

Sri Lanka Institute of Information Technology



Assignment report 10

IT22357762

Web Security -IE2062

Web Security – IE2062

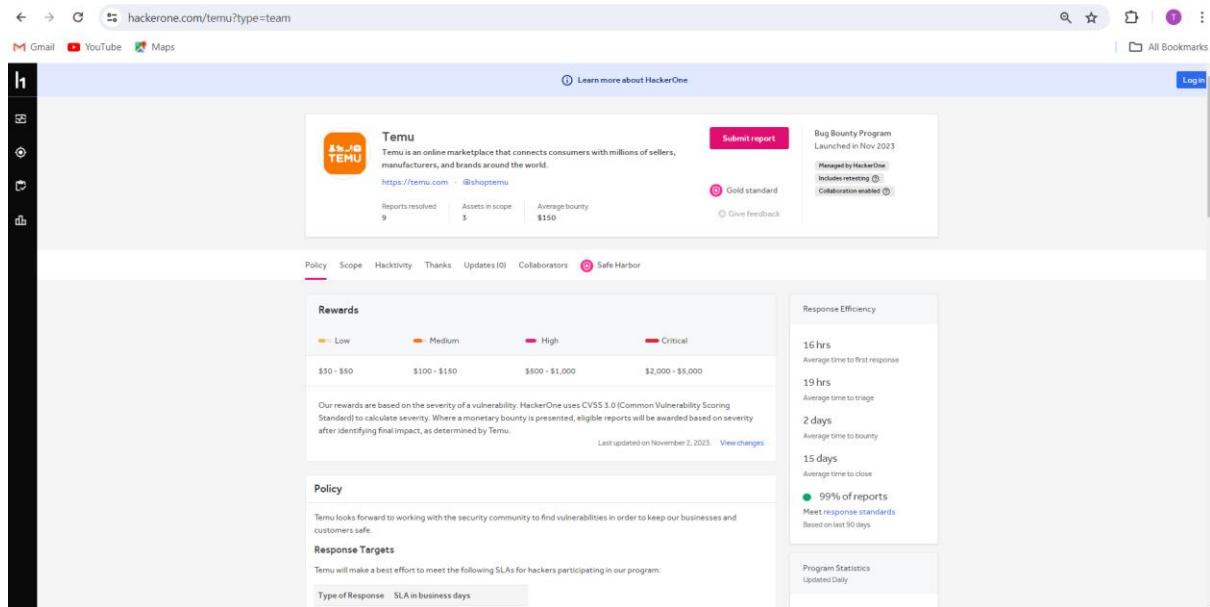
B.Sc. (Hons) in Information

Contents

1	Temu.com	3
1.1	Sub- domain list	3
1.2	Firewall detection	6
1.3	IP scanning	7
1.4	Port scanning	7
1.5	SSL scan.....	8
1.6	Nikto scanning	9
1.7	Burpsuite scanning	10
1.8	Netspaker scan	10
1.9	Vulnerabilities.....	11
1.9.1	Other vulnerabilities.....	12

1 Temu.com

A website which is a marketplace where allows to buy and sell different items with different brands.



1.1 Sub- domain list

Tool – amass

Command – amass enum -passive -d temu.com

Sub domain list –

- www.temu.com
- mxmail-mkt-eu.temu.com
- eu.file.temu.com
- eu.pftk.temu.com
- locale.temu.com
- dan.temu.com
- jp.pftk.temu.com
- thtk.temu.com
- www.mxmail.temu.com
- www.doh.temu.com
- au.matk.temu.com
- mail-76-221.temu.com
- nz.pftk.temu.com
- logistics.temu.com
- eu-ds.temu.com

- au.thtk temu.com
- thtk-us temu.com
- matk temu.com
- br.matk temu.com
- jp.matk temu.com
- o4.ptr3064.order temu.com
- gw-eu temu.com
- nz.matk temu.com
- jp temu.com
- api-eu temu.com
- titan.pftk temu.com
- za.pftk temu.com
- ca temu.com
- www.devdigitalsign.payssl temu.com
- api-us temu.com
- mail-252-217 temu.com
- shr temu.com
- productsign.payssl temu.com
- mail-151-241 temu.com
- thtk-eu temu.com
- www.mxmail-mkt temu.com
- mail-149-250 temu.com
- www.product.payssl temu.com
- br.thtk temu.com
- us.thtk temu.com
- us.file temu.com
- www.mxmail-mkt-eu temu.com
- o7.ptr7420.order temu.com
- mail-149-172 temu.com
- pfs-eu.file temu.com
- us.matk temu.com
- mail-149-156 temu.com
- gw-c-us-ds temu.com
- mxmail-mkt temu.com
- file temu.com
- pftk-qa temu.com
- kr.pftk temu.com
- www.aurl0826.email temu.com
- product.payssl temu.com
- pftk temu.com
- devdigitalsign.payssl temu.com
- eu.matk temu.com
- m temu.com
- app temu.com
- pos-eu.file temu.com
- mail-34-130 temu.com
- kr temu.com
- order temu.com
- gw-cfile-eu temu.com
- www.productsign.payssl temu.com
- o5.ptr9479.order temu.com
- eu temu.com
- us-sp.thtk temu.com
- aurl0826.email temu.com
- o3.ptr454.order temu.com
- seller temu.com

- doh.temu.com
- o1.ptr1892.order.temu.com
- logistics-eu.temu.com
- mxmail-eu.temu.com
- gw-c-eu.temu.com
- devtransport.payssl.temu.com
- pftk-jp.temu.com
- gw-cfile-us.temu.com
- br.temu.com
- au.temu.com
- o5.ptr1143.order.temu.com
- gslb.temu.com
- sg.thtk.temu.com
- temu.com
- o2.ptr1101.order.temu.com
- kr.thtk.temu.com
- mxmail.temu.com
- pftk-eu.temu.com
- gw-cg-us.temu.com
- www.thtk.temu.com
- agentseller.temu.com
- us.pftk.temu.com
- gw-us.temu.com
- gw-tk-us.temu.com
- nz.temu.com
- us.temu.com
- dbm.temu.com
- pos-us.file.temu.com
- ca.matk.temu.com
- sg.pftk.temu.com
- o3.ptr9096.order.temu.com
- ca.pftk.temu.com
- gw-c-us.temu.com
- jp.thtk.temu.com
- o1.ptr1163.order.temu.com
- pfs-us.file.temu.com
- pftk-us.temu.com
- qa.pftk.temu.com
- o5.ptr5925.order.temu.com
- us-ds.temu.com
- eu.thtk.temu.com
- tsrc.temu.com
- br.pftk.temu.com
- mail-36-13.temu.com
- ca.thtk.temu.com
- o2.ptr262.order.temu.com
- za.thtk.temu.com
- au.pftk.temu.com
- o4.ptr1526.order.temu.com
- us-quic.temu.com
- meta-us.temu.com
- qa.thtk.temu.com
- o3.ptr8697.order.temu.com
- nz.thtk.temu.com
- _spf_mail.temu.com
- www.mxmail-eu.temu.com

- share.temu.com
- www.pftk.temu.com
- qa.temu.com
- www.devtransport.payssl.temu.com
- mail-78-163.temu.com

```

[*](tharu@kali):[~]#
$ amass enum -passive -d temu.com
www.temu.com
mxmail-mkt-eu.temu.com
eu.file.temu.com
eu.pftk.temu.com
locale.temu.com
dan.temu.com
jp.pftk.temu.com
thtk.temu.com
www.mxmail.temu.com
www.doh.temu.com
au.matk.temu.com
mail-76-221.temu.com
nz.pftk.temu.com
logistics.temu.com
eu-ds.temu.com
au.thtk.temu.com
thtk-us.temu.com
matk.temu.com
br.matk.temu.com
jp.matk.temu.com
o4.ptr3064.order.temu.com
gw-eu.temu.com
nz.matk.temu.com
jp.temu.com
api-eu.temu.com
titan.pftk.temu.com
za.pftk.temu.com
ca.temu.com
www.devdigitalsign.payssl.temu.com
api-us.temu.com
mail-252-217.temu.com
shr.temu.com
productsign.payssl.temu.com
mail-151-241.temu.com
thtk-eu.temu.com
www.mxmail-mkt.temu.com
mail-149-250.temu.com
www.product.payssl.temu.com
br.thtk.temu.com
us.thtk.temu.com
us.file.temu.com
www.mxmail-mkt-eu.temu.com
o7.ptr7420.order.temu.com
mail-149-172.temu.com
pfs-eu.file.temu.com
us.matk.temu.com
mail-149-156.temu.com
gw-c-us-ds.temu.com
mxmail-mkt.temu.com
file.temu.com

```

1.2 Firewall detection

Command – wafw00f <https://temu.com/>

```
(tharu@kali)-[~]
$ wafw00f https://temu.com/
Multi-Target WAF Fingerprinting Tool
Target IP: https://temu.com
Target Host: temu.com
Target Port: 443
SSL Info:
Status: OK
Start: 2024-07-26 15:00:00
End: 2024-07-26 15:00:05
WAF Fingerprinting Results:
404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://temu.com/
[+] The site https://temu.com/ is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

1.3 IP scanning

Tool – nslookup

Command – nslookup temu.com

```
(tharu@kali)-[~] error(s) and 6 item(s) reported on remote host
$ nslookup temu.com 192.168.1.1 # 192.168.1.1:80 (222 seconds)
Server:                192.168.1.1
Address: (s) resolved 192.168.1.1#53

Non-authoritative answer:
Name:   temu.com
Address: 20.15.0.25
Name:   temu.com
Address: 20.15.0.12
;; communications error to 192.168.1.1#53: timed out
```

1.4 Port scanning

Tool - nmap

Command – `nmap -sV -sC -Pn 20.15.0.25 -A`

```

[~(thorn@kali) ~]$ nmap -sV -sC -Pn 20.15.0.25 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-17 01:51 +0530
Nmap scan report for 20.15.0.25
Host is up (0.19s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp?
|_ fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     500 Syntax error, command unrecognized
|     Hello:
|       552 Invalid domain name in EHLO command.
|_ smtp-commands: Couldn't establish connection on port 25
80/tcp    open  http  nginx
|_ http-title: Site doesn't have a title (application/json).
443/tcp   open  ssl/http nginx
|_ tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|   http/0.9
|_ _ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=*.temu.com
|   Subject Alternative Name: DNS:*.temu.com, DNS=temu.com
|_ Not valid before: 2023-07-13T13:25:20
|_ Not valid after: 2024-08-13T13:25:20
|_ http-title: Site doesn't have a title (application/json).
|_ unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_ SF:Port25-TCP:V=7.93X=750D=4/17XTime=6681D0E6XP=x86_64-pc-linux-gnuXr(Hell
|_ SF:0,2A,"552\x20Invalid\x20domain\x20name\x20in\x20EHLO\x20command\.\r\n")
|_ SF:Xr(GenericLines,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\
|_ SF:ed\r\n")(GetRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecogniz
|_ SF:ed\r\n")(HTTPOptions,28,"500\x20Syntax\x20error,\x20command\x20unreco
|_ SF:gnized\r\n")(RTSPRequest,28,"500\x20Syntax\x20error,\x20command\x20un
|_ SF:recognized\r\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.88 seconds

```

1.5 SSL scan

Command – `sslsan https://www.temu.com/`

```
(tharu@kali)-[~]
$ sslscan https://www.temu.com/
Version: 2.1.3-static
OpenSSL 3.0.12 24 Oct 2023
Target IP: 172.64.144.50
Target Port: 443
Connected to 172.64.144.50
Testing SSL server www.temu.com on port 443 using SNI name www.temu.com
SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 enabled
TLSv1.1 enabled
TLSv1.2 enabled
TLSv1.3 enabled
TLS Fallback SCSV:
Server supports TLS Fallback SCSV
TLS renegotiation:
Secure session renegotiation supported
TLS Compression:
Compression disabled
Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed
Supported Server Cipher(s):
Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
Preferred TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.2 128 bits AES128-GCM-SHA256
Accepted TLSv1.2 128 bits AES128-SHA
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve 25519 DHE 253
Accepted TLSv1.2 256 bits AES256-GCM-SHA384
Accepted TLSv1.2 256 bits AES256-SHA
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits AES128-SHA256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits AES256-SHA256
Preferred TLSv1.1 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
```



```

Accepted TLSv1.1 128 bits AES128-SHA
Preferred TLSv1.1 128 bits ECDHE-RSA-AES128-SHA
Accepted TLSv1.1 128 bits AES128-SHA
Accepted TLSv1.1 256 bits ECDHE-RSA-AES256-SHA
Accepted TLSv1.1 256 bits AES256-SHA
Preferred TLSv1.0 128 bits ECDHE-RSA-AES128-SHA
Accepted TLSv1.0 128 bits AES128-SHA
Accepted TLSv1.0 256 bits ECDHE-RSA-AES256-SHA
Accepted TLSv1.0 256 bits AES256-SHA
Accepted TLSv1.0 112 bits DES-CBC3-SHA

Server Key Exchange Group(s):
TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 260 bits secp521r1 (NIST P-521)
TLSv1.3 128 bits x25519
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 260 bits secp521r1 (NIST P-521)
TLSv1.2 128 bits x25519

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: *.temu.com
AltNames: DNS:*.temu.com, DNS:temu.com
Issuer: Go Daddy Secure Certificate Authority - G2

Not valid before: Jul 13 13:25:20 2023 GMT
Not valid after: Aug 13 13:25:20 2024 GMT

```

1.6 Nikto scanning

Tool – Nikto

Command - sudo nikto -h temu.com

```

(tharu@kali):~$ sudo nikto -h https://temu.com/
[sudo] password for tharu:
- Nikto v2.5.0

+ Multiple IPs found: 20.15.0.25, 20.15.0.12
+ Target IP: 20.15.0.25
+ Target Hostname: temu.com
+ Target Port: 443

+ SSL Info:
  Subject: /CN=*.temu.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://\certs.godaddy.com/repository/\CN=Go Daddy Secure Certificate Authority - G2
  Start Time: 2024-04-17 01:53:25 (GMT+5)

+ Server: nginx
+ /: IP address found in the 'cip' header. The IP is "112.134.238.151". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'cip' found, with contents: 112.134.238.151.
+ /: Uncommon header 'x-pak-request-id' found, with contents: 5713299809553-a718ec7c86a8f9528de39ed856d3656e.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis-sing-content-type-header/
+ /: Cookie api_uid created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page / redirects to: https://www.temu.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000438:SSL routines::tls alert internal error at /var/lib/nikto/plugins/LW2.pm line 5254.
+ at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time: 2024-04-17 01:57:07 (GMT+5) (222 seconds)

+ 1 host(s) tested

```

1.7 Burpsuite scanning

Contents

Host	Method	URL	Params	Status Code	Length	MIME type	Title	Notes
https://us.thkitemu.com	POST	/c/th.gif		200	435			
https://us.thkitemu.com	POST	/c/th.gif		200	435			
https://us.thkitemu.com	POST	/c/th.gif		200	435			
https://us.thkitemu.com	POST	/c/th.gif		200	435			
https://us.thkitemu.com	POST	/c/th.gif		200	435			
https://us.thkitemu.com	POST	/c/th.gif		200	435			

Request

```
POST /c/th.gif HTTP/2
Host: us.thkitemu.com
Cookie: __cf_bm=...
Content-Length: 774
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.1 Safari/537.36
Content-Type: text/plain; charset=UTF-8
Origin: https://www.temu.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.temu.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
PrintKey: url, &
```

Issues

Strict transport security not enforced

Issue: Strict transport security not enforced
Severity: Low
Confidence: Certain
Host: https://us.thkitemu.com
Path: /c/th.gif

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a

1.8 Netsparker scan

Weak Ciphers Enabled

CONFIRMED MEDIUM

URL: https://temu.com/

List of Supported Weak Ciphers:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0008)
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0x0013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0x0014)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x0068)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0x0027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0x0028)
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0x0077)

Progress

Scan Speed: 100.00%

Scan Progress: 100.00%

Links: 1
Elapsed: 00:02:25
Start: 4/17/2024 1:49:46 AM
404 Responses: 0
Head Requests: 0
Total Requests: 264

1.9 Vulnerabilities

Vulnerability Title: Weak SSL/TLS ciphers enabled.

Vulnerability Description: As weak ciphers are enabled, this allows attackers to decrypt SSL traffic between server and visitors.

Affected Components: HTTPS communication on the web server.

Impact Assessment: Impact of vulnerability includes,

- Attackers could potentially intercept and decrypt SSL traffic.
- Sensitive data transmitted over HTTPS, such as login credentials or payment information, could be compromised.
- CIA is at risk.

Steps to Reproduce:

1. Scan the web server using particular scan method. (Netsparker or SSL scan)
2. Identify the weak ciphers in use.
3. Attempt to intercept and decrypt the SSL traffic.

Proof of concept:

Vulnerabilities

2.1. <https://temu.com/>

CONFIRMED

List of Supported Weak Ciphers

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006B)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xC077)
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0x00C4)
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xC076)
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0x00BE)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0x00C0)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0x00BA)

Proposed Mitigation or Fix:

- For Apache, modify the SSLCipher directive in the httpd.conf
`SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4`
- For lighttpd,
`ssl.honor-cipher-order = "enable"`
`ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"`

1.9.1 Other vulnerabilities

1. HTTP Strict Transport Security (HSTS) Policy Not Enabled
2. Weak Ciphers Enabled
3. Missing X-Frame-Options Header
4. Insecure Transportation Security Protocol Supported (TLS 1.0)
5. Content Security Policy (CSP) Not Implemented
6. Expect-CT Not Enabled
7. Missing X-XSS-Protection Header
8. Referrer-Policy Not Implemented
9. Insecure Transportation Security Protocol Supported (TLS 1.1)
10. Nginx Web Server Identified
11. Forbidden Resource Access