten</option>
<option value="Slovakia">Slovakia</option>
<option value="Slovenia">Slovenia</option>
<option value="Solomon Islands">Solomon Islands</option>
<option value="Somalia">Somalia</option>
<option value="South Africa">South Africa</option>
<option value="South Georgia and the South Sandwich Islands">South Georgia and the South Sandwich Islands</option>
<option value="South Korea">South Korea</option>
<option value="South Sudan">South Sudan</option>
<option value="Spain">Spain</option>
<option value="Sri Lanka">Sri Lanka</option>
<option value="Sudan">Sudan</option>
<option value="Suriname">Suriname</option>
<option value="Svalbard and Jan Mayen">Svalbard and Jan Mayen</option>
<option value="Swaziland">Swaziland</option>
<option value="Sweden">Sweden</option>
<option value="Switzerland">Switzerland</option>
<option value="Syria">Syria</option>
<option value="Taiwan">Taiwan</option>
<option value="Tajikistan">Tajikistan</option>
<option value="Tanzania">Tanzania</option>
<option value="Thailand">Thailand</option>
<option value="Togo">Togo</option>
<option value="Tokelau">Tokelau</option>
<option value="Tonga">Tonga</option>
<option value="Trinidad and Tobago">Trinidad and Tobago</option>
<option value="Tunisia">Tunisia</option>
<option value="Turkey">Turkey</option>
<option value="Turkmenistan">Turkmenistan</option>
<option value="Turks and Caicos Islands">Turks and Caicos Islands</option>
<option value="Tuvalu">Tuvalu</option>
<option value="U.S. Minor Outlying Islands">U.S. Minor Outlying Islands</option>
<option value="U.S. Virgin Islands">U.S. Virgin Islands</option>
<option value="Uganda">Uganda</option>
<option value="Ukraine">Ukraine</option>
<option value="United Arab Emirates">United Arab Emirates</option>
<option value="United Kingdom">United Kingdom</option>

<option value="United States">United States</option>
<option value="Uruguay">Uruguay</option>
<option value="USA">USA</option>
<option value="USA / Canada">USA / Canada</option>
<option value="Uzbekistan">Uzbekistan</option>
<option value="Vanuatu">Vanuatu</option>
<option value="Vatican City">Vatican City</option>
<option value="Venezuela">Venezuela</option>
<option value="Vietnam">Vietnam</option>
<option value="Wallis and Futuna">Wallis and Futuna</option>
<option value="Western Sahara">Western Sahara</option>
<option value="Yemen">Yemen</option>
<option value="Zambia">Zambia</option>
<option value="Zimbabwe">Zimbabwe</option>
</select>

<label class="control-label col-sm-3">State/ Province:</label>

<select name="op_state" required class="form-control op_states">
<option value="Alberta">Alberta</option>
<option value="British Columbia">British Columbia</option>
<option value="Manitoba">Manitoba</option>
<option value="New Brunswick">New Brunswick</option>
<option value="Newfoundland and Labrador">Newfoundland and Labrador</option>
<option value="Nova Scotia">Nova Scotia</option>
<option selected='selected' value="Ontario">Ontario</option>
<option value="Prince Edward Island">Prince Edward Island</option>
<option value="Quebec">Quebec</option>
<option value="Saskatchewan">Saskatchewan</option>
<option value="Northwest Territories">Northwest Territories</option>
<option value="Nunavut">Nunavut</option>
<option value="Yukon">Yukon</option>
</select>
<input type="text" name="txt_state" required class="form-control txt_state" style="display:none;" value="" />

<label class="control-label col-sm-3">Postal Code / Zip Code:</label>

<input type="text" name="zip_code" required class="form-control u_zip_code" value="" />

</fieldset>

<h3></h3>
<fieldset class="step p-l-0 m-t-10" id="step2" style="display: none;">

```
<div class="col-sm-11">
<div class="form-group">
<label class="control-label col-sm-3">Package:</label>
<div class="col-sm-7">

<select name="package_id" required class="form-control" id="up_package_id">
<optgroup label="Tier 1">

<option data-pid="14" data-pname="AMD Radeon RX 480/580 8GB (Linux Mint)" value="36">AMD Radeon RX 480/580 8GB (Linux Mint) ( $0.35 / h )</option>

<option data-pid="18" data-pname="Test111" value="41">Test111 ( $200.00 / h )</option>
</optgroup>
<optgroup label="Tier 2">

<option data-pid="15" data-pname="NVIDIA GEFORCE GTX 1070-1080 (Linux Mint)" value="37">NVIDIA GEFORCE GTX 1070-1080 (Linux Mint) ( $0.65 / h )</option>
</optgroup>
<optgroup label="Tier 3">

<option data-pid="12" data-pname="AMD 5700XT,6700XT,6800XT (Linux Mint)" value="35">AMD 5700XT,6700XT,6800XT (Linux Mint) ( $0.75 / h )</option>
</optgroup>

</select>
</div>
</div>
</div>
<input type="hidden" class="existing_package_cls" name="existing_package_id" value="" />
</div>
</fieldset>

<h3></h3>
<fieldset class="step p-l-0 m-t-10" id="step3" style="display: none;">
<div class="content cus-panel col-sm-12">
<div class="col-sm-9">
<!-- <div class="alert alert-primary cc_wrapper" style="display:none;" role="alert">
* IMPORTANT: 3 consecutive failed attempts will result in account suspension. Customer and Credit card information must be within the exact same address.
</div>-->
<div class="form-group">
<label class="control-label col-sm-3">Payment Type:</label>
<div class="col-sm-5">
<select name="payment_type" required class="form-control payment_type_cls" >
<option value="">Select One</option>
<option value="paypal">Paypal</option>
<option value="credit_card">Credit Card</option>
<option value="promo_code">Promo Code</option>
</select>
</div>
</div>

<div class="promo_code_wrapper" style="display:none;">
<div class="form-group">
<label class="control-label col-sm-3">Enter Promo Code:</label>
<div class="col-sm-5">
<input type="text" name="promo_code" required class="form-control promo_code_cls" value="" />
</div>
</div>
</div>
```

```
<div class="cc_wrapper" style="display:none;">
<div class="form-group">
<label class="control-label col-sm-3">Name of card holder:</label>
<div class="col-sm-5">
<input type="text" name="card_on_name" required class="form-control u_card_on_name" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Credit Card type:</label>
<div class="col-sm-5">
<select name="card_type" required class="form-control u_card_type">
<option value="Visa">Visa</option>
<option value="MasterCard">MasterCard</option>
</select>
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Credit card number:</label>
<div class="col-sm-5">
<input type="text" id="u_ccnumber" name="ccnumber" maxlength="16" required class="form-control u_ccnumber" value="" />
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3" >Expiration month /year:</label>
<div class="col-sm-5">
<div class="controls cc-ym-wrapper">
<div class="col-sm-6 p-l-0">
<select name="ccmonth" required class="form-control u_ccmonth">
<option value="">Month </option>
<option value="1">1</option>
<option value="2">2</option>
<option value="3">3</option>
<option value="4">4</option>
<option value="5">5</option>
<option value="6">6</option>
<option value="7">7</option>
<option value="8">8</option>
<option value="9">9</option>
<option value="10">10</option>
<option value="11">11</option>
<option value="12">12</option>

</select>
</div>
<div class="col-sm-6 p-r-0">
<select name="ccyear" required class="form-control u_ccyear col-sm-4">
<option value="">Year</option>
<option value="2022">2022</option>
<option value="2023">2023</option>
<option value="2024">2024</option>
<option value="2025">2025</option>
<option value="2026">2026</option>
<option value="2027">2027</option>
<option value="2028">2028</option>
```

<option value="2029">2029</option>
<option value="2030">2030</option>
<option value="2031">2031</option>
<option value="2032">2032</option>
<option value="2033">2033</option>
</select>

<label class="control-label col-sm-3">CVC code:</label>

<input type="text" name="ccvc" required class="form-control u_ccvc" value="" />

<label class="control-label col-sm-3">Amount:</label>

<select name="amount" required class="form-control cc_amount_opt">
<option value="20">$20</option>
<option value="30">$30</option>
<option value="50">$50</option>
<option value="other">Other (Min $5)</option>
</select>

<label class="control-label col-sm-3"> </label>

<input type="text" name="other_amount" required class="form-control other_amount_cls" placeholder="Amount" value="5" >

</fieldset>
<h3></h3>
<fieldset class="step p-l-0" id="step4" style="display: none;">

Note : this account will automatically be terminated with days if no new funds are added within that period.

<h3>Customer Info</h3>

<label class="control-label col-sm-3">Name:</label>

```
<div class="form-group">
<label class="control-label col-sm-3">Phone:</label>
<div class="col-sm-9">
<span class="summ_phone"></span>
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Email:</label>
<div class="col-sm-9">
<span class="summ_email"></span>
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Address:</label>
<div class="col-sm-9">
<span class="summ_address"></span>
</div>
</div>
</div>


<div class="col-sm-6">
<h3>Package Info</h3>
<div class="form-group">
<label class="control-label col-sm-5">Packages:</label>
<div class="col-sm-6">
<span class="summ_package"></span>
</div>
</div>
<h3>Payment Detail</h3>
<div class="form-group">
<label class="control-label col-sm-5">Payment Type:</label>
<div class="col-sm-6">
<span class="summ_payment"></span>
</div>
</div>

<div class="u_promo_wrapper" style="display:none;">
<div class="form-group" >
<label class="control-label col-sm-5">Promo Name:</label>
<div class="col-sm-6">
<span class="summ_promo_name"></span>
</div>
</div>
</div>
<div class="u_credit_wrapper" style="display:none;">
<div class="form-group" >
<label class="control-label col-sm-5">Name of card holder:</label>
<div class="col-sm-6">
<span class="summ_card_on_name"></span>
</div>
</div>
<div class="form-group" >
<label class="control-label col-sm-5">Credit Card type:</label>
<div class="col-sm-6">
<span class="summ_card_type"></span>
```

```
</div>
</div>
<div class="form-group" >
<label class="control-label col-sm-5">Credit card number:</label>
<div class="col-sm-6">
<span class="summ_ccnumber"></span>
</div>
</div>
<div class="form-group" >
<label class="control-label col-sm-5">Expiration month /year:</label>
<div class="col-sm-6">
<span class="summ_ccmonth_year"></span>
</div>
</div>
<div class="form-group" >
<label class="control-label col-sm-5">CVC code:</label>
<div class="col-sm-6">
<span class="summ_u_ccvc"></span>
</div>
</div>

</div>
<div class="amount_wrapper" style="display:none;">
<div class="form-group" >
<label class="control-label col-sm-5">Amount:</label>
<div class="col-sm-6">
<span class="summ_amount"></span>
</div>
</div>
</div>
<div class="tax_wrapper" style="display:none;">
<div class="form-group" >
<label class="control-label col-sm-5">Tax (<span class="summ_tax_per"></span>) :</label>
<div class="col-sm-6">
<span class="summ_tax"></span>
</div>
</div>
<div class="form-group" >
<label class="control-label col-sm-5"><b>Total Amount:</b></label>
<div class="col-sm-6">
<span class="summ_total_amount"></span>
</div>
</div>
</div>
</div>
</div>
<div class="col-sm-12">
<div class="upgrade_frm_action form-group">
<div class="paypal_wrapper" style="display:none;">
<!--<div id="paypal-button-container"></div>-->
<div><a class="btn btn-frm-submit paypal-checkout" href=&apos;javascript:void(0)&apos;> <img style="height: 38px;margin-top: -10px;" src="https://order.
maximumsettings.com/assets/images/paypal.png" /> </a></div>
<div><a href="javascript:void(0);" onclick="location.reload();" class="btn btn-default btn-cancel">Cancel</a></div>
</div>
<div class="cc_pay_wrapper" style="display:none;">
<div><button type="submit" id="upgrade_btn" class="btn btn-theme btn-frm-submit">Pay Now</button></div>
```

Cancel

<button type="submit" id="promo_btn" class="btn btn-theme btn-frm-submit">Place Order</button>
Cancel

</fieldset>
</form>

<h2 class="nt_ch_1541650940591 poppins capitalize fw-300 mb-5 vc_custom_heading">Need Help ?</h2>

<h2>Join Us On Discord</h2>

<h5 class="modal-title text-center blue_background" id="otp_modal_label">PAID ACCOUNTS</h5>

<h2>Not Yet Available.
Please try again later.</h2>

<button type="button" class="btn btn-secondary close_button" data-dismiss="modal">Close</button>

```
</div>
</div>
</div>
</div> <div class="modal fade" id="otp_modal" tabindex="-1" role="dialog" aria-labelledby="otp_modal_label" aria-hidden="true" data-backdrop="static" data-keyboard="
false">
<div class="modal-dialog" role="document">
<div class="modal-content">
<div class="modal-header">
<h5 class="modal-title text-center blue_background" id="otp_modal_label">Code Sent via SMS</h5>
<button type="button" class="close close_button" data-dismiss="modal" aria-label="Close" onClick=&amp;apos;location.reload();&amp;apos;>
<span aria-hidden="true">&amp;times;</span>
</button>
</div>
<div class="modal-body">
<div class="modal-body-content">
<div class="row">
<div class="col-md-12">
<input type="hidden" id="verification_step" value="1">
<div class="form-group">
<label>Enter Code : </label>
<span class="otp_input">
<input type="text" name="otp" id="otp_input_val" value=&amp;apos;&amp;apos; size="40" class="form-control" placeholder="Enter the code" maxlength="6">
</span>
<span id="verification_error"></span>
<!--<p class="m-t-10 not_received_link">Not Received? <a href="#" onclick="callToPhone(event);">Click here</a></p>-->
</div>
</div>
</div>
</div>
</div>
<div class="modal-footer">
<!--<button type="button" class="btn btn-secondary close_button" data-dismiss="modal" onClick=&amp;apos;location.reload();&amp;apos;>Close</button>-->
<button type="button" class="btn btn-secondary close_button" data-dismiss="modal">Close</button>
<input type="button" name=&amp;apos;sub&amp;apos; id=&amp;apos;otp_submit&amp;apos; value="Next" class="submit-btn btn btn-primary"><span class="ajax-loader"></span><span
name=target id=target></span>
</div>
</div>
</div>
</div> <div class="modal fade modal_sign_up" tabindex="-1" role="dialog" aria-labelledby="signup_modal_label" aria-hidden="true" data-keyboard="false">
<div class="modal-dialog" role="document">
<div class="modal-content">
<div class="modal-header">
<h3 class="modal-title">Trial Accounts</h3>
</div>
<div class="modal-body">
<h4>IMPORTANT</h4>
<div class="martop10">
Dear Potential Customer,<br>
<div class="martop10">This trial service is only available in the United States and Canada. Furthermore, you will require a physical address to obtain a trial activation
code. We will be sending a valid code through your local post office such as Canada Post/ Fedex / DHL/ etc. Only accounts with valid phone numbers are valid. Services
like Text NOW or similar voip services will be rejected and address details automatically banned.</div>
<div class="martop10"><br><b><h4>Note: Trial activation code will <a style="color:red;"><u>NOT</u></a> be sent by Email.</h4></b></div>
<div class="martop10"><br>Paid accounts can be started for as little as $5 and are available in most parts of the world. If you are not located within Canada and the
United states, you can still use Maximumsettings via the regular paid process. If you wish to continue with a Trial activation please click continue otherwise, you can click "
Paid Account Please " and get started within just a few minutes. </div>
<div class="martop10"><u>Limited Time Offer:</u></div>
```

Paid accounts will automatically get an additional $35 credit with any purchase
Thank you
Maximum Settings.

<button type="button" class="btn circle btn-theme btn-sm paid_account">Paid Account Please</button>
<button type="button" class="btn circle btn-theme border btn-sm continue_trial">Continue To Trial</button>

<footer class="bg-light">

 Copyright 2022. All Rights Reserved by Maximum Settings

<li id="menu-item-511" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-511">Terms of user
<li id="menu-item-512" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-512">License
<li id="menu-item-513" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-513">Support

</footer>
<script src="https://canvasjs.com/assets/script/jquery-1.11.1.min.js"></script>
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/bootstrap.min.js'></script>

<script type="text/javascript" src="https://order.maximumsettings.com/assets/js/datatables/datatables.min.js"></script>

<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/bootstrap-datepicker.js'></script>

<script type='text/javascript' src="https://order.maximumsettings.com/assets/js/jquery.steps.js"></script>
<script type='text/javascript' src="https://order.maximumsettings.com/assets/js/jquery.validate.js"></script>
<script type='text/javascript' src="https://order.maximumsettings.com/assets/js/sweetalert2.min.js"></script>
<script type='text/javascript' src="https://order.maximumsettings.com/assets/js/form.min.js"></script>

<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/bootsnav.js'></script>
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/order.js?t=6381192cca07d'></script>
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/trial.js?t=6381192cca085'></script>

<script src="https://canvasjs.com/assets/script/jquery.canvasjs.min.js"></script>
<script src="https://code.highcharts.com/highcharts.js"></script>
<script src="https://code.highcharts.com/modules/series-label.js"></script>
<script src="https://code.highcharts.com/modules/exporting.js"></script>
<script src="https://code.highcharts.com/modules/export-data.js"></script>
<script src="https://canvasjs.com/assets/script/jquery.canvasjs.min.js"></script>

<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/select2.min.js'></script>
<script type='text/javascript' src='https://order.maximumsettings.com/assets/js/jquery.overlayScrollbars.js'></script>
<!--<script type='text/javascript' src='js/bootstrap-datetimepicker.js'></script>-->
<!--<script src="https://www.paypal.com/sdk/js?client-id=AdxTCDDviKQ4NfGkev7ZHmb6dpcARIMXdWiLdkFWAYpwUnNmWbs6HIFQYla0yrYi227svx1cN4J3HkBF&currency=USD"></script>-->

<script src="//www.paypalobjects.com/api/checkout.js"></script>
<script src="https://www.paypal.com/sdk/js?client-id=AXCYoBHG6D0aLrR8_-C8M5J6CT1rvQPPb7H16kP0h994jDOGITw1ufMaqLNZiCTmEkwFWSBPXoDBHzeN&currency=CAD" data-namespace="paypal_sdk"></script>

<script>var env = 'production';</script> <!-- // sandbox | production -->
<script>var client_sandbox = 'AXCYoBHG6D0aLrR8_-C8M5J6CT1rvQPPb7H16kP0h994jDOGITw1ufMaqLNZiCTmEkwFWSBPXoDBHzeN';</script>
<script>var client_production = 'AbVx2eNpll12ZAblvXX9lzPUhkceBr43Z2j3pl280MyQ_THe9FZomXD9lbmEQ8LtWqcN2ObbZPaoJx1d';</script>
<script>var canada_quebec_rate = '14.795';</script>
<script>var canada_wide_rate = '13';</script>

</body>
</html>
GET / HTTP/1.0
Host: orders.maximumsettings.com

<!DOCTYPE html>
<html class="no-js" lang="en">
<head>
<base href="https://orders.maximumsettings.com/">
<meta content="charset=utf-8">
<title>Maximum Settings – Dedicated Game Streaming</title>
<meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<meta name="viewport" content="width=device-width, initial-scale=1">
<base href="https://orders.maximumsettings.com/">
<script type="text/javascript">
var site_url = "https://orders.maximumsettings.com/";
var base_url = "https://orders.maximumsettings.com/";
var show_setting_popup = '';
var security_check = '1';
var iframe_url = '';
var ip_add = '64.39.98.151';
</script>

<link rel='dns-prefetch' href='http://fonts.googleapis.com/' />
<link rel='dns-prefetch' href='http://s.w.org/' />

<link rel='stylesheet' id='softing-fonts-css' href='//fonts.googleapis.com/css?family=Open%2BSans%7CPoppins%3A400%2C500%2C600%2C700%2C800&subset=latin%2Clatin-ext&ver=1.0' type='text/css' media='all' />
<link rel="stylesheet" href="https://orders.maximumsettings.com/assets/css/all.css" integrity="sha384-50oBUHEmvpQ+1lW4y57PTFmhCaXp0ML5d60M1M7uH2+nqUivzIebhndOJK28anvf" crossorigin="anonymous">

<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">

<link rel="alternate" type="application/rss+xml" title="Maximum Settings » Feed" href="indexd784.html?feed=rss2" />
<link rel="alternate" type="application/rss+xml" title="Maximum Settings » Comments Feed" href="indexa6da.html?feed=comments-rss2" />
<link rel='stylesheet' id='wp-block-library-css' href='https://orders.maximumsettings.com/assets/css/style.css' type='text/css' media='all' />
<link rel='stylesheet' id='wp-block-library-css' href='https://orders.maximumsettings.com/assets/css/custom.css' type='text/css' media='all' />

<link rel='stylesheet' id='wp-block-library-css' href='https://orders.maximumsettings.com/assets/css/bootstrap.min.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://orders.maximumsettings.com/assets/css/sweetalert2.min.css' type='text/css'/>
<link rel='stylesheet' href='https://orders.maximumsettings.com/assets/css/select2.min.css' type='text/css'/>
<link rel='stylesheet' id='bootsnav-css' href='https://orders.maximumsettings.com/assets/css/bootsnav.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://cdn.datatables.net/1.10.19/css/jquery.dataTables.min.css' type='text/css' media='all' />
<link rel='stylesheet' href='https://orders.maximumsettings.com/assets/css/OverlayScrollbars.css' type='text/css' media='all' />
<link rel="stylesheet" href="https://orders.maximumsettings.com/assets/css/datepicker.css" />

<script type='text/javascript' src='https://orders.maximumsettings.com/assets/js/jquery.js'></script>

</head>

<body class="">
<!-- Preloader Start -->
<!--<div class="se-pre-con"></div>-->
<!-- Preloader Ends -->
<!-- Header
=== -->
<header id="home" class="nt-site-header">
<!-- Start Navigation -->
<nav class="navbar navbar-default navbar-sticky bootsnav on no-full has-background">
 <!-- Start Atribute Navigation -->

<li class="attr-nav-li-one">
Order Now

<li class="attr-nav-li-two">
Login

<!-- End Atribute Navigation -->

<!-- Start Header Navigation -->

<button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#navbar-menu">

</button>

<!-- sticky logo -->

<!-- End Header Navigation -->

<!-- Collect the nav links, forms, and other content for toggling -->

<ul class="nav navbar-nav navbar-right" data-in="#" data-out="#">
<li id="menu-item-804" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-804"><a href="
http://maximumsettings.com#home" class="scroll">Home
<li id="menu-item-806" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-806"><a href="
http://maximumsettings.com/?author=1" class="scroll">Latest News
<li id="menu-item-807" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-807"><a href="
http://maximumsettings.com#pricing" class="scroll">Pricing
<li id="menu-item-808" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-808"><a href="
http://maximumsettings.com#faq" class="scroll">Faq’s
<li id="menu-item-811" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-811"><a href="
http://maximumsettings.com#features" class="scroll">Features
<li id="menu-item-809" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-809"><a href="
https://community.maximumsettings.com" class="scroll" target="_blank">Community
<li id="menu-item-810" class="menu-item menu-item-type-custom menu-item-object-custom current-menu-item current_page_item menu-item-810"><a href="
http://maximumsettings.com#contact" class="scroll">Support

<!-- /.navbar-collapse -->

</nav>
<!-- End Navigation -->

</header>
<!-- End Header -->

<h2>Account Creation</h2>

<li class="pricing-header"><h4 class="f30">PAID ACCOUNTS</h4> (Instant Activation)

<li class="footer">
Order Now


```
<div style="clear: both;"></div>
<br>
</div>
<div style="display: none;" class="paid_register_content nt-column col-sm-12 col-lg-12 col-md-12 nt_col-has-responsive-data">
<div class="panel panel-blue">
<div class="panel-heading">ACCOUNT CREATION</div>
<div class="panel-body">
<div class="">
<div class="nt-wrapper "><h2 class="capitalize fw-600 mb-30 "></h2>
<div role="form" class="wpcf7" id="wpcf7-f608-p654-o2" lang="en-US" dir="ltr">
<div class="error_msg_div"></div>
<form class="form-basic purchase_package form-horizontal" method="post" id="frm_upgrade" action="#" name="package-info-form">
<h3></h3>
<fieldset class="step p-l-0 m-t-10" id="step1">
<div class="content cus-panel col-sm-12 account_info_block">
<div class="col-sm-6">
<div class="form-group">
<label class="control-label col-sm-3">Name:</label>
<div class="col-sm-9">
<input type="text" name="name" required class="form-control u_name" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Phone :</label>
<div class="col-sm-9">
<input type="text" name="phone" required class="form-control u_phone" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Email :</label>
<div class="col-sm-9">
<input type="text" name="email" required class="form-control u_email" value="" />
</div>
</div>
<div class="form-group">
<label class="control-label col-sm-3">Confirm Email :</label>
<div class="col-sm-9">
<input type="text" name="confirm_email" required class="form-control" value="" />
</div>
</div>
</div>
<div class="col-sm-6">
<div class="form-group">
<label class="control-label col-sm-3">Address:</label>
<div class="col-sm-9">
<textarea name="address" required class="form-control u_address"></textarea>
</div>
</div>

<div class="form-group">
<label class="control-label col-sm-3">City:</label>
<div class="col-sm-9">
<input type="text" name="city" required class="form-control u_city" value="" />
</div>
```

```
</div>

<div class="form-group">
<label class="control-label col-sm-3">Country:</label>
<div class="col-sm-9">
<select name="country" required class="form-control up_country_op">
<option value="Afghanistan">Afghanistan</option>
<option value="land">land</option>
<option value="Albania">Albania</option>
<option value="Algeria">Algeria</option>
<option value="American Samoa">American Samoa</option>
<option value="Andorra">Andorra</option>
<option value="Angola">Angola</option>
<option value="Anguilla">Anguilla</option>
<option value="Antarctica">Antarctica</option>
<option value="Antigua and Barbuda">Antigua and Barbuda</option>
<option value="Argentina">Argentina</option>
<option value="Armenia">Armenia</option>
<option value="Aruba">Aruba</option>
<option value="Australia">Australia</option>
<option value="Austria">Austria</option>
<option value="Azerbaijan">Azerbaijan</option>
<option value="Bahamas">Bahamas</option>
<option value="Bahrain">Bahrain</option>
<option value="Bangladesh">Bangladesh</option>
<option value="Barbados">Barbados</option>
<option value="Belarus">Belarus</option>
<option value="Belgium">Belgium</option>
<option value="Belize">Belize</option>
<option value="Benin">Benin</option>
<option value="Bermuda">Bermuda</option>
<option value="Bhutan">Bhutan</option>
<option value="Bolivia">Bolivia</option>
<option value="Bonaire">Bonaire</option>
<option value="Bosnia and Herzegovina">Bosnia and Herzegovina</option>
<option value="Botswana">Botswana</option>
<option value="Bouvet Island">Bouvet Island</option>
<option value="Brazil">Brazil</option>
<option value="British Indian Ocean Territory">British Indian Ocean Territory</option>
<option value="British Virgin Islands">British Virgin Islands</option>
<option value="Brunei">Brunei</option>
<option value="Bulgaria">Bulgaria</option>
<option value="Burkina Faso">Burkina Faso</option>
<option value="Burundi">Burundi</option>
<option value="Cambodia">Cambodia</option>
<option value="Cameroon">Cameroon</option>
<option selected=&apos;selected&apos; value="Canada">Canada</option>
<option value="Cape Verde">Cape Verde</option>
<option value="Cayman Islands">Cayman Islands</option>
<option value="Central African Republic">Central African Republic</option>
<option value="Chad">Chad</option>
<option value="Chile">Chile</option>
<option value="China">China</option>
<option value="Christmas Island">Christmas Island</option>
<option value="Cocos [Keeling] Islands">Cocos [Keeling] Islands</option>
<option value="Colombia">Colombia</option>
```

<option value="Comoros">Comoros</option>
<option value="Cook Islands">Cook Islands</option>
<option value="Costa Rica">Costa Rica</option>
<option value="Croatia">Croatia</option>
<option value="Cuba">Cuba</option>
<option value="Curacao">Curacao</option>
<option value="Cyprus">Cyprus</option>
<option value="Czech Republic">Czech Republic</option>
<option value="Democratic Republic of the Congo">Democratic Republic of the Congo</option>
<option value="Denmark">Denmark</option>
<option value="Djibouti">Djibouti</option>
<option value="Dominica">Dominica</option>
<option value="Dominican Republic">Dominican Republic</option>
<option value="East Timor">East Timor</option>
<option value="Ecuador">Ecuador</option>
<option value="Egypt">Egypt</option>
<option value="El Salvador">El Salvador</option>
<option value="Equatorial Guinea">Equatorial Guinea</option>
<option value="Eritrea">Eritrea</option>
<option value="Estonia">Estonia</option>
<option value="Ethiopia">Ethiopia</option>
<option value="Falkland Islands">Falkland Islands</option>
<option value="Faroe Islands">Faroe Islands</option>
<option value="Fiji">Fiji</option>
<option value="Finland">Finland</option>
<option value="France">France</option>
<option value="French Guiana">French Guiana</option>
<option value="French Polynesia">French Polynesia</option>
<option value="French Southern Territories">French Southern Territories</option>
<option value="Gabon">Gabon</option>
<option value="Gambia">Gambia</option>
<option value="Georgia">Georgia</option>
<option value="Germany">Germany</option>
<option value="Ghana">Ghana</option>
<option value="Gibraltar">Gibraltar</option>
<option value="Greece">Greece</option>
<option value="Greenland">Greenland</option>
<option value="Grenada">Grenada</option>
<option value="Guadeloupe">Guadeloupe</option>
<option value="Guam">Guam</option>
<option value="Guatemala">Guatemala</option>
<option value="Guernsey">Guernsey</option>
<option value="Guinea">Guinea</option>
<option value="Guinea-Bissau">Guinea-Bissau</option>
<option value="Guyana">Guyana</option>
<option value="Haiti">Haiti</option>
<option value="Heard Island and McDonald Islands">Heard Island and McDonald Islands</option>
<option value="Honduras">Honduras</option>
<option value="Hong Kong">Hong Kong</option>
<option value="Hungary">Hungary</option>
<option value="Iceland">Iceland</option>
<option value="India">India</option>
<option value="Indonesia">Indonesia</option>
<option value="Iran">Iran</option>
<option value="Iraq">Iraq</option>
<option value="Ireland">Ireland</option>

<option value="Isle of Man">Isle of Man</option>
<option value="Israel">Israel</option>
<option value="Italy">Italy</option>
<option value="Ivory Coast">Ivory Coast</option>
<option value="Jamaica">Jamaica</option>
<option value="Japan">Japan</option>
<option value="Jersey">Jersey</option>
<option value="Jordan">Jordan</option>
<option value="Kazakhstan">Kazakhstan</option>
<option value="Kenya">Kenya</option>
<option value="Kiribati">Kiribati</option>
<option value="Kosovo">Kosovo</option>
<option value="Kuwait">Kuwait</option>

Results were truncated

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:	2006-07-27 21:45:19.0

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.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

IP ID changes observed (network order) for port 443: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 33 milli seconds

List of Web Directories — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

THREAT:

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

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Directory Source

/images/ brute force
/assets/ brute force
/assets/images/ brute force
/orders/ brute force
/Orders/ brute force
/application/ brute force
/assets/ web page
/assets/css/ web page
/assets/images/ web page
/assets/js/ web page
/index.php brute force
/icons/ brute force
/orders/ web page
/Orders/ web page

Open TCP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-06-15 18:32:21.0

THREAT:

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

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

IMPACT:

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

SOLUTION:

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

RESULT:

Port IANA Assigned Ports/Services Description Service Detected OS On Redirected Port

443 https http protocol over TLS/SSL http over ssl

SSL Session Caching Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous

connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is enabled on the target.

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

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

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

SOLUTION:
N/A

RESULT:
The network handle is: CANACA-COM
Network description:
Canaca-com 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:	2013-09-27 19:31:33.0

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

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

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

SOLUTION:
N/A

RESULT:
The ISP network handle is: COGENT-A
ISP Network description:
PSINet, Inc.

HTTP Response Method and Header Information Collected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

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

IMPACT:
N/A
SOLUTION:
N/A
RESULT:
HTTP header and method information collected on port 443.

GET / HTTP/1.0
Host: orders.maximumsettings.com

HTTP/1.1 200 OK
Date: Fri, 25 Nov 2022 20:44:56 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Set-Cookie: ci_session=ae4455f018teou242l98ja8gi0ioi2n9; expires=Fri, 25-Nov-2022 20:54:56 GMT; Max-Age=600; path=/; HttpOnly;HttpOnly;Secure;SameSite=Strict
Connection: close
Content-Type: text/html; charset=UTF-8

Links Crawled — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 9.00
Number of links: 4
(This number excludes form requests and links re-requested during authentication.)

https://order.maximumsettings.com/
https://order.maximumsettings.com/indexa6da.html?feed=comments-rss2
https://order.maximumsettings.com/indexd784.html?feed=rss2
https://order.maximumsettings.com/js/bootstrap-datetimepicker.js

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2003-05-09 18:28:51.0

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Hops IP Round Trip Time Probe
Port
1 139.87.10.2 0.09ms ICMP
2 4.15.10.202 0.57ms ICMP
3 4.15.10.201 0.97ms ICMP
4 4.69.219.218 2.19ms ICMP
5 *.*.*.* 0.00ms Other 443
6 154.54.28.145 1.93ms ICMP
7 154.54.42.78 9.84ms ICMP
8 154.54.87.65 10.66ms ICMP
9 154.54.87.30 30.57ms ICMP

10 154.54.31.90 34.26ms ICMP
11 154.54.44.170 45.06ms ICMP
12 154.54.7.130 56.51ms ICMP
13 154.54.31.234 62.48ms ICMP
14 38.111.102.68 64.37ms ICMP
15 66.49.252.119 64.82ms TCP 443

Links Crawled — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 8.00
Number of links: 4
(This number excludes form requests and links re-requested during authentication.)

https://orders.maximumsettings.com/
https://orders.maximumsettings.com/indexa6da.html?feed=comments-rss2
https://orders.maximumsettings.com/indexd784.html?feed=rss2
https://orders.maximumsettings.com/js/bootstrap-datetimepicker.js

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

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

Web Server Version — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Apache

ICMP Replies Received

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2003-01-16 20:14:30.0

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.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

ICMP Reply Type Triggered By Additional Information
Echo (type=0 code=0) Echo Request Echo Reply
Time Stamp (type=14 code=0) Time Stamp Request 19:24:24
GMT

HTTP Response Method and Header Information Collected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

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

IMPACT:
N/A

SOLUTION:
N/A

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

GET / HTTP/1.0
Host: order.maximumsettings.com

HTTP/1.1 200 OK
Date: Fri, 25 Nov 2022 19:36:12 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Set-Cookie: ci_session=n42ba10tkmmlbamoc4glo6is8a6nd14m; expires=Fri, 25-Nov-2022 19:46:12 GMT; Max-Age=600; path=/; HttpOnly;HttpOnly;Secure; SameSite=Strict
Connection: close
Content-Type: text/html; charset=UTF-8

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

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

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

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

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

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

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

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:
https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css
https://www.paypal.com/sdk/js?client-id=AXCYoBHG6D0aLrR8_-C8M5J6CT1rvQPPb7H16kP0h994jDOGITw1ufMaqLNZiCTmEkwFWSBPXoDBHzeN&currency=CAD
https://www.paypal.com/sdk/js?client-id=AdxTCDDviKQ4NfGkev7ZHmb6dpcARIMXdWiLdkFWAYpwUnNmWbs6HIFQYla0yrYi227svx1cN4J3HkBF&currency=USD
https://www.paypalobjects.com/api/checkout.js
https://cdn.datatables.net/1.10.19/css/jquery.dataTables.min.css
https://code.highcharts.com/highcharts.js
https://code.highcharts.com/modules/export-data.js
https://code.highcharts.com/modules/exporting.js
https://code.highcharts.com/modules/series-label.js
https://community.maximumsettings.com/

IP based excluded links:

Server Returns HTTP 4XX Error Code During Scanning — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150528
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-11-21 19:33:11.0

THREAT:
During the WAS scan, links with HTTP 4xx response code were observed and these are listed in the Results section. The HTTP 4xx message indicates a client error. The list of supported 4xx response code are as below:

400 - Bad Request
401 - Unauthorized
403 - Forbidden
404 - Not Found
405 - Method Not Allowed
407 - Proxy Authentication Required
408 - Request Timeout
413 - Payload Too Large
414 - URI Too Long

IMPACT:
The presence of a HTTP 4xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depends on responses to detect many vulnerabilities if the link does not respond with an expected response then any vulnerabilities present on such links may not be detected.

SOLUTION:
Review each link to determine why the client encountered an error while requesting the link. Additionally review and investigate the results of QID 150042 which lists 5xx errors, QID 150019 which lists unexpected response codes and QID 150097 which lists a potential blocked request.

RESULT:
Number of links with 4xx response code: 3
(Only first 50 such links are listed)

404 https://order.maximumsettings.com/indexa6da.html?feed=comments-rss2
404 https://order.maximumsettings.com/indexd784.html?feed=rss2
404 https://order.maximumsettings.com/js/bootstrap-datetimepicker.js

List of Web Directories — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

THREAT:

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

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Directory Source

/images/ brute force
/assets/ brute force
/assets/images/ brute force
/orders/ brute force
/Orders/ brute force
/application/ brute force
/index.php brute force
/icons/ brute force
/assets/ web page
/assets/css/ web page
/assets/images/ web page
/assets/js/ web page
/orders/ web page
/Orders/ web page

Cookies Collected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150028
Category:	Web Application
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:46:27.0

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

IMPACT:
Cookies may potentially contain sensitive information about the user.

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

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

RESULT:
Total cookies: 1
ci_session=aevqoh5bev8av1l56nl2anurkemkg72k; expires=Fri Nov 25 19:36:10 2022; path=/; domain=orders.maximumsettings.com; SameSite=SameSite=Strict; max-age=594; secure; httponly

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-11-19 21:53:59.0

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Average change between subsequent TCP initial sequence numbers is 1116584880 with a standard deviation of 536791857. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5103 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

HTTP Public-Key-Pins Security Header Not Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.0
Host: orders.maximumsettings.com

Host Scan Time - Scanner

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Scan duration: 9938 seconds

Start time: Fri, Nov 25 2022, 19:24:34 GMT

End time: Fri, Nov 25 2022, 22:10:12 GMT

Server Returns HTTP 4XX Error Code During Scanning — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150528
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-11-21 19:33:11.0

THREAT:
During the WAS scan, links with HTTP 4xx response code were observed and these are listed in the Results section. The HTTP 4xx message indicates a client error. The list of supported 4xx response code are as below:

400 - Bad Request
401 - Unauthorized
403 - Forbidden
404 - Not Found
405 - Method Not Allowed
407 - Proxy Authentication Required
408 - Request Timeout
413 - Payload Too Large
414 - URI Too Long

IMPACT:
The presence of a HTTP 4xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depends on responses to detect many vulnerabilities if the link does not respond with an expected response then any vulnerabilities present on such links may not be detected.

SOLUTION:
Review each link to determine why the client encountered an error while requesting the link. Additionally review and investigate the results of QID 150042 which lists 5xx errors, QID 150019 which lists unexpected response codes and QID 150097 which lists a potential blocked request.

RESULT:
Number of links with 4xx response code: 3
(Only first 50 such links are listed)

404 https://orders.maximumsettings.com/indexa6da.html?feed=comments-rss2
404 https://orders.maximumsettings.com/indexd784.html?feed=rss2
404 https://orders.maximumsettings.com/js/bootstrap-datetimepicker.js

Referrer-Policy HTTP Security Header Not Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:26.0

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

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

QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

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

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

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

RESULT:
Referrer-Policy HTTP Header missing on 443 port.

Cookies Collected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150028
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:46:27.0

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

IMPACT:
Cookies may potentially contain sensitive information about the user.

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

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

RESULT:
Total cookies: 1
ci_session=6t7ju6kdld0hqba8ddr2p0am2q2a1ok0; expires=Fri Nov 25 19:35:33 2022; path=/; domain=order.maximumsettings.com; SameSite=SameSite=Strict; max-age=594; secure; httponly

Scan Diagnostics — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:

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

IMPACT:

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

SOLUTION:

No action is required.

RESULT:

Target web application page https://orders.maximumsettings.com/ fetched. Status code:200, Content-Type:text/html, load time:409 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 3 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 28 links overall in 0 hours 0 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 3) + files:(0 x 4) + directories:(9 x 6) + paths:(0 x 10) = total (54)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 10 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 36 requests, 0 seconds. Completed 36 requests of 54 estimated requests (66.6667%). All tests completed.
WSEnumeration no tests enabled.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (95 tests, 1 inputs)
Batch #1 URI parameter manipulation (no auth): 95 vulnsigs tests, completed 83 requests, 2 seconds. Completed 83 requests of 95 estimated requests (87.3684%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 1 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 16 requests, 0 seconds. Completed 16 requests of 24 estimated requests (66.6667%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 1 inputs)
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 14 requests, 1 seconds. Completed 14 requests of 14 estimated requests (100%). All tests completed.
Time based tests for Apache Struts Vulnerabilities - no tests enabled.
Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (95 tests, 1 inputs)
Batch #2 URI parameter manipulation (no auth): 95 vulnsigs tests, completed 83 requests, 1 seconds. Completed 83 requests of 95 estimated requests (87.3684%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 1 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 16 requests, 1 seconds. Completed 16 requests of 24 estimated requests (66.6667%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 1 inputs)
Batch #2 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 14 requests, 1 seconds. Completed 14 requests of 14 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 1 minute (107 tests, 1 inputs)
Batch #4 WebCgiOob: 107 vulnsigs tests, completed 54 requests, 1 seconds. Completed 54 requests of 1190 estimated requests (4.53782%). All tests completed.
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, 4 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 4 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 1 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 72 requests, 2 seconds. Completed 72 requests of 72 estimated requests (100%). XSS optimization removed 116 links. All tests completed.
Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 4 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 252 requests, 4 seconds. Completed 252 requests of 520 estimated requests (48.4615%). XSS optimization removed 116 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 4 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 4 requests, 1 seconds. Completed 4 requests of 4 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.
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 3) + files:(0 x 4) + directories:(4 x 6) + paths:(11 x 10) = total (134)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 10 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 92 requests, 2 seconds. Completed 92 requests of 134 estimated requests (68.6567%). 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 3) + files:(10 x 4) + directories:(95 x 6) + paths:(9 x 10) = total (709)
Batch #5 Path manipulation: estimated time < 1 minute (117 tests, 10 inputs)
Batch #5 Path manipulation: 117 vulnsigs tests, completed 474 requests, 5 seconds. Completed 474 requests of 709 estimated requests (66.8547%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 minute (247 tests, 1 inputs)
Batch #5 WebCgiGeneric: 247 vulnsigs tests, completed 468 requests, 8 seconds. Completed 468 requests of 3130 estimated requests (14.9521%). All tests completed.
Duration of Crawl Time: 8.00 (seconds)
Duration of Test Phase: 29.00 (seconds)
Total Scan Time: 37.00 (seconds)

Total requests made: 1755
Average server response time: 0.10 seconds

Average browser load time: 0.11 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-08-27 03:28:53.0

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Host Name Source
order.maximumsettings.com
FQDN

Form Contains Credit Card Information — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150043
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-30 21:20:25.0

THREAT:
The links listed below have forms that accept credit card information. This information is provided to help you identify areas of the web application that may need careful review due to the sensitive data being handled.

IMPACT:
N/A

SOLUTION:
If possible, review of the source code responsible for handling these form inputs.

RESULT:
https://orders.maximumsettings.com/

TLS Secure Renegotiation Extension Support Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

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

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

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	34011

Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-04-22 02:37:57.0

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 445.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-442,444-6128,6130-46835,46837-65535

Appendices

Hosts Scanned

66.49.252.119

Hosts Not Alive

Option Profile

Scan	
Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing	Standard
Vulnerability Detection	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off

Advanced	
Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Payment Card Industry (PCI) Status

An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards. A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host.

An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards. A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host.

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

	3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	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, vulnerabilites 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.