

Sri Lanka Institute of Information Technology



Year 2 semester 2

IT23360600

G. P. I. Perera

SLIIT KANDY UNI

BUG BOUNTY REPORT 4

Web Security – IE2062

B.Sc. (Hons) in information Technology Specializing in Cyber Security

1. Requirement gathering and analysis

Selected sub domain	www.temu.com
Hackerone URL	https://hackerone.com/temu
IP address	151.101.66.58 / 151.101.2.58

Subdomain list

```
(lynx@vbox)-[~]
$ subfinder -d temu.com

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/lynx/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for temu.com
seller.temu.com
www.gtm-us.temu.com
www.productsign.payssl.temu.com
gw-b-us.temu.com
gw-gslb-eu.temu.com
pftk-br.temu.com
mxmail-mkt.temu.com
pftk-jp.temu.com
ca.pftk.temu.com
gslb.temu.com
gw-c-qa.temu.com
gw-cfile-us.temu.com
pftk-us.temu.com
eu-ds.temu.com
www.mxmail-us.temu.com
pftk-qa.temu.com
api-euo.temu.com
devtransport.payssl.temu.com
www.mxmail-usg.temu.com
appreciation.app.temu.com
us.matk.temu.com
br.temu.com
qa.temu.com
us.temu.com
app.temu.com
gw-cfile-eu.temu.com
o5.ptr1143.order.temu.com
o4.ptr316.order.temu.com
gw-euo.temu.com
www.mxmail-market-us.temu.com
gtm.temu.com
```

Firewall detection:

```
(lynx@vbox)-[~]
$ wafw00f https://temu.com/

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

~ WAFW00F : v2.3.1 ~
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
```

Nmap scan:

```
(lynx@vbox)-[~]
$ nmap temu.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 02:25 EDT
Nmap scan report for temu.com (151.101.2.58)
Host is up (0.32s latency).
Other addresses for temu.com (not scanned): 151.101.66.58
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 25.17 seconds
```

Nikto scan result

```
(lynx@vbox)-[~]
$ nikto -h https://www temu.com/
- Nikto v2.5.0

+ Multiple IPs found: 172.64.144.50, 104.18.43.206
+ Target IP: 172.64.144.50
+ Target Hostname: www 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: 2025-04-27 02:41:25 (GMT-4)

+ Server: cloudflare
+ /: IP address found in the 'cf_bm' cookie. The IP is "1.0.1.1".
+ /: IP address found in the 'cip' header. The IP is "123.231.125.137". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: IP address found in the 'set-cookie' header. The IP is "1.0.1.1". 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: 123.231.125.137.
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: 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/
+ /CBFIfAk4.mdb: Cookie region created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /CBFIfAk4.mdb: Cookie language created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /CBFIfAk4.mdb: Cookie currency created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /CBFIfAk4.mdb: Cookie api_uid created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /CBFIfAk4.mdb: Uncommon header 'x-gateway-request-id' found, with contents: 1745736091747-07875cab3dd83e8e5b50b8010e1df3-2.
```

Active scan result from OWASP ZAP:

URL to attack:

Use traditional spider: ☒

Use ajax spider: with

Attack Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

History Search Alerts Output Spider Active Scan

Alerts (9)

- Content Security Policy (CSP) Header Not Set (3)
- Missing Anti-clickjacking Header (3)
- Cookie with SameSite Attribute None (3)
- Timestamp Disclosure - Unix (4)
- X-Content-Type-Options Header Missing (3)
- Loosely Scoped Cookie (4)
- Modern Web Application (4)
- Re-examine Cache-control Directives (3)
- Session Management Response Identified (4)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Developer Tools:

Name	Headers	Preview	Response	Initiator	Timing
react_webpack_runtime_ed65e1485f68b76...	Status Code:		200 OK (from memory cache)		
biz_vendors_cb94d10a96abfbbbjs	Remote Address:		[2606:4700:4400:6812:2397]:443		
vendors_1c44a9111bbc4d51js	Referrer Policy:		strict-origin-when-cross-origin		
index_2670ca446cba2b4bjs	▼ Response Headers				
165_7e5d12057bbe96de8145js	Access-Control-Allow-Origin:		*		
2705_c1830bd952e38dd0eecd0js	Age:		162373		
5042_7a76b44499dc8d2101cdjs	Alt-Svc:		h3=":443"; ma=86400		
index_fed_temp_05bdbe66e20d22320e0ejs	Cache-Control:		max-age=31536000		
2.4.41js	Cf-Cache-Status:		HIT		
6400_4d693ab3907d12c20a5ajjs	Cf-Ray:		936c4c67088bb305-CMB		
dynamic_flash_b4408967dbd8e2e38757js	Colloid:		260		
5908_a70fdb5690afecca0994js	Content-Encoding:		br		
7523_294ae2d88e771c7f4acajjs	Content-Md5:		4vys6h2mplajzswWpq9OA=		
blobhttps://www.temu.com/2f4e76d-b...	Content-Type:		application/javascript; charset=utf-8		
4970_ca0e22357da03f28e243js	Date:		Sun, 27 Apr 2025 06:35:11 GMT		
biz_layout_sc_sidebar_e6a11fd29ec8d81ea0...	Etag:		W/"0x8DD83DA9628C135"		
biz_layout_activity_coupon_popup_76e246...	Last-Modified:		Fri, 25 Apr 2025 09:21:40 GMT		
biz_layout_sc_float_4389121591d44bc9768f...	Priority:		u=3,j=20		
smoothscroll-polyfill_e83e58bef2b726379a...	Server:		cloudflare		
biz_layout_toolbar_b494160df542bb43f42js	Server-Timing:		cfExtPri		
1648_f7b6a4d1d4a37c5ae95cjs	Timing-Allow-Origin:		*		
home-unified-popup_5018e7101a33a71cd...	Vary:		Accept-Encoding		
home-other-popup_ad5f02d84e3bc322e70...	X-Cache-Status:		HIT		
4128_cbda2f0ac1cede589a3bjs	X-Cip:		2402:4000:20c3d7a1fd61:28c6f10d:2a4f		
biz_sc_popup_sep_check_97e681f5f94e63e...	X-Content-Type-Options:		nosniff		
biz_sc_popup_low_price_e31b632b0611e28...	X-Store-Request-Id:		f88bf4bf75f4a5f7da6aba0d9941ef69		
biz_sc_popup_separate_checkout_093e4efb...	▼ Request Headers				
261_22d1772a063d192db681js					
sku-selector_6f22cbec4cc660049268js					

2. Report Details

1. Vulnerability Title: CSP header not set

2. Vulnerability Description:

A **Content Security Policy (CSP)** is a security feature that **helps prevent certain attacks**, especially **Cross-Site Scripting (XSS)**, **data injection attacks**, and some forms of **clickjacking**.

When the CSP header is **missing**, browsers **don't have extra rules** to restrict what content (scripts, styles, frames, etc.) can load.

Result:

- Attackers can inject **malicious scripts** into the site much more easily.
- Data theft, session hijacking, malware downloads can happen without the browser blocking them.

In short: No CSP = Less protection against frontend attacks like XSS.

Conclusion/ Inference:

- The web server **lacks important security headers**, making it **vulnerable to common attacks** like:
 - Clickjacking,
 - Browser content-type sniffing issues,
 - Potential future XSS risks (if found elsewhere).
- There is **minor information leakage** via headers and cookies, **increasing reconnaissance risks** for attackers.
- **Cookie security is weak** because the HttpOnly attribute is missing, making it easier for attackers to steal session info if other attacks (like XSS) succeed.
- **No critical vulnerabilities** like SQLi, XSS, or RCE were detected yet from this surface scan, but **security hardening is needed** to prevent exploitation.
- The presence of **Cloudflare** is good, but **defense in depth** is missing at the application layer (the app itself needs security headers and secure cookie handling).

3. Affected Components:

1. <https://www temu.com>
2. <https://www temu.com/robots.txt>
3. <https://www temu.com/sitemap.xml>

4. Impact Assessment:

OWASP analysis:

Risk level	Medium
Confidence	High

Nikto –

Nikto finding	Meaning	Risk
IP address found in __cf_bm cookie / cip header	Some internal or user IP addresses are leaking into headers and cookies. Could be minor privacy issue.	Low-Medium

No X-Frame-Options header	The website doesn't set the X-Frame-Options header → Clickjacking attacks possible	Medium Risk (social engineering, UI deception).
Uncommon header 'cip' found	An uncommon header revealing a user's IP (123.231.125.137) is being sent. Can be used for profiling users.	Low Risk (info disclosure)
Missing X-Content-Type-Options header	No X-Content-Type-Options: nosniff header → Browser could wrongly guess file types → Content-type confusion attacks	Medium Risk (minor injection surface).
Cookies without HttpOnly flag (region, language, currency, api_uid)	Cookies can be accessed by JavaScript (like if XSS happens), making session hijacking easier	Medium Risk (session theft possible if XSS is found).

5. Steps to reproduce –

- **On owasp zap –**
Start the application, input target URL and run an automated scan.
Observe alerts.
- **nikto-**
perform a manual nikto scan by,
`nikto -h https://temu.com`
- **Developer Tools –**
Click inspect and go to the network tab. Discover that in response headers there are no CSP headers set.



6. Proposed mitigation or fix

1. Set Security Headers:

- a. Add the following HTTP headers:
 - i. X-Frame-Options: SAMEORIGIN → Prevent Clickjacking.
 - ii. X-Content-Type-Options: nosniff → Prevent MIME-type sniffing.
 - iii. Content-Security-Policy: default-src 'self'; → Limit external resources.
 - iv. Strict-Transport-Security: max-age=31536000; includeSubDomains; preload → Enforce HTTPS.

2. Secure Cookies:

- a. Add attributes to all cookies:
 - i. HttpOnly → Prevent JavaScript access.
 - ii. Secure → Ensure cookies are only sent over HTTPS.
 - iii. SameSite=Strict OR SameSite=Lax → Prevent CSRF.

3. Remove Information Leakage:

- a. Sanitize or remove unnecessary headers (like cip and x-gateway-request-id) that expose backend or client IP addresses.
- b. Avoid embedding IP addresses into cookies.

4. Monitor and Harden Backend Infrastructure:

- a. Mask internal identifiers in public responses.
- b. Regularly audit headers exposed to users.

5. Periodic Security Scans:

- a. Schedule automated scans (Nikto, Nuclei, or OWASP ZAP) to catch regressions early.