Sri Lanka Institute of Information Technology

Year 2 semester 2

IT23360600
G. P. I. Perera

SLIIT KANDY UNI

BUG BOUNTY REPORT 4

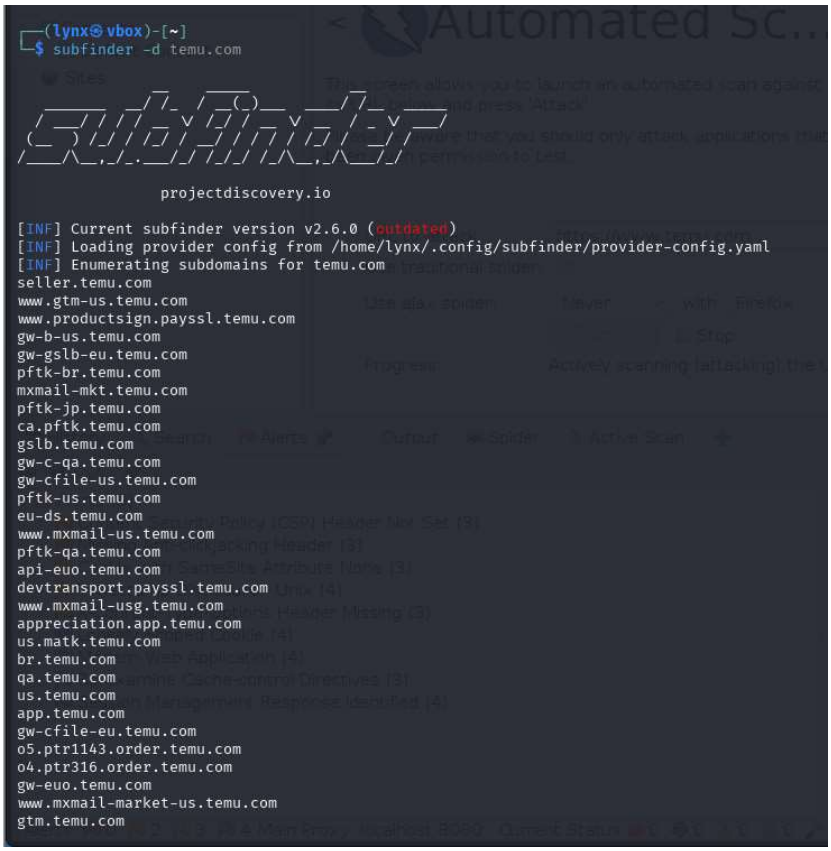
Web Security – IE2062

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

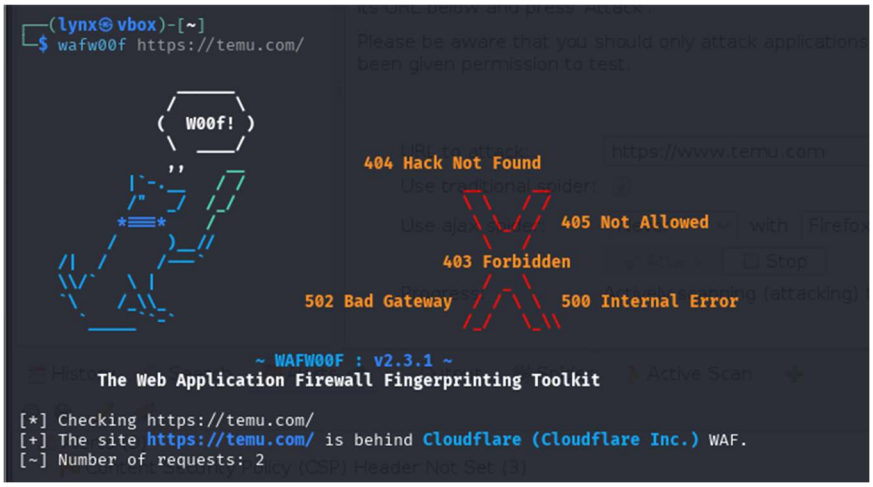
1. Requirement gathering and analysis

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

Subdomain list



Firewall detection:



Nmap scan:

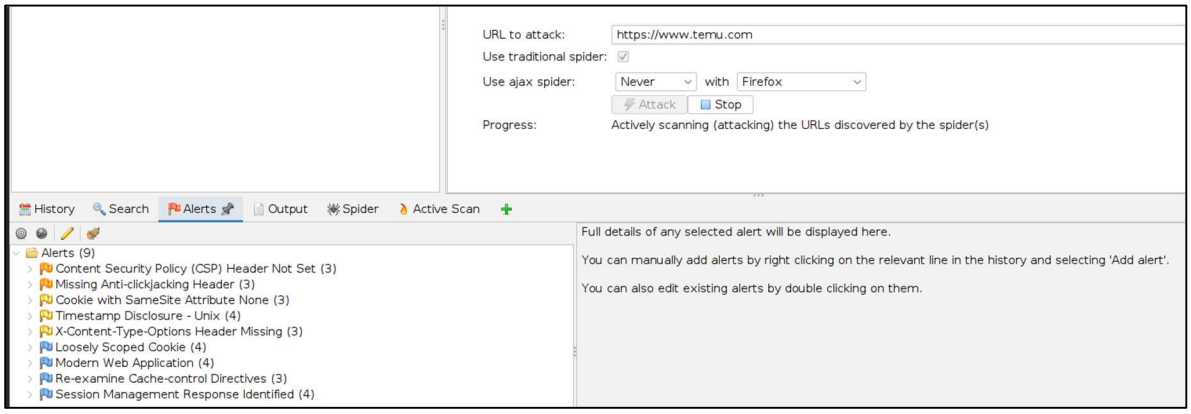
```
┌──(lynx㉿vbox)-[~]
└─$ nmap temu.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 02:25 EDT
Nmap scan report for temu.com (151.101.2.58)
Host is up (0.32s latency).
Other addresses for temu.com (not scanned): 151.101.66.58
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
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
```

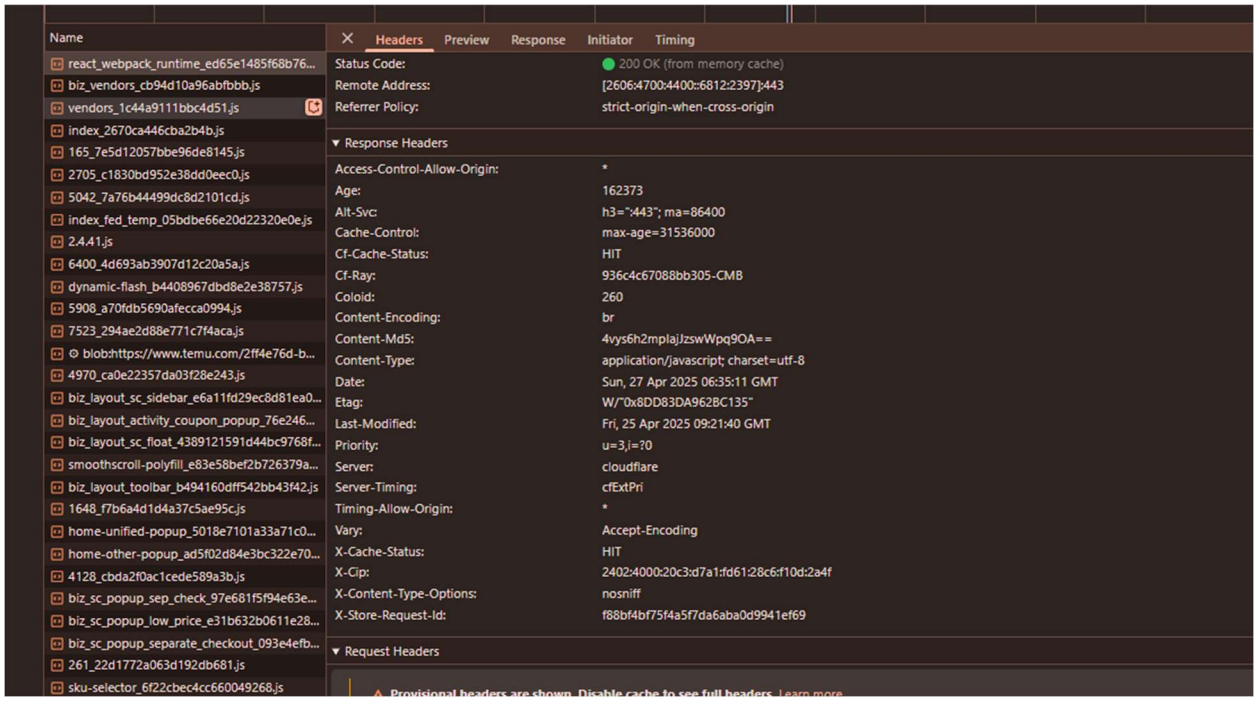
Nikto scan result

```
┌──(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: 1745736091747-07875cab3dd83e80e5b50b8b010e1df3-2.
```

Active scan result from OWASP ZAP:



Developer Tools:



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 –

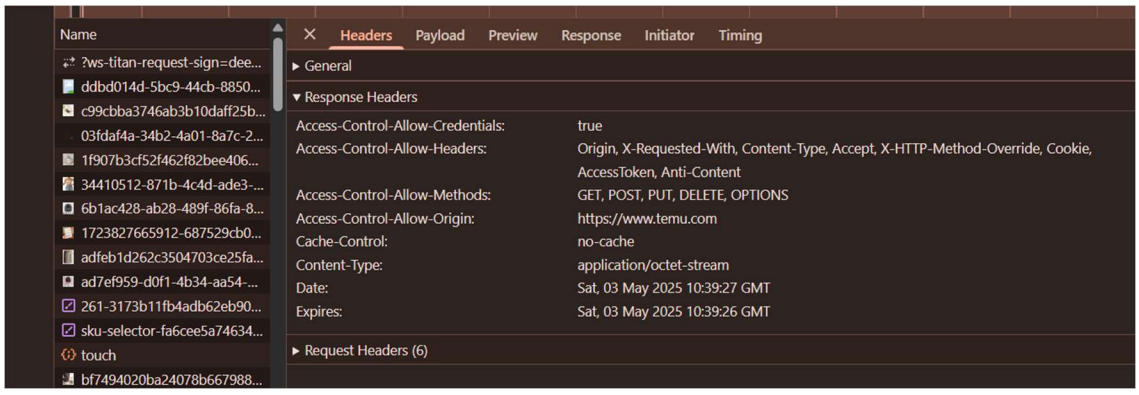
Nikto finding	Meaning	Risk
IP address found in __cf_bm cookie / cip header	Some internal or user IP addresses are leaking into headers and cookies. Could be minor privacy issue.	Low-Medium

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`

- **Developor 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.