Sri Lanka Institute of Information Technology

Assignment report 08

IT22357762

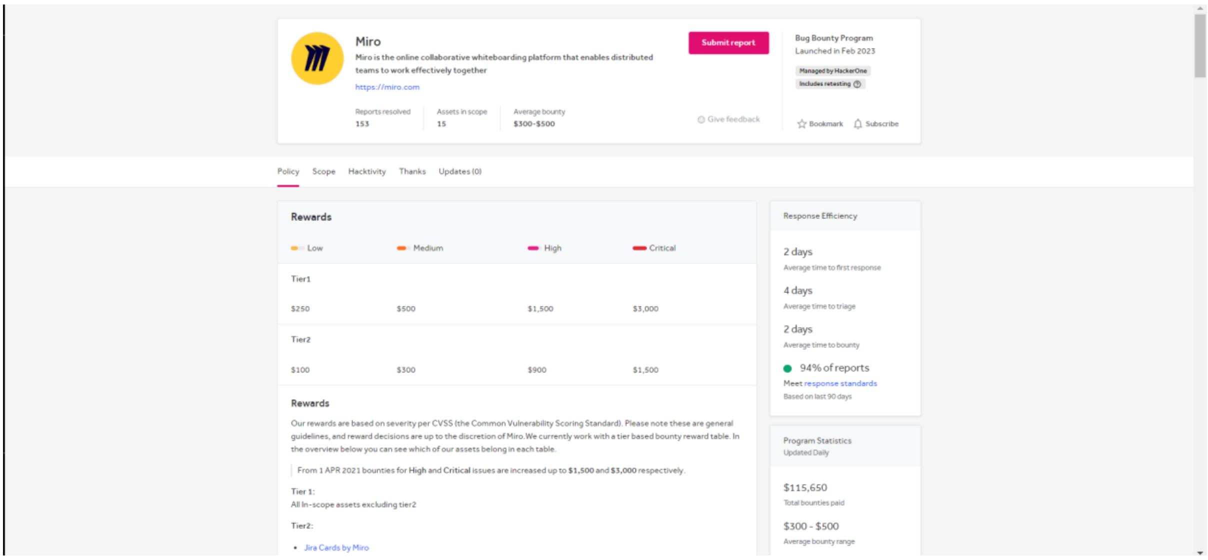
Web Security -IE2062

Web Security – IE2062

B.Sc. (Hons) in Information

Contents

1 miro.com



Miro

Miro is the online collaborative whiteboarding platform that enables distributed teams to work effectively together

https://miro.com

Reports resolved 153

Assets in scope 15

Average bounty $300-$500

Bug Bounty Program

Launched in Feb 2023

Rewards

Low	Medium	High	Critical
Tier1			
$250	$500	$1,500	$3,000
Tier2			
$100	$300	$900	$1,500

Rewards

Our rewards are based on severity per CVSS (the Common Vulnerability Scoring Standard). Please note these are general guidelines, and reward decisions are up to the discretion of Miro.We currently work with a tier based bounty reward table. In the overview below you can see which of our assets belong in each table.

> From 1 APR 2021 bounties for **High** and **Critical** issues are increased up to **$1,500** and **$3,000** respectively.

Tier 1:
All In-scope assets excluding tier2

Tier2:

- Jira Cards by Miro

Response Efficiency

2 days
Average time to first response

4 days
Average time to triage

2 days
Average time to bounty

● 94% of reports
Meet response standards
Based on last 90 days

Program Statistics
Updated Daily

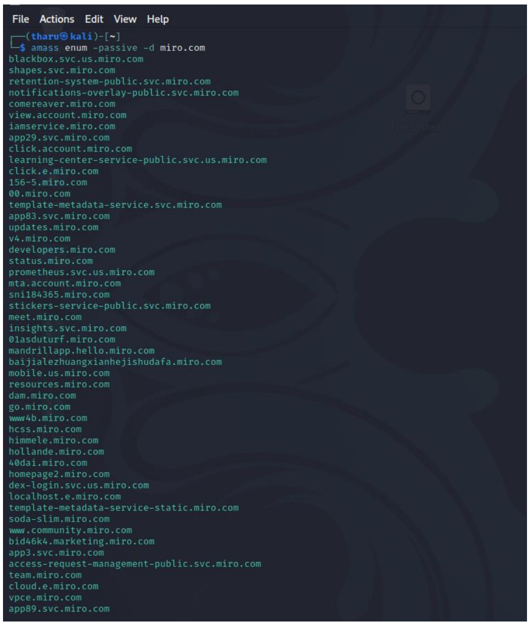
$115,650
Total bounties paid

$300 - $500
Average bounty range

1.1 Sub- domain list

Tool – amass

Command – amass enum -passive -d miro.com



```
┌──(tharu㉿kali)-[~]
└─$ amass enum -passive -d miro.com
blackbox.svc.us.miro.com
shapes.svc.miro.com
retention-system-public.svc.miro.com
notifications-overlay-public.svc.miro.com
comereaver.miro.com
view.account.miro.com
iamservice.miro.com
app29.svc.miro.com
click.account.miro.com
learning-center-service-public.svc.us.miro.com
click.e.miro.com
156-5.miro.com
00.miro.com
template-metadata-service.svc.miro.com
app83.svc.miro.com
updates.miro.com
v4.miro.com
developers.miro.com
status.miro.com
prometheus.svc.us.miro.com
mta.account.miro.com
sni184365.miro.com
stickers-service-public.svc.miro.com
meet.miro.com
insights.svc.miro.com
01asduturf.miro.com
mandrillapp.hello.miro.com
baijialezhuangxianhejishudafa.miro.com
mobile.us.miro.com
resources.miro.com
dam.miro.com
go.miro.com
www4b.miro.com
hcss.miro.com
himmele.miro.com
hollande.miro.com
40dai.miro.com
homepage2.miro.com
dex-login.svc.us.miro.com
localhost.e.miro.com
template-metadata-service-static.miro.com
soda-slim.miro.com
www.community.miro.com
bid46k4.marketing.miro.com
app3.svc.miro.com
access-request-management-public.svc.miro.com
team.miro.com
cloud.e.miro.com
vpce.miro.com
app89.svc.miro.com
```

Sub domain list –

- blackbox.svc.us.miro.com
- shapes.svc.miro.com
- retention-system-public.svc.miro.com
- notifications-overlay-public.svc.miro.com
- comereaver.miro.com
- view.account.miro.com
- iamservice.miro.com
- app29.svc.miro.com
- click.account.miro.com
- learning-center-service-public.svc.us.miro.com
- click.e.miro.com
- 156-5.miro.com
- 00.miro.com
- template-metadata-service.svc.miro.com
- app83.svc.miro.com
- updates.miro.com
- v4.miro.com
- developers.miro.com
- status.miro.com
- prometheus.svc.us.miro.com
- mta.account.miro.com
- sni184365.miro.com
- stickers-service-public.svc.miro.com
- meet.miro.com
- insights.svc.miro.com
- 01asduturf.miro.com
- mandrillapp.hello.miro.com
- baijialezhuangxianhejishudafa.miro.com
- mobile.us.miro.com
- resources.miro.com
- dam.miro.com
- go.miro.com
- www4b.miro.com
- hcss.miro.com
- himmele.miro.com
- hollande.miro.com
- 40dai.miro.com
- homepage2.miro.com
- dex-login.svc.us.miro.com
- localhost.e.miro.com
- template-metadata-service-static.miro.com
- soda-slim.miro.com
- www.community.miro.com
- bid46k4.marketing.miro.com
- app3.svc.miro.com
- access-request-management-public.svc.miro.com
- team.miro.com
- cloud.e.miro.com
- vpce.miro.com
- app89.svc.miro.com
- app1.svc.miro.com
- api.eu01.miro.com
- notifications-email.svc.us.miro.com

- phone.miro.com
- r01.miro.com
- template-metadata-service-public.svc.miro.com
- m.b.hollande.miro.com
- e.miro.com
- humana.miro.com
- jrigwqfdrha847.miro.com
- ad.miro.com
- mandrillapp.miro.com
- www5f.miro.com
- app21.svc.miro.com
- sticker-beta.miro.com
- sni208637.miro.com
- mandrillapp.billing.miro.com
- template-social-service-public.svc.miro.com
- brandkit.miro.com
- board-recording-service-private.svc.miro.com
- image.e.miro.com
- test-esa.miro.com
- app23.svc.miro.com
- app82.svc.miro.com
- exclusivejeans.miro.com
- marketplace.svc.miro.com
- dex.svc.miro.com
- learns.miro.com
- template-metadata-service-public.svc.us.miro.com
- mwww.miro.com
- board-recording-storage.miro.com
- app32.svc.miro.com
- int-blog.miro.com
- insights-public.svc.miro.com
- marketplace-static.us.miro.com
- mona.miro.com
- n.m.b.hollande.miro.com
- externalapi.miro.com
- sign-in-public.svc.miro.com
- eventhub.eu01.miro.com
- sni225463.miro.com
- app43.svc.miro.com
- api.miro.com
- vendor-icons.svc.miro.com
- rc.meet.miro.com
- convidado.miro.com
- kratosdefense.miro.com
- developers.us.miro.com
- ai-proxy-service-public.svc.miro.com
- r01.us.miro.com
- cv-apps.svc.us.miro.com
- integrations.us01.miro.com
- pages.e.miro.com
- mandrillapp.notifications.miro.com
- demo.miro.com
- account.miro.com
- jessicas-senior--1.miro.com
- pages.account.miro.com
- admin.miro.com

- dex-login.svc.miro.com
- support.miro.com
- payment-public.svc.us.miro.com
- fe-rtm.eu01.miro.com
- svc.us.miro.com
- image.account.miro.com
- cloud.miro.com
- payment.svc.miro.com
- communitygroups.miro.com
- app52.svc.miro.com
- help.miro.com
- szkolamuzyczna.miro.com
- ww.miro.com
- com.miro.com
- r.miro.com
- ea.developers.miro.com
- app48.svc.miro.com
- sni41174.miro.com
- cutoff.svc.miro.com
- sierraspace.miro.com
- harborfreight.miro.com
- eu01.miro.com
- integrations.miro.com
- wwww.miro.com
- mta.e.miro.com
- roboticresearch.miro.com
- web.miro.com
- app15.svc.miro.com
- payment.svc.us.miro.com
- template-social-service.svc.miro.com
- svg-convert.eu01.miro.com
- svc.miro.com
- api.us01.miro.com
- brand.miro.com
- app47.svc.miro.com
- professionaltrainer.miro.com
- links.m.miro.com
- msbot.svc.miro.com
- lefleury.miro.com
- alertmanager.svc.us.miro.com
- cdn.miro.com
- identity-public.svc.miro.com
- app31.svc.miro.com
- msbot-public.svc.us.miro.com
- 04-events.miro.com
- marketplace.svc.us.miro.com
- internalapi.miro.com
- corp.miro.com
- template-social-service.svc.us.miro.com
- access-request-management-public.svc.us.miro.com
- cloud.account.miro.com
- app39.svc.miro.com
- xn--oqe.miro.com
- community-profiles-service-public.svc.miro.com
- fe-rtm.us01.miro.com
- otile2.miro.com

- debtcounselling.miro.com
- shapes.miro.com
- us01.miro.com
- sni253985.miro.com
- academy.miro.com
- goldilocks.svc.miro.com
- board-recording-service-1.svc.miro.com
- app7.svc.miro.com
- app20.svc.miro.com
- email.info.miro.com
- board-recording-service.svc.miro.com
- shop.miro.com
- app22.svc.miro.com
- _dmarc.miro.com
- cdt.miro.com
- 10730.miro.com
- learning-center-service.svc.us.miro.com
- info.miro.com
- app51.svc.miro.com
- email.miro.com
- help.us.miro.com
- dr-dbdr-euc1.dr.miro.com
- encore-2018-portail.miro.com
- xn--p1ai.miro.com
- coopersquare.miro.com
- hello.svc.miro.com
- baoimage.miro.com
- svc.eu01.miro.com
- org.miro.com
- msbot-public.svc.miro.com
- adm-marketplace.miro.com
- beta.miro.com
- sticker.miro.com
- blackbox.svc.miro.com
- zendesk2.miro.com
- app10.svc.miro.com
- zendesk1.miro.com
- notifications-email.svc.miro.com
- beta.developers.miro.com
- app38.svc.miro.com
- disabledtesla.miro.com
- mmankin.miro.com
- miro-us.miro.com
- alertmanager.svc.miro.com
- static-website.miro.com
- www.miro.com
- sni51763.miro.com
- sof1.miro.com
- vendor-icons.svc.us.miro.com
- app40.svc.miro.com
- svc.us01.miro.com
- bounces.miro.com
- b.hollande.miro.com
- trust.miro.com
- board-recording-service-public.svc.miro.com
- jira-cards.miro.com

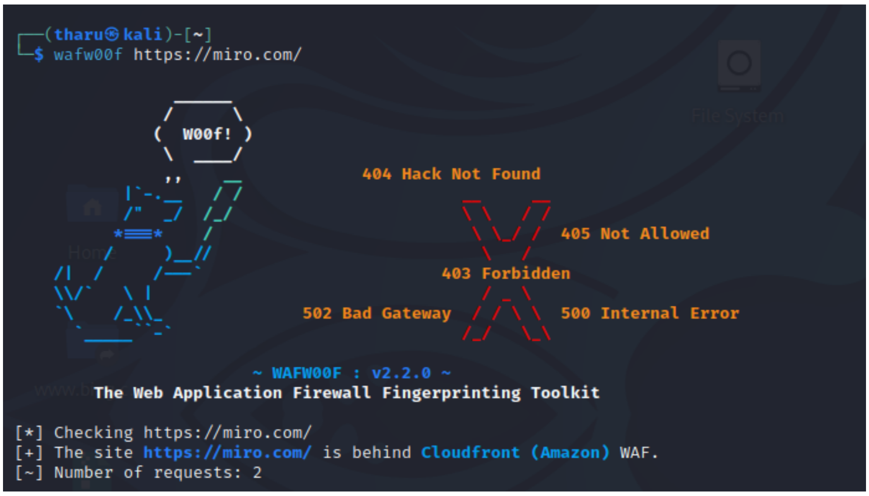
- hello.miro.com
- app12.svc.miro.com
- app88.svc.miro.com
- learning-center-service.svc.miro.com
- cv-apps.svc.miro.com
- app81.svc.miro.com
- distributed.miro.com
- miskofinance.miro.com
- trcksplt.miro.com
- app14.svc.miro.com
- image-segmentation-public.svc.miro.com
- app46.svc.miro.com
- trial-community.miro.com
- app28.svc.miro.com
- zoom-app-backend.svc.us.miro.com
- dub2.miro.com
- app11.svc.miro.com
- adm-marketplace.svc.miro.com
- grosirkaospolos.miro.com
- ext-blog.miro.com
- app19.svc.miro.com
- mobile.miro.com
- stickers-service-public.svc.us.miro.com
- r.us.miro.com
- integrations-internal.miro.com
- ftp.miro.com
- google-meet-integration.svc.miro.com
- gslink.miro.com
- app2.svc.miro.com
- zoom-app-backend.svc.miro.com
- app25.svc.miro.com
- esplorarebergamo.miro.com
- app42.svc.miro.com
- mta3.account.miro.com
- externalapi.us.miro.com
- admin.us.miro.com
- events.miro.com
- app26.svc.miro.com
- heb.miro.com
- learning-center-service-public.svc.miro.com
- sni117180.miro.com
- mandrillapp.updates.miro.com
- elb.miro.com
- adm-marketplace.svc.us.miro.com
- gtmail.miro.com
- track.miro.com
- consultantcommunity.miro.com
- app41.svc.miro.com
- qa.miro.com
- agonizing.miro.com
- caramembuatjus.miro.com
- buf.miro.com
- staging.miro.com
- hello-pub.svc.miro.com
- apina21.miro.com
- view.e.miro.com

- app5.svc.miro.com
- m.miro.com
- dex.svc.us.miro.com
- eventhub-public.svc.miro.com
- _amazonses.miro.com
- www1.miro.com
- webctdev.miro.com
- mta2.account.miro.com
- retention-system-public.svc.us.miro.com
- billing.miro.com
- app24.svc.miro.com
- lubo.miro.com
- notifications-overlay.svc.us.miro.com
- hillsgrammar.miro.com
- 1e30a.miro.com
- learning-center-service-1.svc.us.miro.com
- lapedrera.miro.com
- test-org.miro.com
- bl.miro.com
- app4.svc.miro.com
- www.help.miro.com
- files.miro.com
- go2.miro.com
- us.miro.com
- integrations.eu01.miro.com
- enterpriseadvocates.miro.com
- zendesk4.miro.com
- bid46k4.3782705m.miro.com
- app37.svc.miro.com
- templates.miro.com
- zendesk3.miro.com
- eventhub.us01.miro.com
- cdcr.miro.com
- app91.svc.miro.com
- app9.svc.miro.com
- payment-public.svc.miro.com
- notifications.miro.com
- insights.svc.us.miro.com
- www.events.miro.com
- prometheus.svc.miro.com
- miro.com
- desktop.miro.com
- msbot.svc.us.miro.com
- richese.miro.com
- stage.meet.miro.com
- community.miro.com
- jaeger.svc.miro.com
- internal.miro.com
- shapes.svc.us.miro.com
- mail.miro.com
- jaeger.svc.us.miro.com
- segmentation-public.svc.miro.com
- marketplace-static.miro.com
- app13.svc.miro.com
- marketing.miro.com
- blog.miro.com

- identity-public.svc.us.miro.com
- app45.svc.miro.com
- notifications-overlay.svc.miro.com
- desktop2.miro.com
- app6.svc.miro.com

1.2 Firewall detection

Command – wafw00f https://miro.com /

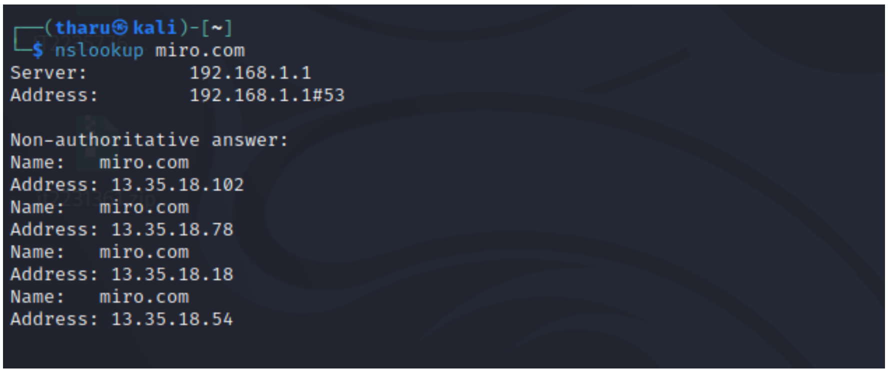


```
┌──(tharu㉿kali)-[~]
└─$ wafw00f https://miro.com/

                 ( 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://miro.com/
[+] The site https://miro.com/ is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

1.3 IP scanning

Tool – nslookup

Command – nslookup miro.com

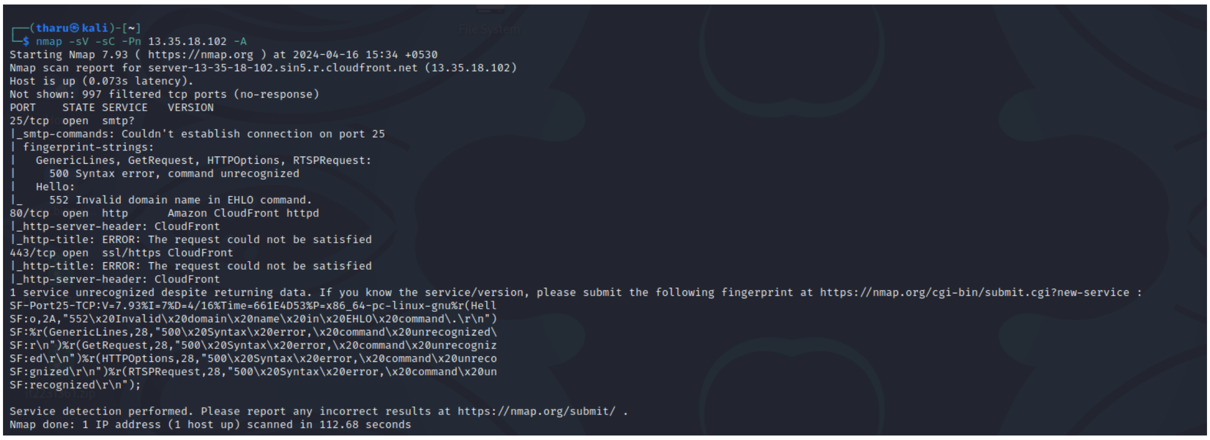


```
┌──(tharu㉿kali)-[~]
└─$ nslookup miro.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   miro.com
Address: 13.35.18.102
Name:   miro.com
Address: 13.35.18.78
Name:   miro.com
Address: 13.35.18.18
Name:   miro.com
Address: 13.35.18.54
```

1.4 Port scanning

Tool - nmap

Command – nmap -sV -sC -Pn 13.35.18.102 -A

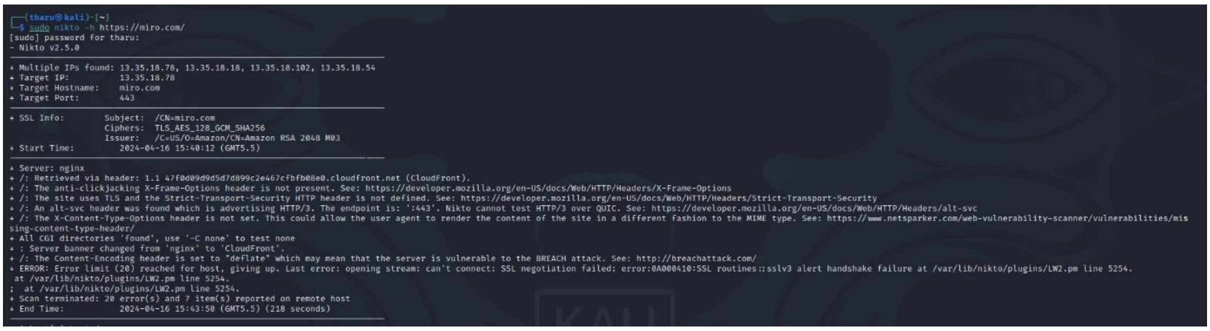


```
┌──(tharu㉿kali)-[~]
└─$ nmap -sV -sC -Pn 13.35.18.102 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-16 15:34 +0530
Nmap scan report for server-13-35-18-102.sin5.r.cloudfront.net (13.35.18.102)
Host is up (0.073s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
25/tcp  open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     500 Syntax error, command unrecognized
|   Hello:
|_    552 Invalid domain name in EHLO command.
80/tcp  open  http      Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: ERROR: The request could not be satisfied
443/tcp open  ssl/https CloudFront
|_http-title: ERROR: The request could not be satisfied
|_http-server-header: CloudFront
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.93%I=7%D=4/16%Time=661E4D53%P=x86_64-pc-linux-gnu%r(Hell
SF:o,2A,"552\x20Invalid\x20domain\x20name\x20in\x20EHLO\x20command\.\r\n")
SF:%r(GenericLines,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\
SF:r\n")%r(GetRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecogniz
SF:ed\r\n")%r(HTTPOptions,28,"500\x20Syntax\x20error,\x20command\x20unreco
SF:gnized\r\n")%r(RTSPRequest,28,"500\x20Syntax\x20error,\x20command\x20un
SF:recognized\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 112.68 seconds
```

1.5 Nikto scanning

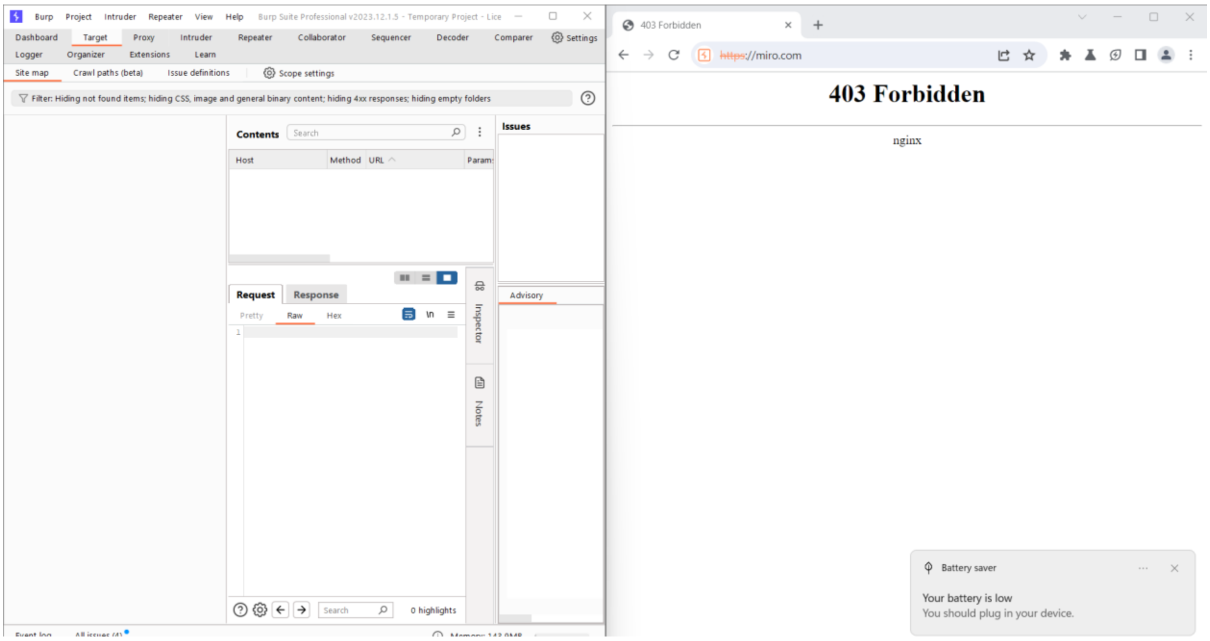
Tool – Nikto

Command - sudo nikto -h miro.com



```
┌──(tharu㉿kali)-[~]
└─$ sudo nikto -h https://miro.com/
[sudo] password for tharu:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 13.35.18.78, 13.35.18.18, 13.35.18.102, 13.35.18.54
+ Target IP:          13.35.18.78
+ Target Hostname:    miro.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=miro.com
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=Amazon/CN=Amazon RSA 2048 M03
+ Start Time:         2024-04-16 15:40:12 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx
+ /: Retrieved via header: 1.1 47f0d09d9d5d7d899c2e467cfbfb08e0.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: 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/mis
sing-content-type-header/
+ All CGI directories 'found', use '-C none' to test none
+ : Server banner changed from 'nginx' to 'CloudFront'.
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::sslv3 alert handshake failure 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 7 item(s) reported on remote host
+ End Time:           2024-04-16 15:43:50 (GMT5.5) (218 seconds)
---------------------------------------------------------------------------
```

1.6 Burpsuite scanning



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

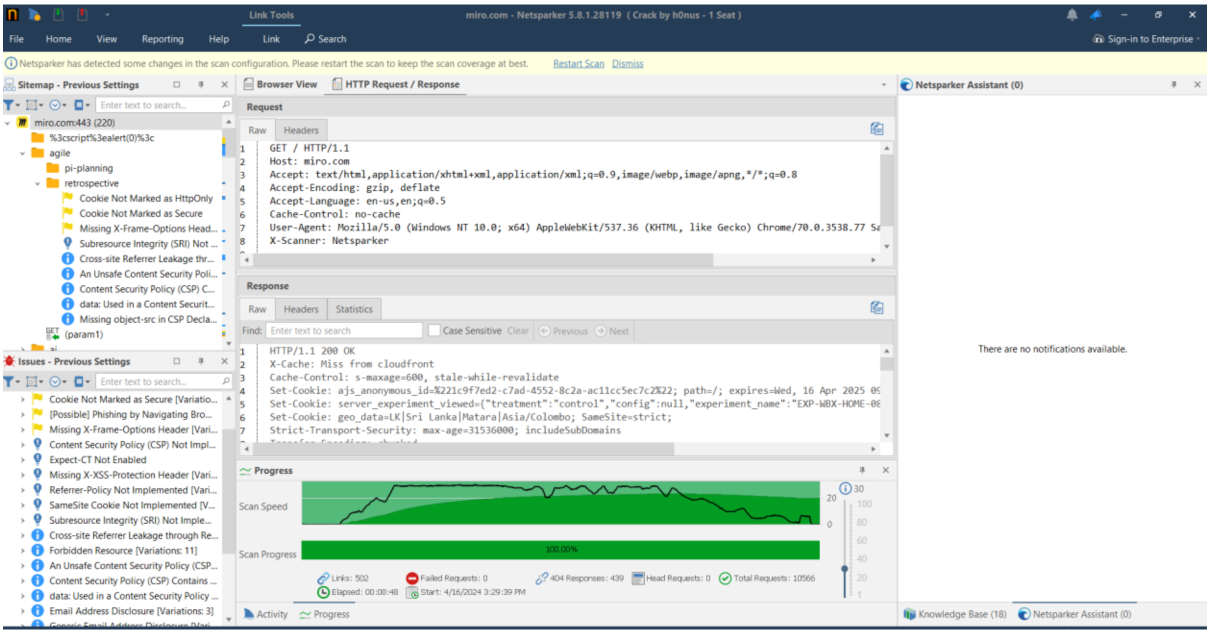
403 Forbidden

nginx

Battery saver

Your battery is low
You should plug in your device.

1.7 Netspaker scan



Netsparker has detected some changes in the scan configuration. Please restart the scan to keep the scan coverage at best.

- miro.com:443 (220)
  - %3cscript%3ealert(0)%3c
  - agile
    - pi-planning
    - retrospective
      - Cookie Not Marked as HttpOnly
      - Cookie Not Marked as Secure
      - Missing X-Frame-Options Head...
      - Subresource Integrity (SRI) Not ...
      - Cross-site Referrer Leakage thr...
      - An Unsafe Content Security Poli...
      - Content Security Policy (CSP) C...
      - data: Used in a Content Securit...
      - Missing object-src in CSP Decla...
    - GET (param1)

```
GET / HTTP/1.1
Host: miro.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Sa
X-Scanner: Netsparker
```

```
HTTP/1.1 200 OK
X-Cache: Miss from cloudfront
Cache-Control: s-maxage=600, stale-while-revalidate
Set-Cookie: ajs_anonymous_id=%221c9f7ed2-c7ad-4552-8c2a-ac11cc5ec7c2%22; path=/; expires=Wed, 16 Apr 2025 09
Set-Cookie: server_experiment_viewed={"treatment":"control","config":null,"experiment_name":"EXP-WBX-HOME-08
Set-Cookie: geo_data=LK|Sri Lanka|Matara|Asia/Colombo; SameSite=strict;
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

- Cookie Not Marked as Secure [Variatio...
- [Possible] Phishing by Navigating Bro...
- Missing X-Frame-Options Header [Vari...
- Content Security Policy (CSP) Not Impl...
- Expect-CT Not Enabled
- Missing X-XSS-Protection Header [Vari...
- Referrer-Policy Not Implemented [Vari...
- SameSite Cookie Not Implemented [V...
- Subresource Integrity (SRI) Not Imple...
- Cross-site Referrer Leakage through Re...
- Forbidden Resource [Variations: 11]
- An Unsafe Content Security Policy (CSP...
- Content Security Policy (CSP) Contains ...
- data: Used in a Content Security Policy ...
- Email Address Disclosure [Variations: 3]

Links: 502 Failed Requests: 0 404 Responses: 439 Head Requests: 0 Total Requests: 10566
Elapsed: 00:08:48 Start: 4/16/2024 3:29:39 PM

There are no notifications available.

1.8 Vulnerabilities

Vulnerability Title: Security Vulnerabilities in Cookie Handling

Vulnerability Description: The application possesses two crucial security flaws pertaining to the management of cookies. The application is vulnerable to potential cross-site scripting (XSS) attacks due to the presence of non-HTTPOnly cookies. Unsecured cookies provide a danger of exposing sensitive information when transmitted across unsecured channels.

Affected Components: geo_data cookie

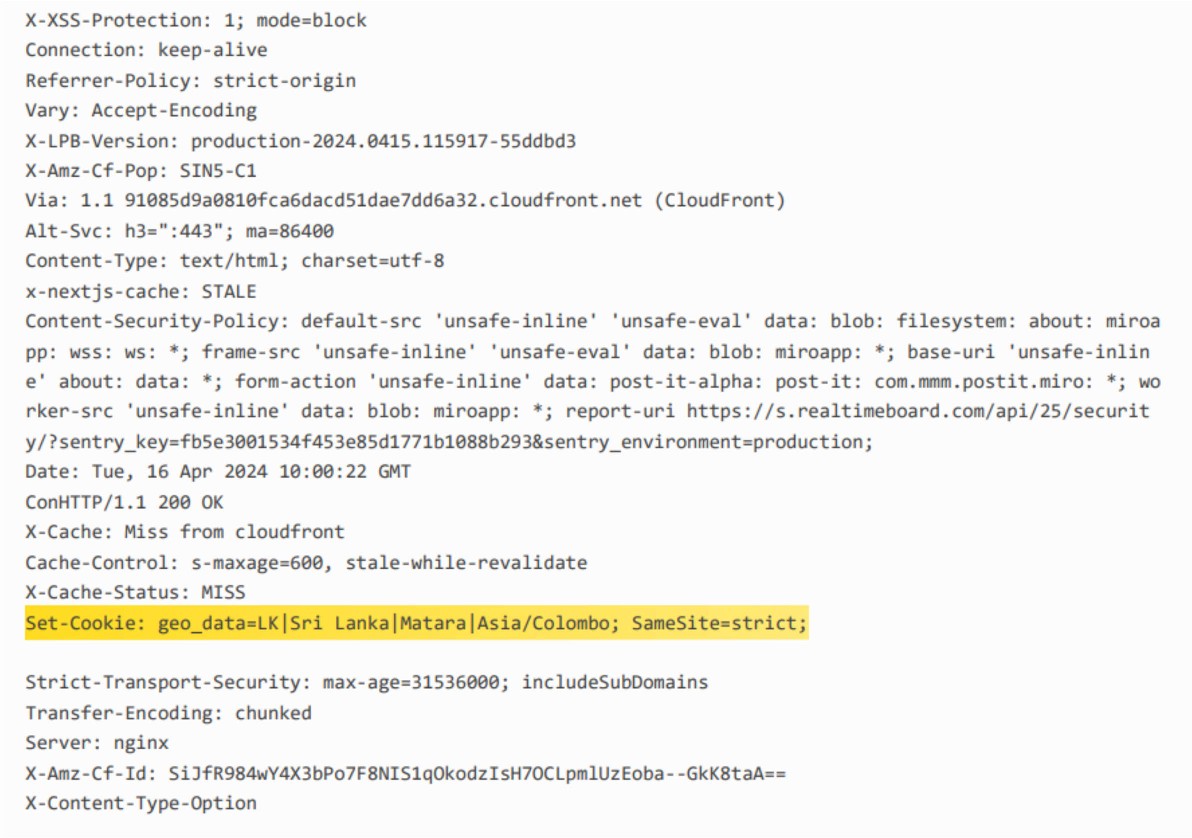
Impact Assessment: Impact of vulnerability includes,

- Session hijacking
- Data interception
- Sensitive cookies theft

Steps to Reproduce:

1. Navigate to https://miro.com/agile/retrospective/
2. Inspect the HTTP headers exchanged during the request.
3. Identify the presence of the "geo_data" cookie without the HTTPOnly and Secure flags.
4. Note that the cookie can be accessed by client-side scripts and is transmitted over HTTP, respectively.

Proof of concept:



```
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Referrer-Policy: strict-origin
Vary: Accept-Encoding
X-LPB-Version: production-2024.0415.115917-55ddbd3
X-Amz-Cf-Pop: SIN5-C1
Via: 1.1 91085d9a0810fca6dacd51dae7dd6a32.cloudfront.net (CloudFront)
Alt-Svc: h3=":443"; ma=86400
Content-Type: text/html; charset=utf-8
x-nextjs-cache: STALE
Content-Security-Policy: default-src 'unsafe-inline' 'unsafe-eval' data: blob: filesystem: about: miroa
pp: wss: ws: *; frame-src 'unsafe-inline' 'unsafe-eval' data: blob: miroapp: *; base-uri 'unsafe-inlin
e' about: data: *; form-action 'unsafe-inline' data: post-it-alpha: post-it: com.mmm.postit.miro: *; wo
rker-src 'unsafe-inline' data: blob: miroapp: *; report-uri https://s.realtimeboard.com/api/25/securit
y/?sentry_key=fb5e3001534f453e85d1771b1088b293&sentry_environment=production;
Date: Tue, 16 Apr 2024 10:00:22 GMT
ConHTTP/1.1 200 OK
X-Cache: Miss from cloudfront
Cache-Control: s-maxage=600, stale-while-revalidate
X-Cache-Status: MISS
Set-Cookie: geo_data=LK|Sri Lanka|Matara|Asia/Colombo; SameSite=strict;

Strict-Transport-Security: max-age=31536000; includeSubDomains
Transfer-Encoding: chunked
Server: nginx
X-Amz-Cf-Id: SiJfR984wY4X3bPo7F8NIS1qOkodzIsH7OCLpmlUzEoba--GkK8taA==
X-Content-Type-Option
```

Proposed Mitigation or Fix:

- Mark the "geo_data" cookie as HTTPOnly to mitigate XSS attacks.
- Mark all cookies used within the application as Secure to ensure they are transmitted only over secure channels.
- Regularly review and update the application's security policies and configurations to prevent similar vulnerabilities in the future

1.8.1 Other vulnerabilities

1. Missing X-Frame-Options Header.
2. Content Security Policy (CSP) Not Implemented
3. Expect-CT Not Enabled
4. Missing X-XSS-Protection Header
5. Referrer-Policy Not Implemented
6. SameSite Cookie Not Implemented
7. Subresource Integrity (SRI) Not Implemented
8. An Unsafe Content Security Policy (CSP) Directive in Use
9. Content Security Policy (CSP) Contains Out of Scope report-uri Domain
10. data: Used in a Content Security Policy (CSP) Directive
11. Email Address Disclosure
12. Generic Email Address Disclosure
13. Insecure Protocol Detected in Content Security Policy (CSP)
14. Missing object-src in CSP Declaration
15. Nginx Web Server Identified
16. Reverse Proxy Detected (Envoy)
17. Web Application Firewall Detected
18. Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive
19. Cross-site Referrer Leakage through Referrer-Policy
20. Forbidden Resource