Sri Lanka Institute of Information Technology

Year 2 semester 2

IT23360600
G. P. I. Perera

SLIIT KANDY UNI

BUG BOUNTY REPORT 9

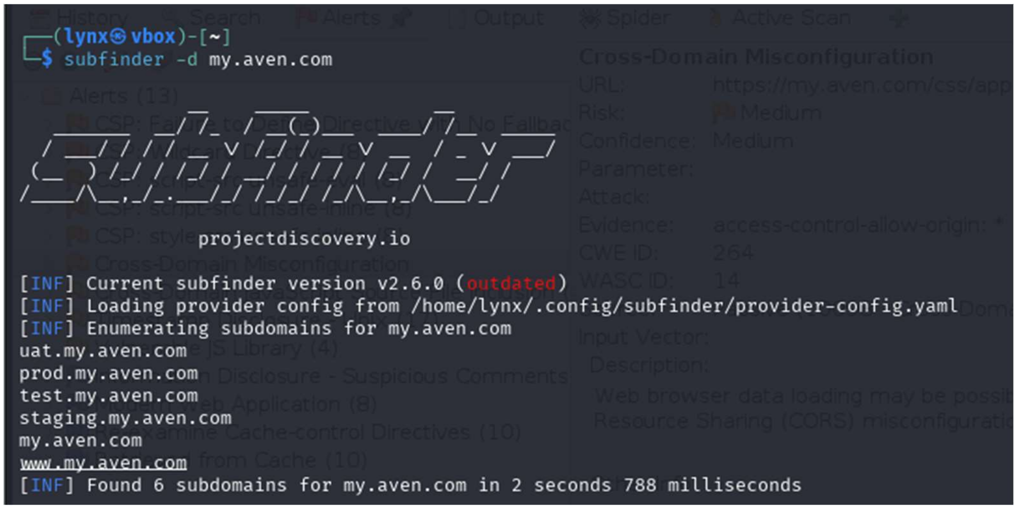
Web Security – IE2062

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

1. Requirement gathering and analysis

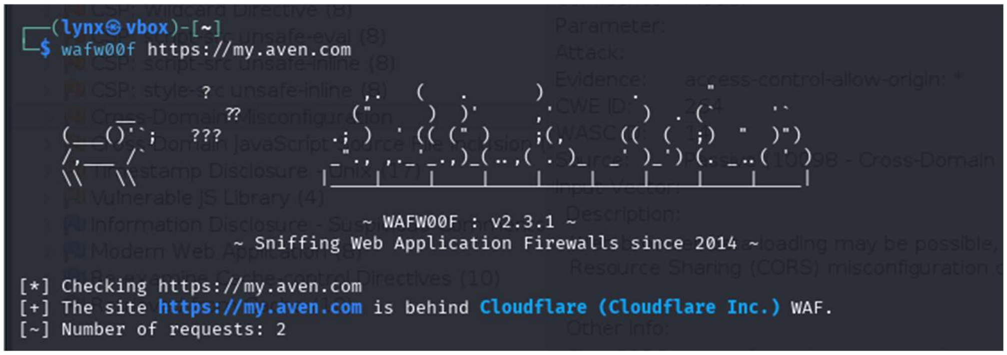
Selected sub domain	aven.com
Hakerone URL	https://hackerone.com/aven_response/
IP address	18.239.153.78

Subdomain list



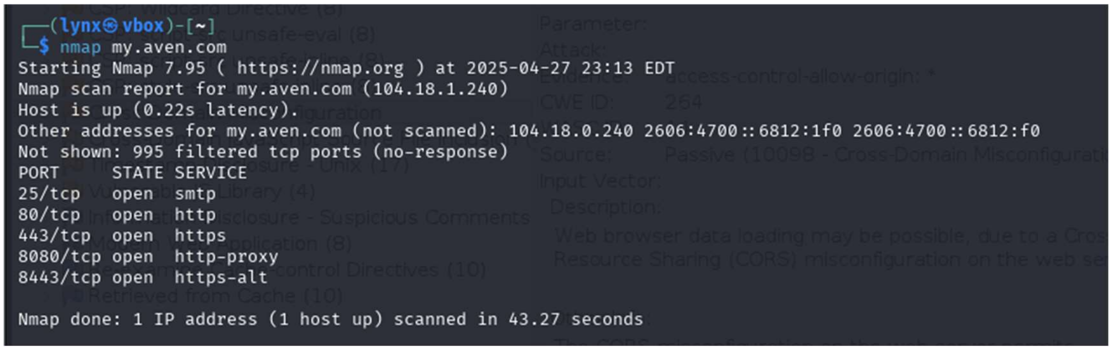
```
┌──(lynx㉿vbox)-[~]
└─$ subfinder -d my.aven.com

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/lynx/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for my.aven.com
uat.my.aven.com
prod.my.aven.com
test.my.aven.com
staging.my.aven.com
my.aven.com
www.my.aven.com
[INF] Found 6 subdomains for my.aven.com in 2 seconds 788 milliseconds
```

Firewall detection:



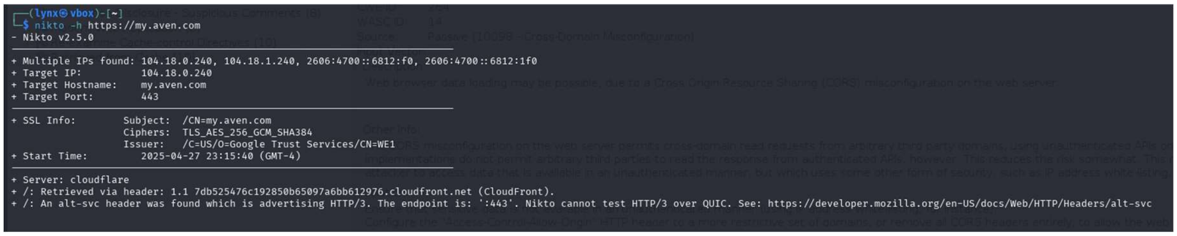
```
┌──(lynx㉿vbox)-[~]
└─$ wafw00f https://my.aven.com

                    ~ WAFW00F : v2.3.1 ~
        ~ Sniffing Web Application Firewalls since 2014 ~

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

Nmap scan:



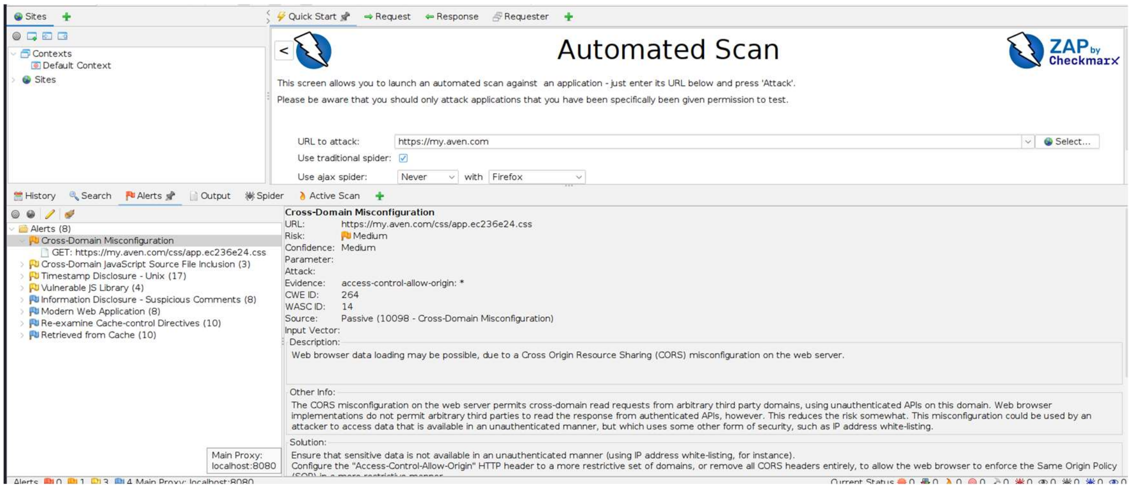
```
┌──(lynx㉿vbox)-[~]
└─$ nmap my.aven.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 23:13 EDT
Nmap scan report for my.aven.com (104.18.1.240)
Host is up (0.22s latency).
Other addresses for my.aven.com (not scanned): 104.18.0.240 2606:4700::6812:1f0 2606:4700::6812:f0
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 43.27 seconds
```

Nikto scan result:



```
┌──(lynx㉿vbox)-[~]
└─$ nikto -h https://my.aven.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.18.0.240, 104.18.1.240, 2606:4700::6812:f0, 2606:4700::6812:1f0
+ Target IP:          104.18.0.240
+ Target Hostname:    my.aven.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=my.aven.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services/CN=WE1
+ Start Time:         2025-04-27 23:15:40 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: Retrieved via header: 1.1 7db525476c192850b65097a6bb612976.cloudfront.net (CloudFront).
+ /: 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
```

Active scan result from OWASP ZAP:



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://my.aven.com

Use traditional spider: ☑

Use ajax spider: Never with Firefox

Alerts (8)
- Cross-Domain Misconfiguration
  - GET: https://my.aven.com/css/app.ec236e24.css
- Cross-Domain JavaScript Source File Inclusion (3)
- Timestamp Disclosure - Unix (17)
- Vulnerable JS Library (4)
- Information Disclosure - Suspicious Comments (8)
- Modern Web Application (8)
- Re-examine Cache-control Directives (10)
- Retrieved from Cache (10)

Main Proxy: localhost:8080

Cross-Domain Misconfiguration

URL: https://my.aven.com/css/app.ec236e24.css
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: access-control-allow-origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:

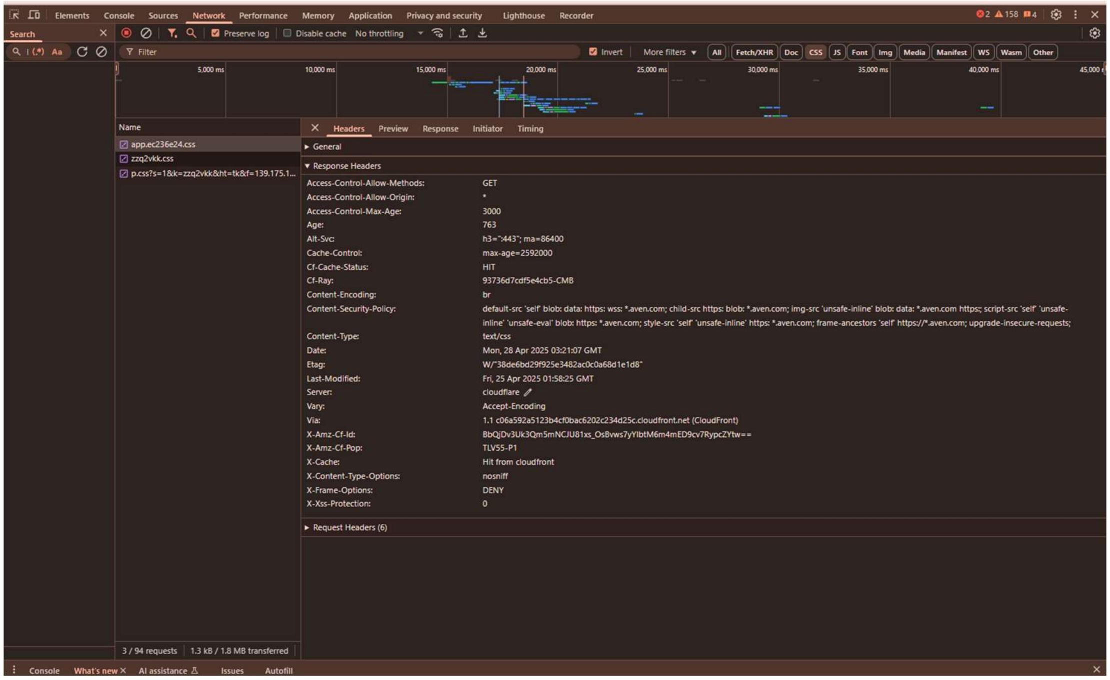
Description:
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Other Info:
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

Solution:
Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

Alerts 0 1 3 4 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 0 0

Developer Tools:



Name
- app.ec236e24.css
- zzq2vkk.css
- p.css?s=1&k=zzq2vkk&ht=tk&f=139.175.1...

3 / 94 requests | 1.3 kB / 1.8 MB transferred

▸ General

▾ Response Headers

Access-Control-Allow-Methods: GET
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 3000
Age: 763
Alt-Svc: h3=":443"; ma=86400
Cache-Control: max-age=2592000
Cf-Cache-Status: HIT
Cf-Ray: 93736d7cdf5e4cb5-CMB
Content-Encoding: br
Content-Security-Policy: default-src 'self' blob: data: https: wss: *.aven.com; child-src https: blob: *.aven.com; img-src 'unsafe-inline' blob: data: *.aven.com https:; script-src 'self' 'unsafe-inline' 'unsafe-eval' blob: https: *.aven.com; style-src 'self' 'unsafe-inline' https: *.aven.com; frame-ancestors 'self' https://*.aven.com; upgrade-insecure-requests;
Content-Type: text/css
Date: Mon, 28 Apr 2025 03:21:07 GMT
Etag: W/"38de6bd29f925e3482ac0c0a68d1e1d8"
Last-Modified: Fri, 25 Apr 2025 01:58:25 GMT
Server: cloudflare
Vary: Accept-Encoding
Via: 1.1 c06a592a5123b4cf0bac6202c234d25c.cloudfront.net (CloudFront)
X-Amz-Cf-Id: BbQjDv3Uk3Qm5mNCJU81xs_OsBvws7yYIbtM6m4mED9cv7RypcZYtw==
X-Amz-Cf-Pop: TLV55-P1
X-Cache: Hit from cloudfront
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 0

▸ Request Headers (6)

2. Report Details

1. Vulnerability Title – Cross-Domain Misconfiguration

2. Vulnerability Description:

The server at https://my.aven.com is improperly configured to allow cross-origin resource sharing (CORS) for unauthorized domains. During testing, it was observed that the Access-Control-Allow-Origin header was set to a wildcard (*), potentially allowing malicious third-party sites to access resources intended only for same-origin use.

Specifically, the asset app.ec236e24.css can be requested and loaded with a cross-origin without any restriction, suggesting a broader CORS misconfiguration across the domain.

Although the specific file tested (app.ec236e24.css) is a static CSS resource and not sensitive by itself, the misconfiguration could extend to API endpoints or sensitive assets in the future, exposing the system to:

- Unauthorized reading of confidential data
- Session hijacking (if credentials are allowed via Access-Control-Allow-Credentials)
- Cross-origin attacks such as **data theft**, **account takeover**, or **privilege escalation**

3. Affected Components:

1. https://my.aven.com/css/app.ec236e24.css

4. Impact Assessment:

OWASP analysis:

Risk level	**Medium**
Confidence	Medium

5. Steps to reproduce –

- **On owasp zap –**

  Start the application, input target URL and run an automated scan.

  Observe alerts.

- **Network developer tools** -
  - Open the web application in your browser
  - Press F12 to open the **Developer Tools**.
  - Go to the **Network** tab.
  - Refresh the page and look for the **HTTP Response Headers** section.
  - Look for the Access-Control-Allow-Origin: *

6. Proposed mitigation or fix

- Restrict Access-Control-Allow-Origin to trusted, specific domains only (no wildcards, no reflection).
- Avoid setting Access-Control-Allow-Credentials: true unless absolutely necessary, and only with exact origin matches.
- Regularly audit CORS configurations, especially on authentication endpoints and sensitive API routes.
- Implement strict server-side validation for Origin headers.