Sri Lanka Institute of Information Technology

Assignment report 10

IT22357762

Web Security -IE2062

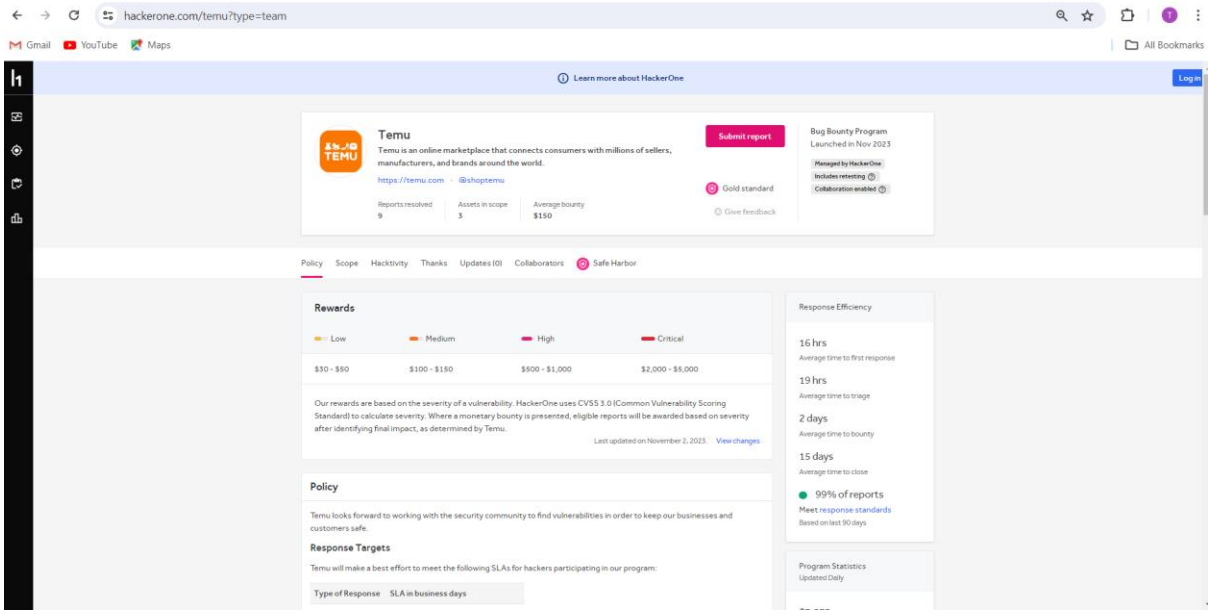
Web Security – IE2062

B.Sc. (Hons) in Information

Contents

1 Temu.com

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

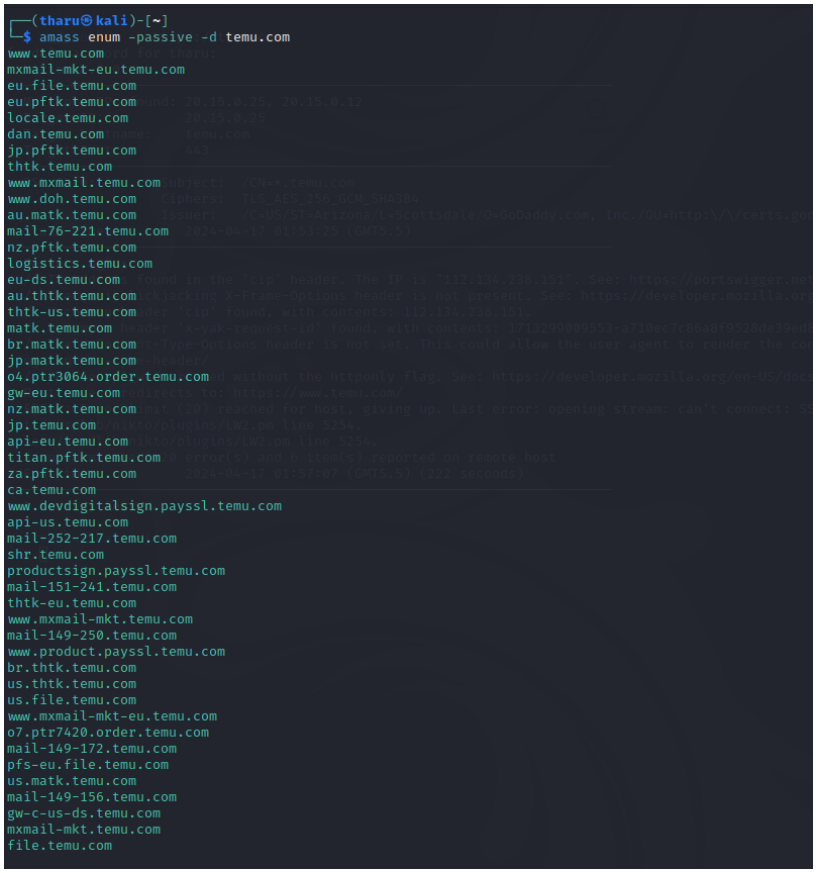
Sub domain list –

- 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



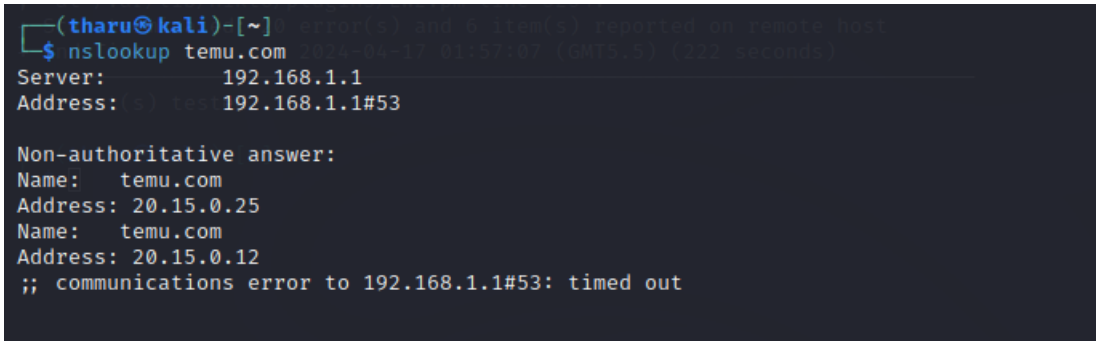
1.2 Firewall detection

Command – wafw00f https://temu.com /

1.3 IP scanning

Tool – nslookup

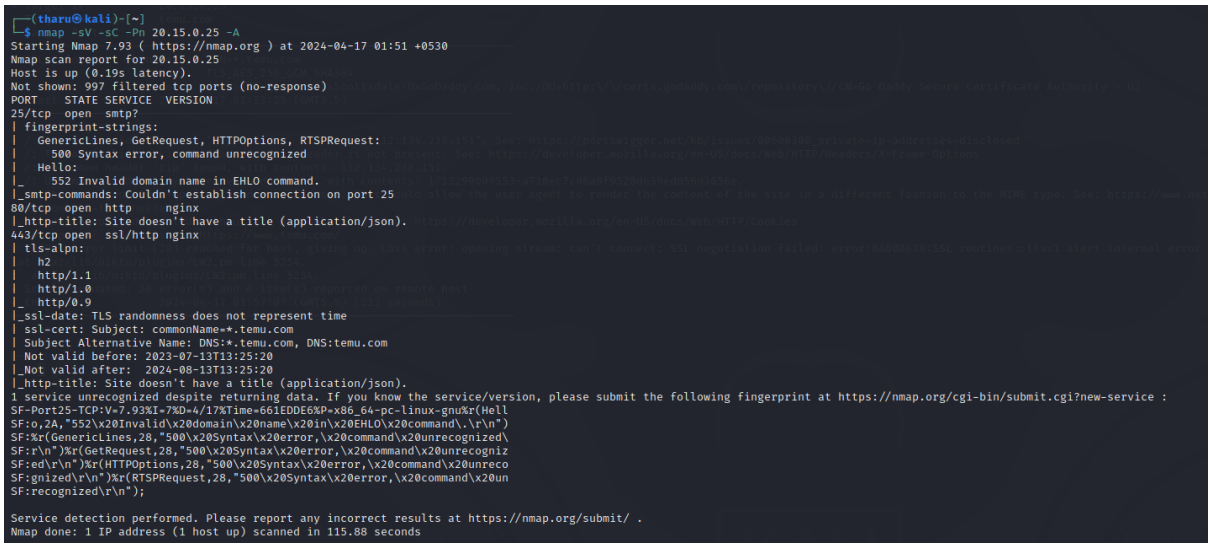
Command – nslookup temu.com



1.4 Port scanning

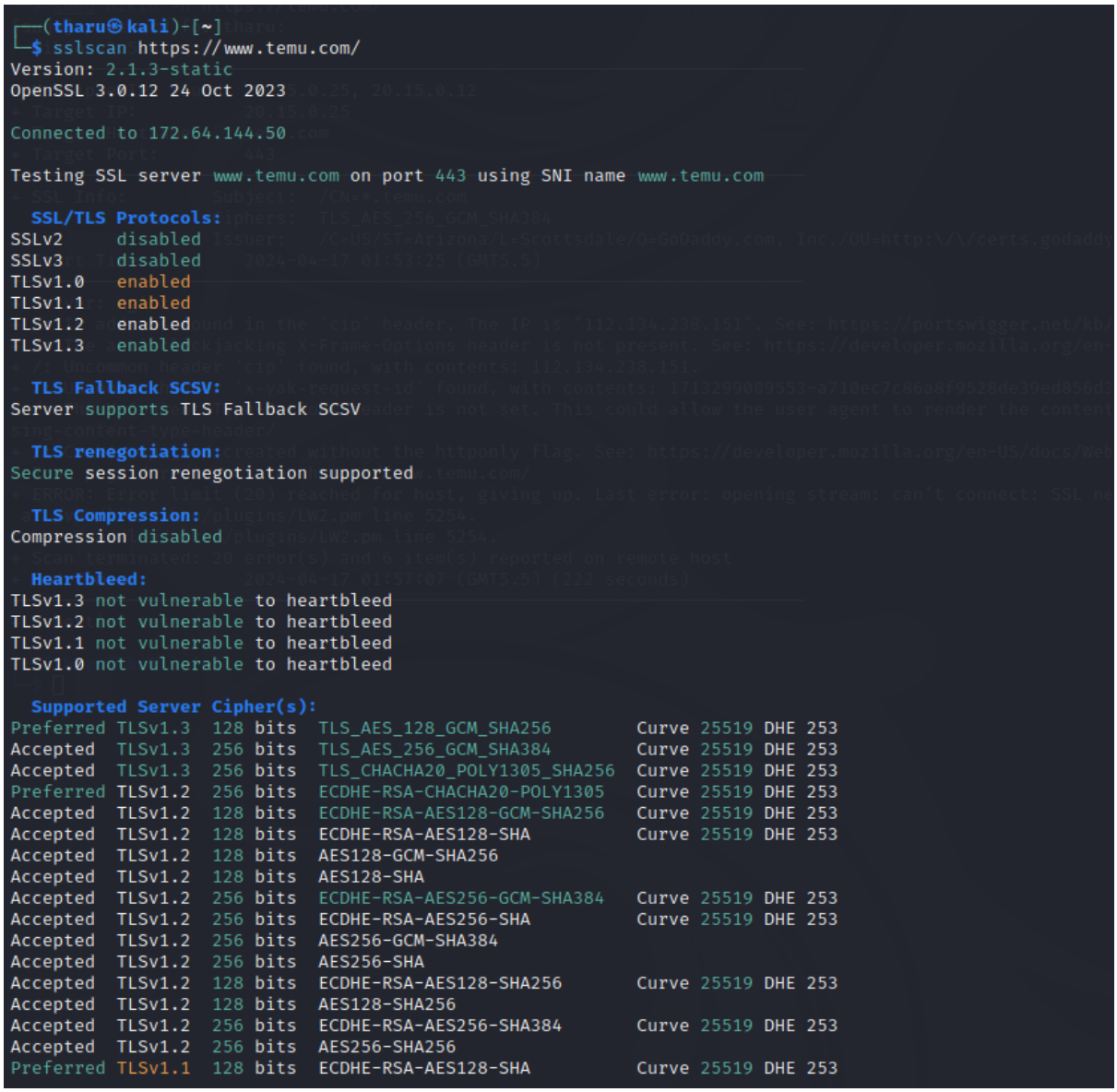
Tool - nmap

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



1.5 SSL scan

Command – sslscan https://www.temu.com/



```
Preferred TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA        Curve 25519 DHE 253
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA        Curve 25519 DHE 253
Accepted  TLSv1.1  256 bits  AES256-SHA
Preferred TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA        Curve 25519 DHE 253
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA        Curve 25519 DHE 253
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
```

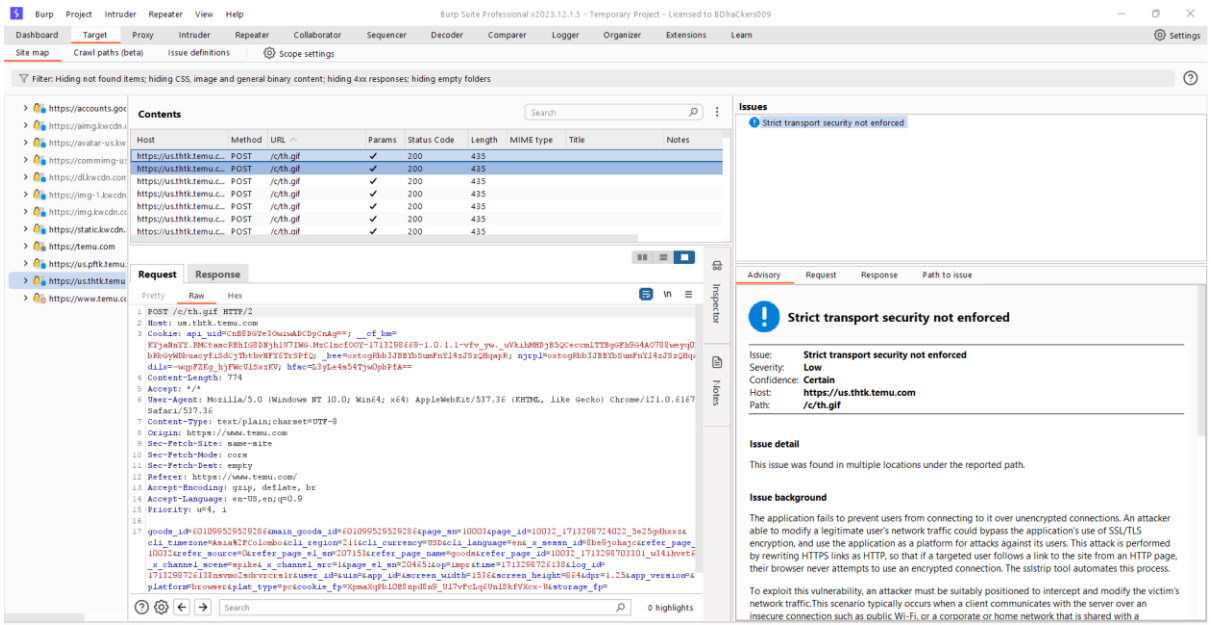
1.6 Nikto scanning

Tool – Nikto

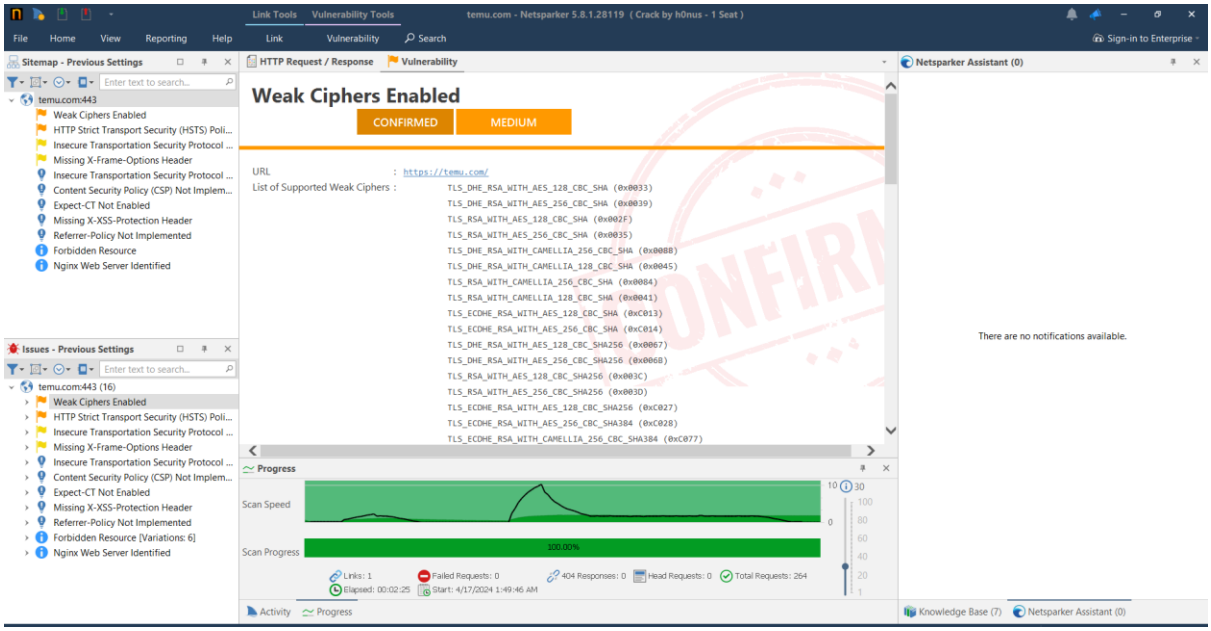
Command - sudo nikto -h temu.com

```
┌──(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 (GMT5.5)
---------------------------------------------------------------------------
+ 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-yak-request-id' found, with contents: 1713299009553-a710ec7c86a8f9528de39ed856d3656e.
+ /: 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/missing-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::tlsv1 alert internal error at /var/lib/nikto/plugins/LW2.pm line 5254.
 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 (GMT5.5) (222 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

1.7 Burpsuite scanning



1.8 Netspaker scan



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.

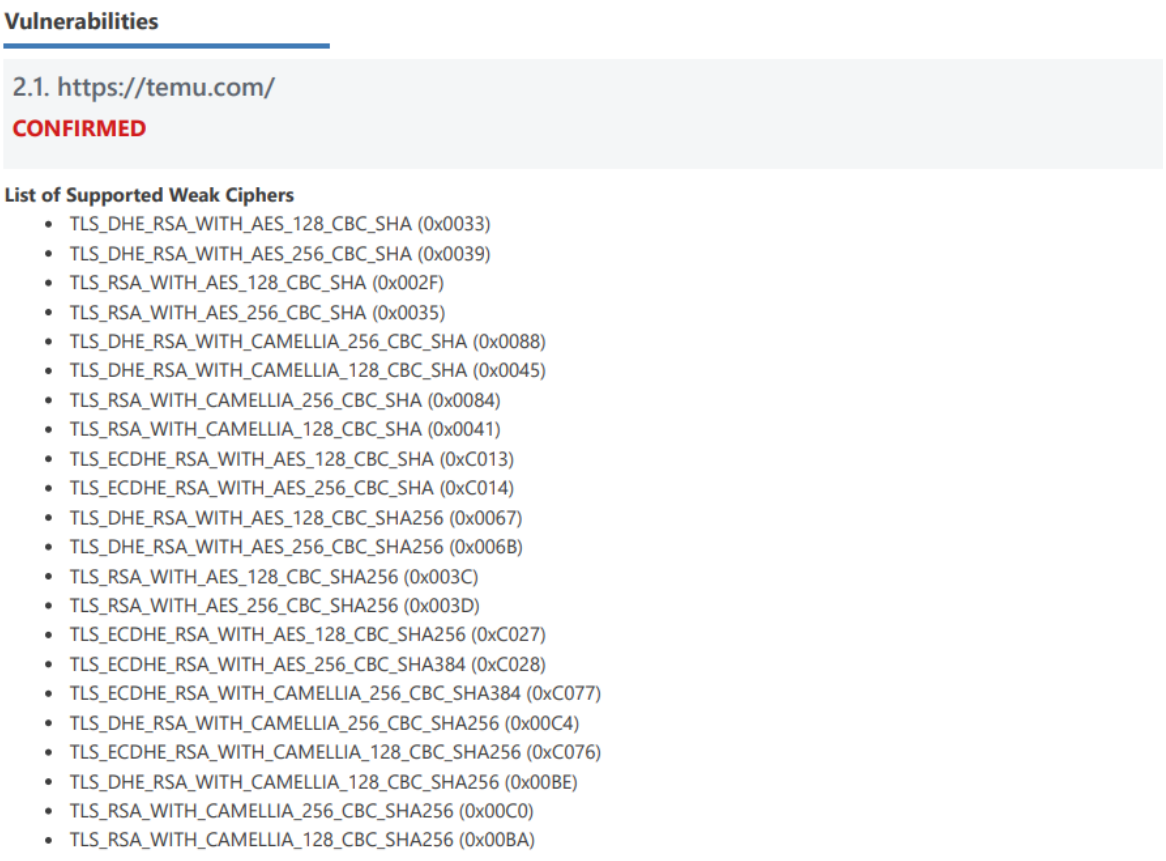
Impact Assessment: Impact of vulnerability includes,

- 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 sacn)
2. Identify the weak ciphers in use.
3. Attempt to intercept and decrypt the SSL traffic.

Proof of concept:



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