

Sri Lanka Institute of Information Technology



BUG BOUNTY REPORT - 5

Web Security – IE2062

IT22362780

Jayaweera N.S

Report Details

Report # - 05

Domain - <https://temu.com>

Platform -bugcrowd.com

Scans performed -
Nmap scan
Nslookup
metasploit
Wafw00f scan
Dotdotpwn scan
Nikto scan
Sqlmap scan
Manual scanning using Wapplyzer
Recon-ng scan

Nmap scan

Using nmap scan all the open ports in the target can be identified.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS -T4 temu.com
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-27 13:18 EDT
Nmap scan report for temu.com (20.15.0.12)
Host is up (0.024s latency).
Other addresses for temu.com (not scanned): 20.15.0.25
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 9.11 seconds and n
```

No unusual ports are open.

But Smtip port 25 is vulnerable when it's opened, because it lacks authentication and encryption.

Let's see if we can establish a connection on port 25.

```
(kali㉿kali)-[~]
└─$ nmap temu.com --script=smtp* -p 25
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-27 13:24 EDT
Nmap scan report for temu.com (20.15.0.25)
Host is up (0.18s latency).
Other addresses for temu.com (not scanned): 20.15.0.12

PORT      STATE SERVICE
25/tcp    open  smtp
| smtp-enum-users:
|_ Couldn't establish connection on port 25
|_smtp-commands: Couldn't establish connection on port 25
|_smtp-open-relay: Couldn't establish connection on port 25

Nmap done: 1 IP address (1 host up) scanned in 31.17 seconds
```

Connection cannot be established therefore a vulnerability cannot be identified.

Nslookup

```
(kali@kali)-[~]  
$ nslookup temu.com  
Server:      192.168.1.1  
Address:     192.168.1.1#53  
  
Non-authoritative answer:  
Name:   temu.com  
Address: 20.15.0.25  
Name:   temu.com  
Address: 20.15.0.12
```

The ip address of temu.com can be found.

Metasploit

[illegible]

Search for smtp

```

safe > search setp
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/linux/setp/apache_jones_exec 2015-10-01 normal Yes Apache James Server 2.3.2 Insecure User Creation
1 auxiliary/server/capture/setp normal No Authentication Capture: SETP
2 auxiliary/scanner/http/gavazzi_en_login_loot normal No Carlo Gavazzi Energy Meters - Login Brute Force
p Plant Database
3 exploit/unix/setp/clamav_milter_blackhole 2007-08-24 excellent No ClamAV Milter Blackhole-Mode Remote Code Execution
4 exploit/windows/browser/communiCrypt_mail_activeX 2010-05-19 great No CommuniCrypt Mail 1.16 SETP ActiveX Stack Buffer Overflow
5 exploit/linux/setp/exim_gethostbyname_bof 2015-01-27 great Yes Exim GHOST (glibc gethostbyname) Buffer Overflow
6 exploit/linux/setp/exim4_dovecot_exec 2013-05-03 excellent No Exim Dovecot Insecure Configuration Command Execution
7 exploit/unix/setp/exim4_string_format 2010-12-07 excellent No Exim4 string-format Function Heap Buffer Overflow
8 auxiliary/client/setp/esmiller normal No Generic Emailer (SETP)
9 exploit/linux/setp/haraka excellent Yes Haraka SETP Command Injection
10 exploit/windows/http/mdaemon_worldclient_form2raw 2003-12-29 great Yes MDAemon WorldClient form2raw.cgi Stack Buffer Overflow
11 exploit/windows/setp/ms03_046_exchange2000_exch50 2003-10-15 good Yes MS03-046 Exchange 2000 EXCH50 Heap Overflow
12 exploit/windows/ssll/ms06_011_gct average No MS06-011 Microsoft Private Communications Transport
13 auxiliary/dos/windows/setp/ms06_019_exchange 2004-11-12 normal No MS06-019 Exchange MDOOPROP Heap Overflow
14 exploit/windows/setp/mercury_cram_md5 2007-08-18 great No Mercury Mail SETP AUTH CRAM-MD5 Buffer Overflow
15 exploit/unix/setp/morris_sendmail_debug average Yes Morris Worm sendmail Debug Mode Shell Escape
16 exploit/windows/setp/njstar_setp_bof normal Yes NJStar Communicator 3.00 MiniSETP Buffer Overflow
17 exploit/unix/setp/opensttd_mail_from_rcv excellent Yes OpenSMTPD MAIL FROM Remote Code Execution
18 exploit/unix/local/opensttd_oob_read_lpe average Yes OpenSMTPD OOB Read Local Privilege Escalation
19 exploit/windows/browser/oracle_dc_subeltttoexpress normal No Oracle Document Capture 10g Activex Control Buffer Overflow
20 exploit/unix/setp/quail_bash_env_exec normal No Quail SETP Bash Environment Variable Injection
21 auxiliary/scanner/setp/setp_version normal No SETP Banner Grabber
22 auxiliary/scanner/setp/setp_ntlm_domain normal No SETP NTLM Domain Extraction

```

The module “fuzzer” is used to fuzz the smtp service. And “smtp_enum” is used for the username enumeration.

```
msf6 > use auxiliary/fuzzers/smtp/smtp_fuzzer
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > show options

Module options (auxiliary/fuzzers/smtp/smtp_fuzzer):
```

Name	Current Setting	Required	Description
CMD	EHLO	yes	Command to fuzzer (Accepted: EHLO, HELO, MAILFROM, RCPTTO, DATA, VRFY, EXPN)
INTERACTIONS	100	no	Number of interactions to run
MAILFROM	sender@example.com	yes	FROM address of the e-mail
MAILTO	target@example.com	yes	TO address of the e-mail
RESPECTORDER	true	no	Respect order of commands
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	25	yes	The target port (TCP)
STARTLEN	100	yes	Length of the string + start number
THREADS	1	yes	The number of concurrent threads (max one per host)

View the full module info with the `info`, or `info -d` command.

Set the RHOSTS to temu.com

```
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > set RHOSTS temu.com
RHOSTS => temu.com
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > run
```

```
[*] 20.15.0.25:25 - The connection with (20.15.0.25:25) timed out.
[*] 20.15.0.25:25 - Fuzzing with iteration 1

[*] 20.15.0.25:25 - Could not connect to the service:
[*] temu.com:25 - Scanned 1 of 2 hosts (50% complete)
[*] temu.com:25 - Scanned 1 of 2 hosts (50% complete)
[*] temu.com:25 - Scanned 1 of 2 hosts (50% complete)
[*] temu.com:25 - Scanned 1 of 2 hosts (50% complete)
[*] temu.com:25 - Scanned 1 of 2 hosts (50% complete)
[-] 20.15.0.12:25 - The connection with (20.15.0.12:25) timed out.
[*] 20.15.0.12:25 - Fuzzing with iteration 1

[*] 20.15.0.12:25 - Could not connect to the service:
[*] temu.com:25 - Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) >
```

Fuzzing failed due to connection time out indicating inability to enumerate the service. Fuzzing attempts are blocked by the server.

Nikto scan

```
(kali@kali)~$ nikto -h https://temu.com
- Nikto v2.1.6

+ 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.

+ Message:      Multiple IP addresses found: 20.15.0.25, 20.15.0.12
+ Start Time:    2024-04-27 13:51:47 (GMT-4)
```

```
+ Server: nginx
+ IP address found in the 'cip' header. The IP is "112.134.191.78".
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.
+ Uncommon header 'cip' found, with contents: 112.134.191.78
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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.
+ All CGI directories 'found', use '-C none' to test none
+ The Content-Encoding header is set to 'deflate' this may mean that the server is vulnerable to the BREACH attack.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000438:SSL routines::tls
real error at /var/lib/nikto/plugins/LW2.pm line 5157,
at /var/lib/nikto/plugins/LW2.pm line 5157,
; at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 20 error(s) and 8 item(s) reported on remote host
+ End Time:      2024-04-27 13:57:32 (GMT-4) (345 seconds)

+ 1 host(s) tested
```

Results obtained from the scan:

- The anti-clickjacking "X-Frame-Options" header, which helps prevent clickjacking attacks, is not present.
- The "X-XSS-Protection" header is not defined, which can protect against some forms of XSS.
- The site uses SSL and Expect-CT header is not present.

The "expect-CT" header is a security feature that helps websites, and their users avoid the risks associated with incorrectly issued SSL certificates.

It supports transparency and accountability when issuing SSL certificates, which improves overall web security.

There are some issues/disadvantages occurred when the “expect-CT” header is absent:

- The protection against the mis issuing of SSL certificates will be low.
- Mismanagement of SSL certificates.
- No trust and security

But the absence of “expected-CT” header is not a huge vulnerability or a security issue in a website.

- The site uses SSL and the Strict-transport-security HTTP header is not defined.
- The X-content-Type-options header is not set.

Recon-ng

here the recon-ng will be used to find all the sub domains in the target.

```
[1] Recon modules
```

```
[recon-ng][default] > workspaces create bb1  
[recon-ng][bb1] > modules load hackertarget  
[recon-ng][bb1][hackertarget] > show options  
Shows various framework items
```

```
Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|
```

```
[recon-ng][bb1][hackertarget] > options set SOURCE temu.com  
SOURCE ⇒ temu.com  
[recon-ng][bb1][hackertarget] > run
```

```
TEMU.COM
```

```
[*] Country: None  
[*] Host: temu.com  
[*] Ip_Address: 20.15.0.25  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: pfs-us.file.temu.com  
[*] Ip_Address: 20.120.64.10  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: gw-c-eu.temu.com  
[*] Ip_Address: 20.105.12.146  
[*] Latitude: None  
[*] Longitude: None
```

```
SUMMARY
```

```
[*] 33 total (33 new) hosts found.  
[recon-ng][bb1][hackertarget] > █
```

33 sub domains were found.

Wafw00f scan

Used to identify the type of WAF that is used to protect the web application.

```

(kali㉿kali)-[~]
$ wafw00f https://temu.com

```

(W00f!)
 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

```

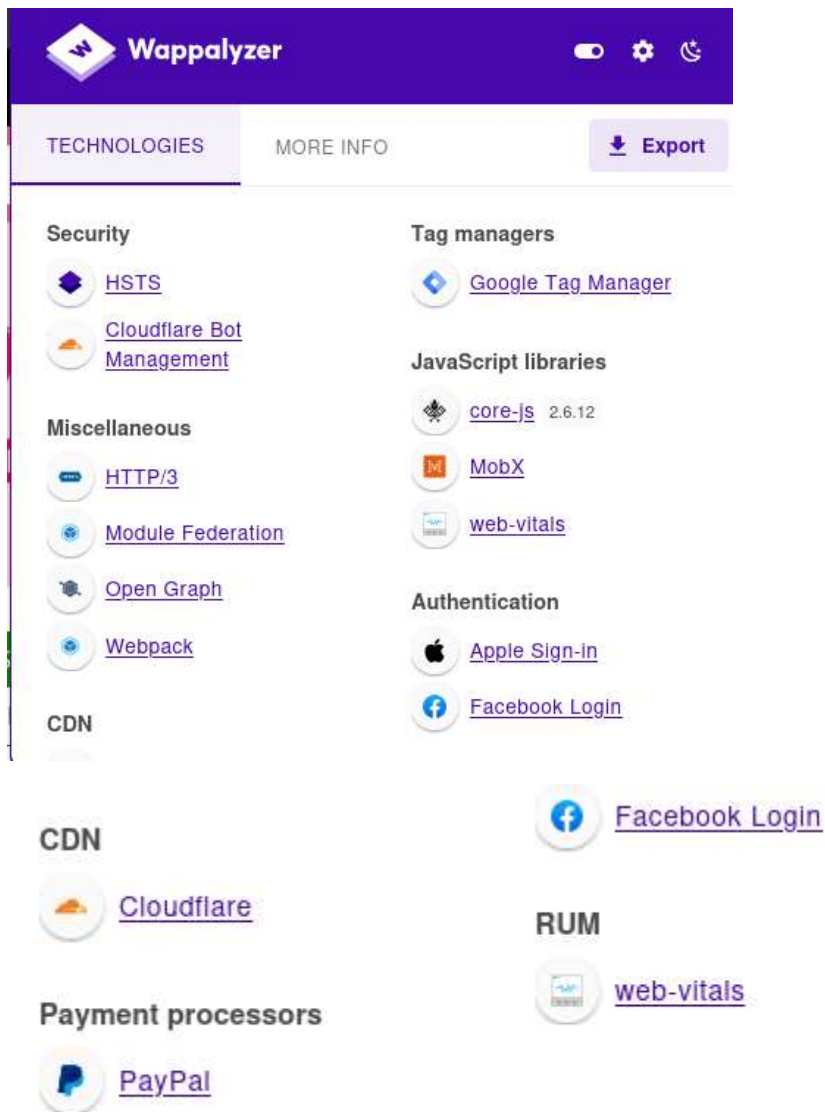
[*] Checking https://temu.com
[+] The site https://temu.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

```

According to the test results, “Cloudflare (Cloudflare Inc.)” is used as the firewall of the web application.

Wappalyzer

The Wappalyzer is used to identify the technologies used in the web application.



these are the technologies used.

The java script library contains a core.js

Snyk Vulnerability Database › npm › core-js › core-js@2.6.12

core-js@2.6.12 vulnerabilities

Standard library

Direct Vulnerabilities

No direct vulnerabilities have been found for this package in Snyk's vulnerability database. This does not include vulnerabilities belonging to this package's dependencies.

[1] figure from <https://security.snyk.io>

there are no direct vulnerabilities in this version of core.js

Dotdotpwn

Dotdotpwn is a directory traversal checker.

```
[+] Report name: Reports/temu.com_04-27-2024_14-50.txt

[===== TARGET INFORMATION =====]
[+] Hostname: temu.com
[+] Protocol: http
[+] Port: 80

[===== TRAVERSAL ENGINE =====]
[+] Creating Traversal patterns (mix of dots and slashes)
[+] Multiplying 6 times the traversal patterns (-d switch)
[+] Creating the Special Traversal patterns
[+] Translating (back)slashes in the filenames
[+] Adapting the filenames according to the OS type detected (unix)
[+] Including Special suffixes
[+] Traversal Engine DONE ! - Total traversal tests created: 11028

[===== TESTING RESULTS =====]
[+] Ready to launch 3.33 traversals per second
[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)

[*] HTTP Status: 400 | Testing Path: http://temu.com:80/../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://temu.com:80/../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://temu.com:80/../../etc/passwd
```

```
[+] Testing Path: http://temu.com:80/?%00%vetc%00%vpasswd ← VULNERABLE!

[*] Testing Path: http://temu.com:80/?%00%vetc%00%vissue ← VULNERABLE!
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%v?%00%vetc%00%vpasswd
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%v?%00%vetc%00%vissue
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%v?%00%v?%00%vetc%00%vpasswd
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%v?%00%v?%00%vetc%00%vissue
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%v?%00%v?%00%v?%00%vetc%00%vpasswd
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%v?%00%v?%00%v?%00%vetc%00%vissue
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%v?%00%v?%00%v?%00%v?%00%vetc%00%vpasswd
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%v?%00%v?%00%v?%00%v?%00%vetc%00%vissue
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%v?%00%v?%00%v?%00%v?%00%v?%00%vetc%00%vpasswd
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%v?%00%v?%00%v?%00%v?%00%v?%00%vetc%00%vissue

[*] Testing Path: http://temu.com:80/?%00%qfetc%00%qpasswd ← VULNERABLE!
[*] Testing Path: http://temu.com:80/?%00%qfetc%00%qissue ← VULNERABLE!
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%qf?%00%qfetc%00%qpasswd
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%qf?%00%qfetc%00%qissue
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%qf?%00%qf?%00%qfetc%00%qpasswd
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%qf?%00%qf?%00%qfetc%00%qissue
[*] HTTP Status: 403 | Testing Path: http://temu.com:80/?%00%qf?%00%qf?%00%qf?%00%qfetc%00%qpasswd
```

The scan results returned status codes within the range 400 (400-499). It shows a client error.

Therefore, we can conclude that the tested destinations are not vulnerable to a directory traversal.

Sqlmap

With the use of this scan, we can identify whether a sql injection can be done or not.

```
(kali@kali)-[~]
$ sqlmap -u https://www temu.com/search_result.html?search_key=newtestword12345

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused

[*] starting @ 15:58:50 /2024-04-27/

[15:58:50] [INFO] testing connection to the target URL
[15:58:50] [WARNING] potential permission problems detected ('Access denied')
[15:58:50] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the resu
you have not declared cookie(s), while server wants to set its own ('__cf_bm=.lrGUCkoK68...hD4xT4llag'). Do you
[15:58:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:58:54] [INFO] testing if the target URL content is stable
[15:58:55] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page compar
parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'

[15:59:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:59:00] [WARNING] GET parameter 'search_key' does not seem to be injectable
[15:59:00] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. Pl
ease retry with the switch '--test-only' (along with --technique=00) as this case looks like a perfect candidate (low textual content along with inability of compariso
n engine to detect at least one dynamic parameter). If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use optio
n '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[15:59:06] [WARNING] HTTP error codes detected during run:
403 (Forbidden) = 87 times
[15:59:06] [WARNING] your sqlmap version is outdated

[*] ending @ 15:59:06 /2024-04-27/
```

there is no injection vulnerability in the above web application.