Sri Lanka Institute of Information Technology

Web Security – IE 2062

Bug Bounty - Journal Book

IT22123404 - WIJESINGHE R P D K N

Introduction

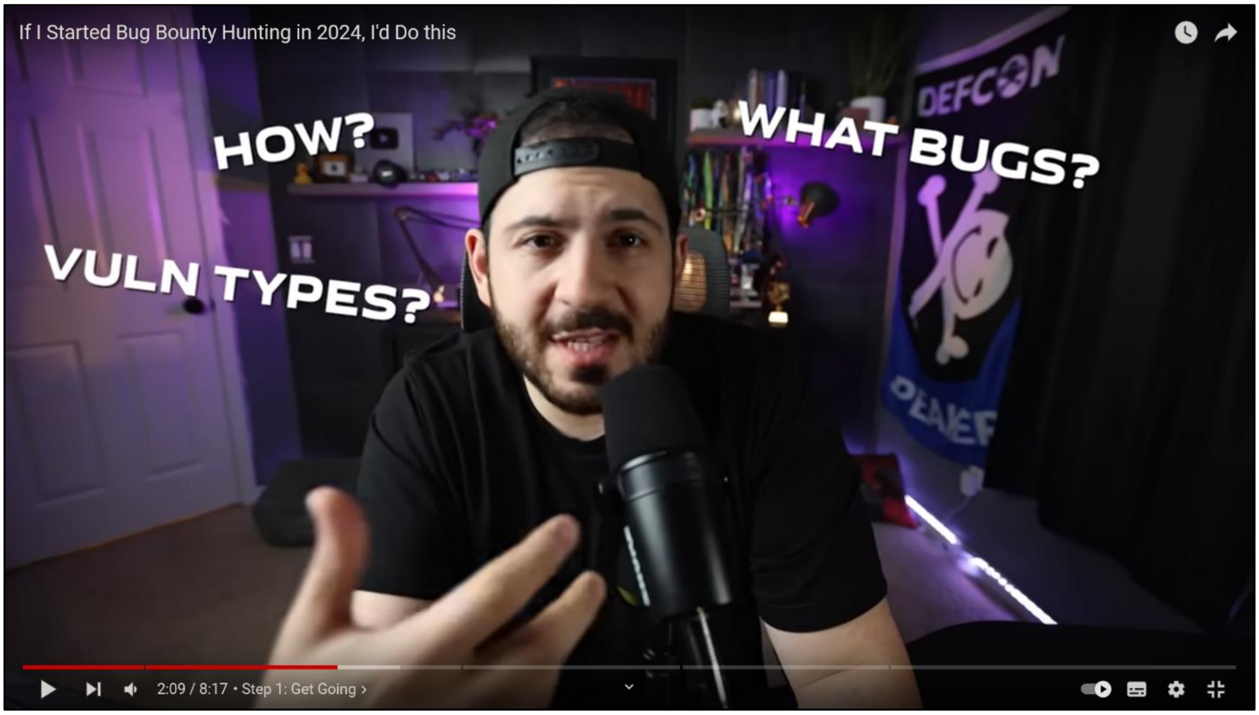
In the ever-evolving landscape of cybersecurity ,hunting for vulnerabilities play a crucial role.it is somewhat essential in the present get updated about the security vulnerabilities and know how they effect the user experience in a website or a web application.

Welcome to this journal of mine which I maintained throughout my bug bounty journey.In this journal I hope to give a insight about my experience, discuss the challenges I faced and how I overcame those challenges.join me through my journey bug bounty with this journal.

Chapter One – Getting informed

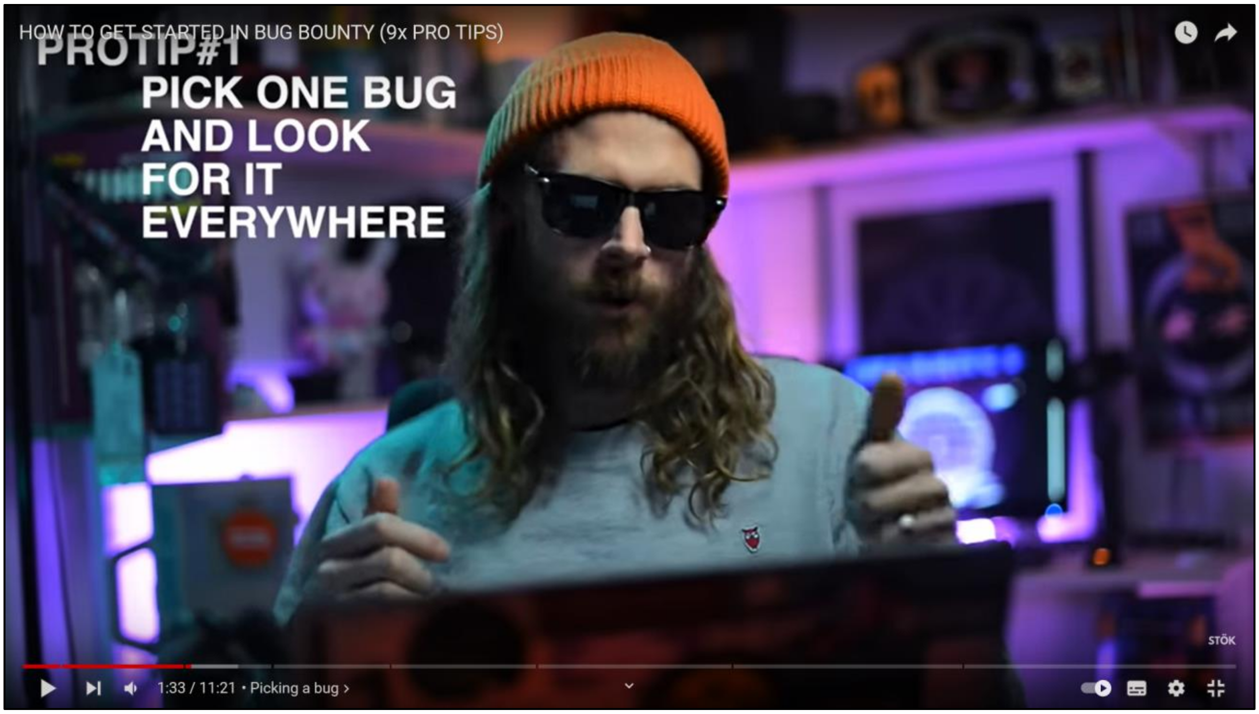
Day 1 and 2

To begin my bug bounty process first of all I started to search what bug bounty is.for that I started to search the internet for educational videos and documents.i went through and watched few videos of famous Youtubers like NahamSec (https://www.youtube.com/@NahamSec) and STOK (https://www.youtube.com/@STOKfredrik) About how to get started with bug bounty,what are the basics of bug bounty, how to find my first vulnerability etc

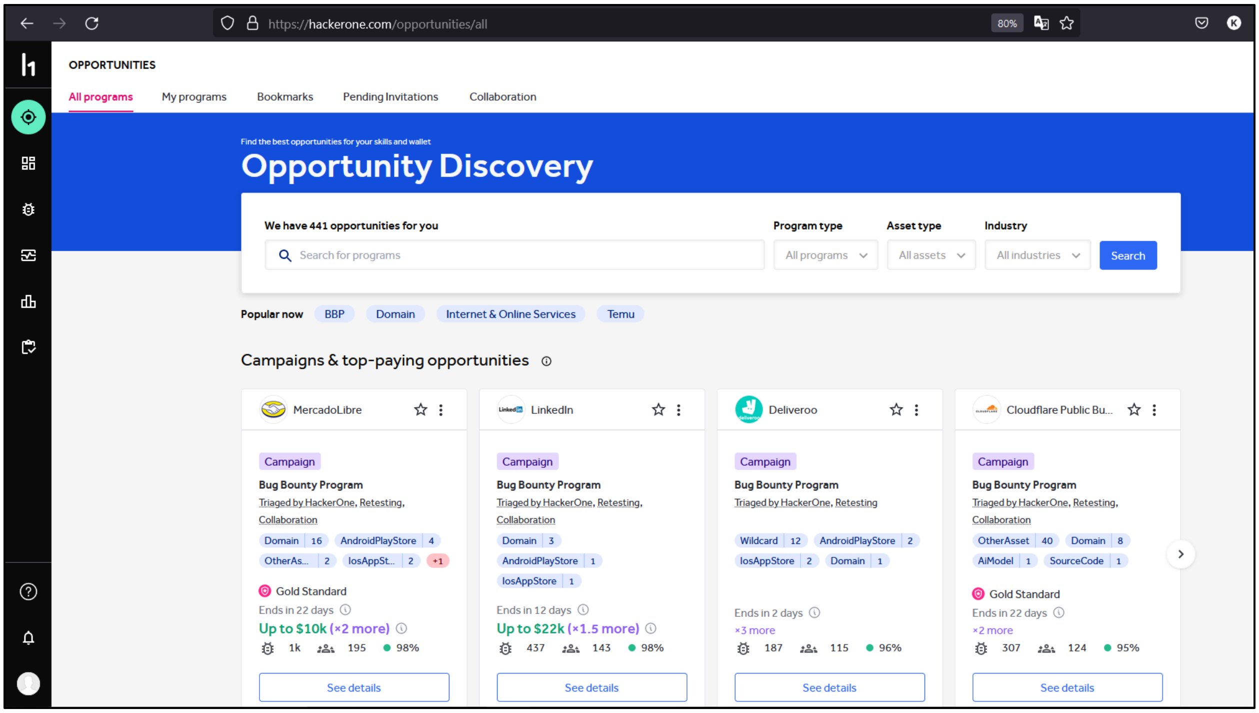


If I Started Bug Bounty Hunting in 2024, I'd Do this

2:09 / 8:17 • Step 1: Get Going ›


HOW TO GET STARTED IN BUG BOUNTY (9x PRO TIPS)
PROTIP#1
PICK ONE BUG AND LOOK FOR IT EVERYWHERE
STÖK
1:33 / 11:21 • Picking a bug ›

Following that I went to the bug bounty platforms such as hackerone.com and bugcrowd.com.i waned to get a general idea about how these platforms work so I took some time and navigated through both sites and got familiarized with their interface and how they offer bug bounty programs,what are the different types of available programs,how the bug bounty community operates etc.



https://hackerone.com/opportunities/all

OPPORTUNITIES

All programs | My programs | Bookmarks | Pending Invitations | Collaboration

Find the best opportunities for your skills and wallet

Opportunity Discovery

We have 441 opportunities for you

Search for programs

Program type: All programs | Asset type: All assets | Industry: All industries | Search

Popular now: BBP | Domain | Internet & Online Services | Temu

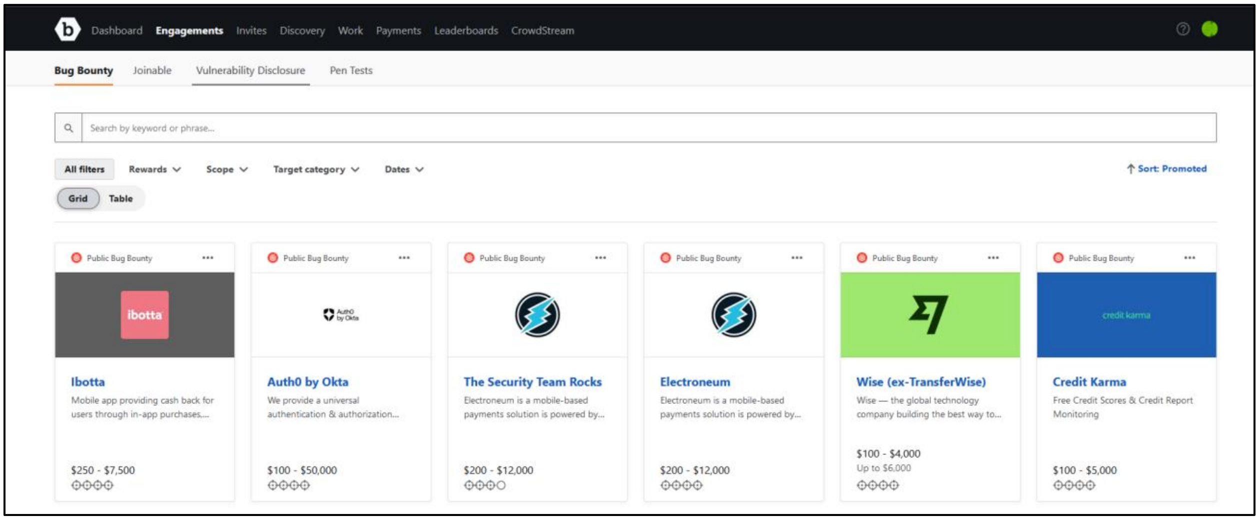
Campaigns & top-paying opportunities

MercadoLibre
Campaign
Bug Bounty Program
Triaged by HackerOne, Retesting, Collaboration
Domain 16 | AndroidPlayStore 4 | OtherAs... 2 | IosAppSt... 2 | +1
Gold Standard
Ends in 22 days
Up to $10k (×2 more)
1k | 195 | 98%
See details

LinkedIn
Campaign
Bug Bounty Program
Triaged by HackerOne, Retesting, Collaboration
Domain 3 | AndroidPlayStore 1 | IosAppStore 1
Ends in 12 days
Up to $22k (×1.5 more)
437 | 143 | 98%
See details

Deliveroo
Campaign
Bug Bounty Program
Triaged by HackerOne, Retesting
Wildcard 12 | AndroidPlayStore 2 | IosAppStore 2 | Domain 1
Ends in 2 days
×3 more
187 | 115 | 96%
See details

Cloudflare Public Bu...
Campaign
Bug Bounty Program
Triaged by HackerOne, Retesting, Collaboration
OtherAsset 40 | Domain 8 | AiModel 1 | SourceCode 1
Gold Standard
Ends in 22 days
×2 more
307 | 124 | 95%
See details



Dashboard | Engagements | Invites | Discovery | Work | Payments | Leaderboards | CrowdStream

Bug Bounty | Joinable | Vulnerability Disclosure | Pen Tests

Search by keyword or phrase...

All filters | Rewards | Scope | Target category | Dates | Sort: Promoted

Grid | Table

Public Bug Bounty
Ibotta
Mobile app providing cash back for users through in-app purchases,...
$250 - $7,500

Public Bug Bounty
Auth0 by Okta
We provide a universal authentication & authorization...
$100 - $50,000

Public Bug Bounty
The Security Team Rocks
Electroneum is a mobile-based payments solution is powered by...
$200 - $12,000

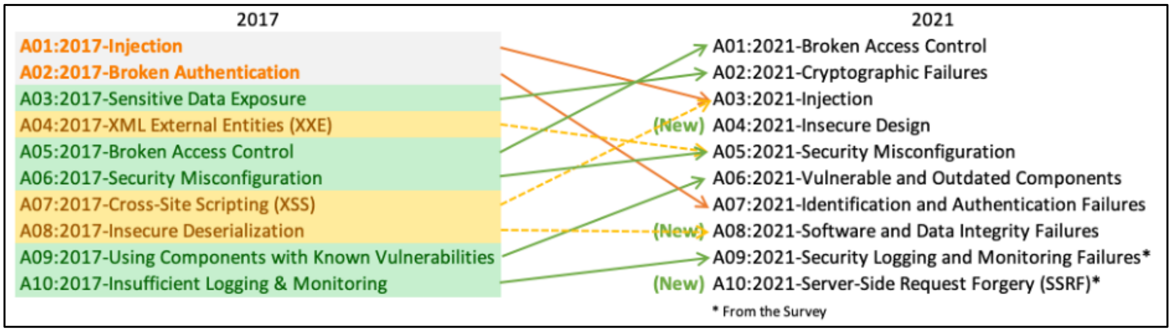
Public Bug Bounty
Electroneum
Electroneum is a mobile-based payments solution is powered by...
$200 - $12,000

Public Bug Bounty
Wise (ex-TransferWise)
Wise — the global technology company building the best way to...
$100 - $4,000
Up to $6,000

Public Bug Bounty
Credit Karma
Free Credit Scores & Credit Report Monitoring
$100 - $5,000

After the initial phase of getting know about bug bounty my next agenda was to get familiar with the bug bounty programs and their guidelines.i went through both hackerone and bugcrowd to see what are the available information about these programs.in there I found a thing called scope in each program.then I took a look at what the scope is,there are two parts.In scope and out of scope.as I found out scope basically gives us an idea about what are the assests we have to hack on In order to find bugs.bounties can only be applicable for the in scope assests.futheremore I found out there are mainly two types of bug bounty program types available.Bug bounty program (BBP) and Vulnerability Disclosure Program (VDP). As I went through the programs t instead of the scope they have listed types of vulnerabilities they want us to find,what are the assests that are available for us to hack on,Bounties we can obtailn according to each category,things we have permission to do and things we don't have permissions to do to the relevant target.With some other information.

Next I went online and searched for what OWASP Top 10 is?As I found out,
Owasp top 10 is the most critical 10 vulnerabilities that can be found in a web application.OWASP stands for Open Web Application Security Project.it is a non-profit organization focused on improving software security.



2017	2021
A01:2017-Injection	A01:2021-Broken Access Control
A02:2017-Broken Authentication	A02:2021-Cryptographic Failures
A03:2017-Sensitive Data Exposure	A03:2021-Injection
A04:2017-XML External Entities (XXE)	(New) A04:2021-Insecure Design
A05:2017-Broken Access Control	A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration	A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting (XSS)	A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	(New) A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with Known Vulnerabilities	A09:2021-Security Logging and Monitoring Failures*
A10:2017-Insufficient Logging & Monitoring	(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

As of late,owasp top 10 can be listed as follows:

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfigurations
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

These top 10 will be the main target when participating in the bug bounty programs

Chapter 2 – Starting With Bug Bounty

Day 3 and 4

Selecting 10 Domains to make the report.

As the assignment,I was asked to do bug bounty scans for 10 Domains.selecting the final 10 domains was kind of tricky process.after I went through so many domains/subdomains I had to finalize it to 10 domains.

I tested the following domains in the early stages of vulnerability scanning.

1. wise.com
2. linkedin.com
3. vendasta.com
4. soundcloud.com
5. opera.com
6. koho.ca
7. Krisha.kz
8. Floqast.com
9. grammerly.com
10. redoxengine.com
11. alshaya.com
12. picsart.com
13. rockstargames.com
14. payoneer.com
15. trello.com
16. indrive.com
17. exoscale.com
18. arkoselabs.com

After hours and hours of scans I selected the following as my final 10 domains

1. blog.vendasta.com (a subdomain of vendasta.com)
2. wise.com
3. devimages.alshaya.com (subdomain of alshaya.com)
4. opera.com
5. floqast.com
6. krisha.kz
7. soundcloud.com
8. picsart.com
9. trello.com
10. rockstargames.com

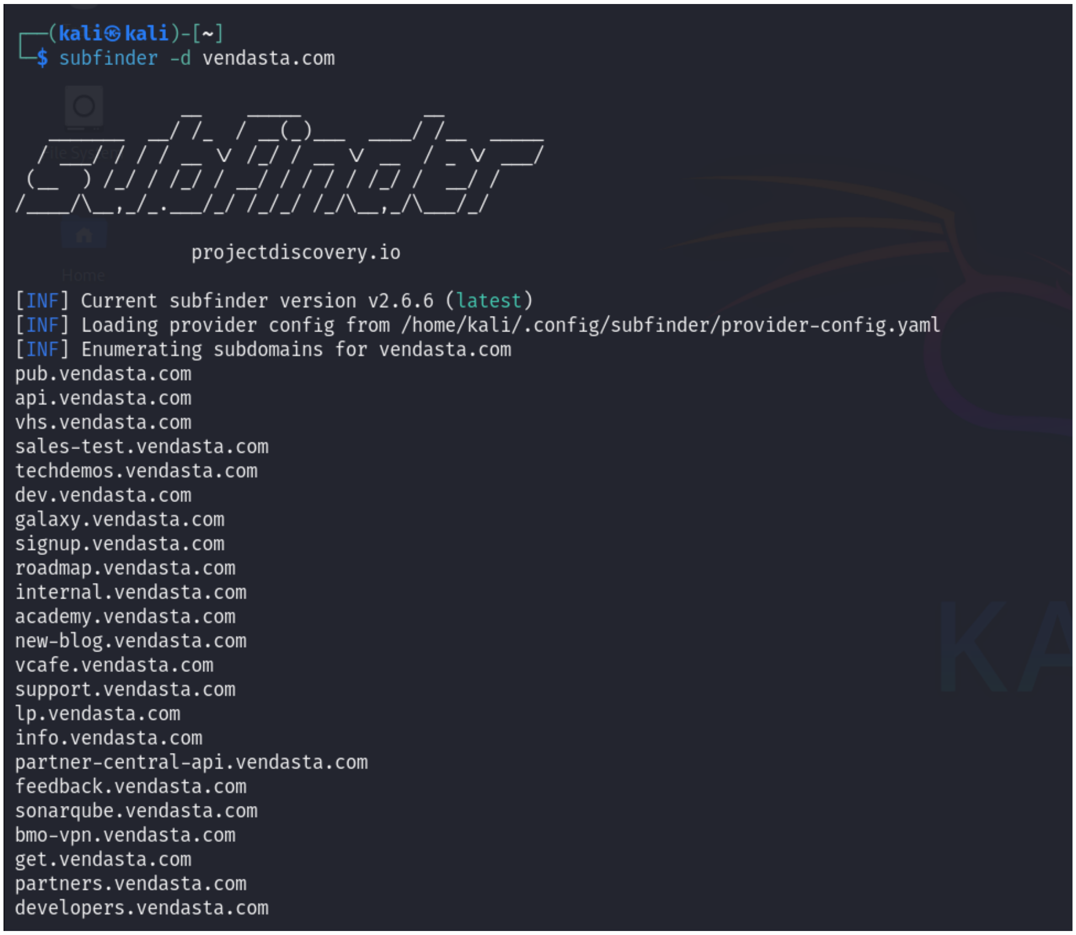
Chapter 3 - Reconnaissance

Day 5 and 6

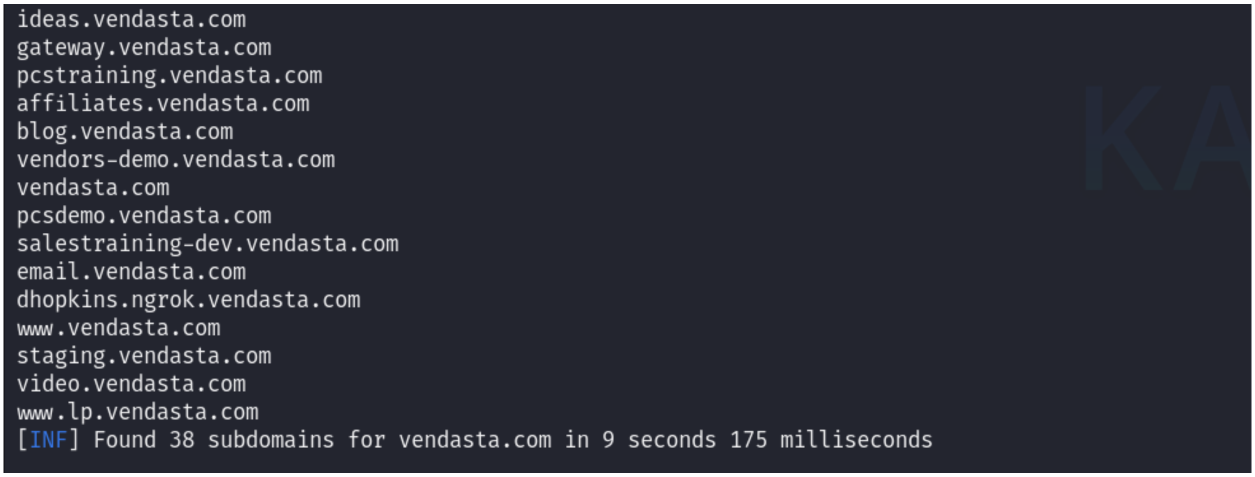
In this chapter my main focus is to give a idea about my reconnaissance journey. Reconnaissance is the initial phase of bug bounty.it can simply be described as information gathering.this phase is the foundation of a successful bug bounty.and this phase unveils some hidden details about the target and their potential vulnerabilities.

To start reconnaissance I did some sub domain enumeration with Subfinder and sublist3r.both being very popular tools among thousands of kali Linux users.subdomains could be a crutial factor when it comes to bug bounty.this can revel many hidden information in a website.

Subfinder



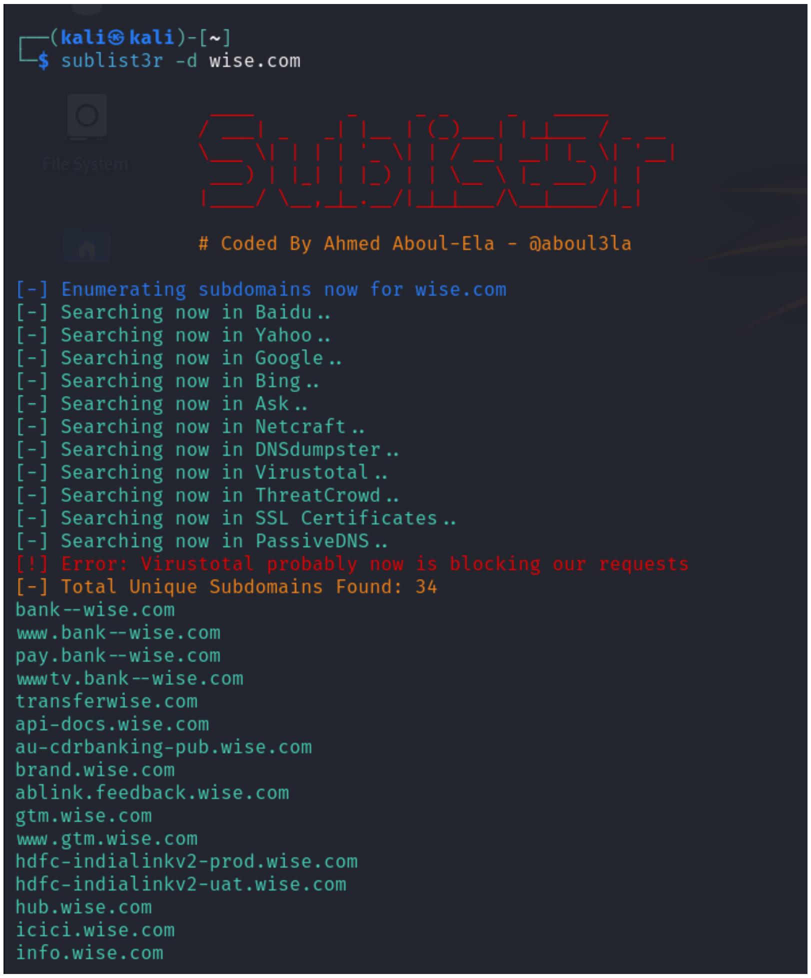
```
┌──(kali㉿kali)-[~]
└─$ subfinder -d vendasta.com

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.6 (latest)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for vendasta.com
pub.vendasta.com
api.vendasta.com
vhs.vendasta.com
sales-test.vendasta.com
techdemos.vendasta.com
dev.vendasta.com
galaxy.vendasta.com
signup.vendasta.com
roadmap.vendasta.com
internal.vendasta.com
academy.vendasta.com
new-blog.vendasta.com
vcafe.vendasta.com
support.vendasta.com
lp.vendasta.com
info.vendasta.com
partner-central-api.vendasta.com
feedback.vendasta.com
sonarqube.vendasta.com
bmo-vpn.vendasta.com
get.vendasta.com
partners.vendasta.com
developers.vendasta.com
```



```
ideas.vendasta.com
gateway.vendasta.com
pcstraining.vendasta.com
affiliates.vendasta.com
blog.vendasta.com
vendors-demo.vendasta.com
vendasta.com
pcsdemo.vendasta.com
salestraining-dev.vendasta.com
email.vendasta.com
dhopkins.ngrok.vendasta.com
www.vendasta.com
staging.vendasta.com
video.vendasta.com
www.lp.vendasta.com
[INF] Found 38 subdomains for vendasta.com in 9 seconds 175 milliseconds
```

After scanning vendasta.com with subfinder I found out 38 subdamins of vendasta.com

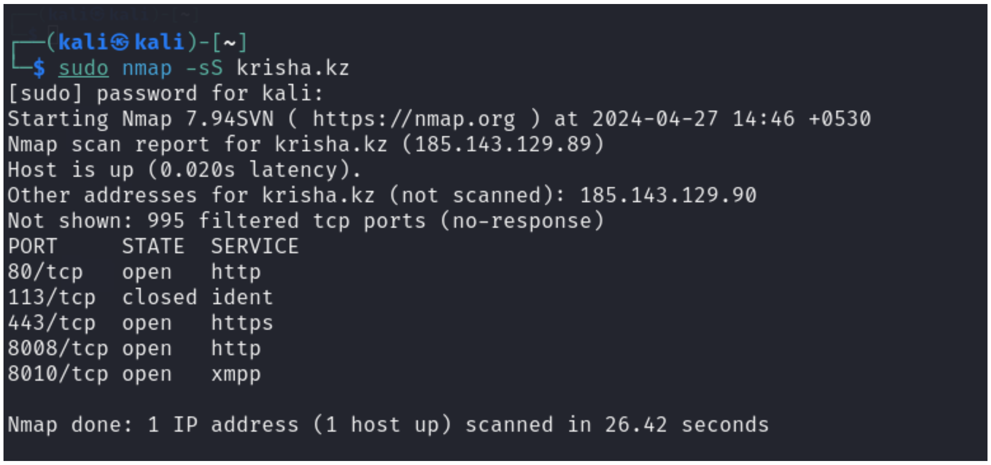
Sublist3r



```
┌──(kali㉿kali)-[~]
└─$ sublist3r -d wise.com

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for wise.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 34
bank--wise.com
www.bank--wise.com
pay.bank--wise.com
wwwtv.bank--wise.com
transferwise.com
api-docs.wise.com
au-cdrbanking-pub.wise.com
brand.wise.com
ablink.feedback.wise.com
gtm.wise.com
www.gtm.wise.com
hdfc-indialinkv2-prod.wise.com
hdfc-indialinkv2-uat.wise.com
hub.wise.com
icici.wise.com
info.wise.com
```

After scanning wise.com with sublist3r I fount there are 34 subdomains associated with the wise.com

After subdomain hunting next step was to identify open ports of a given website with Nmap.Nmap is a powerful and also a popular tool among kali linux users.



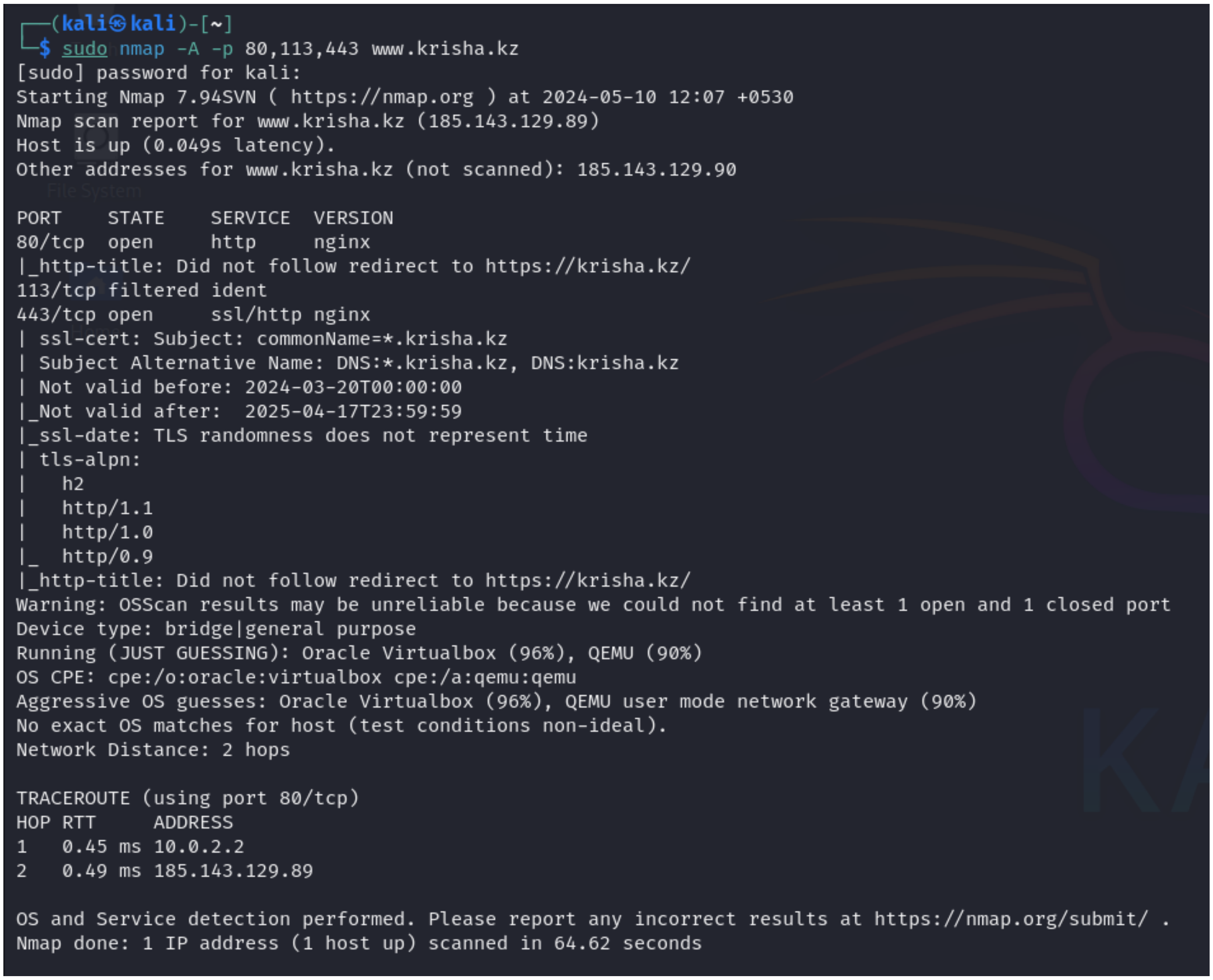
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS krisha.kz
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 14:46 +0530
Nmap scan report for krisha.kz (185.143.129.89)
Host is up (0.020s latency).
Other addresses for krisha.kz (not scanned): 185.143.129.90
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
8008/tcp open   http
8010/tcp open   xmpp

Nmap done: 1 IP address (1 host up) scanned in 26.42 seconds
```

By scanning Krisha.kz with Nmap I found out these information.

Port	State	Service
80/tcp	open	http
113/tcp	closed	ident
443/tcp	open	https
8008/tcp	open	http
8010/tcp	open	xmpp

Furthermore, I targeted the specific ports like port 80,113 and 443 and scanned with using the command

sudo nmap -A -p 80,113,443 www.krisha.kz



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -p 80,113,443 www.krisha.kz
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 12:07 +0530
Nmap scan report for www.krisha.kz (185.143.129.89)
Host is up (0.049s latency).
Other addresses for www.krisha.kz (not scanned): 185.143.129.90

PORT    STATE    SERVICE  VERSION
80/tcp  open     http     nginx
|_http-title: Did not follow redirect to https://krisha.kz/
113/tcp filtered ident
443/tcp open     ssl/http nginx
| ssl-cert: Subject: commonName=*.krisha.kz
| Subject Alternative Name: DNS:*.krisha.kz, DNS:krisha.kz
| Not valid before: 2024-03-20T00:00:00
|_Not valid after:  2025-04-17T23:59:59
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|_  http/0.9
|_http-title: Did not follow redirect to https://krisha.kz/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.45 ms 10.0.2.2
2   0.49 ms 185.143.129.89

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.62 seconds
```

With that I found out the following

1. Host Information:

   - Host: www.krisha.kz (185.143.129.89)
   - Status: Up (Latency: 0.049s)

2. Open Ports:

   - Port 80/tcp: HTTP service with Nginx (Not redirecting to HTTPS).
   - Port 443/tcp: SSL/HTTP service with Nginx (Wildcard SSL certificate for *.krisha.kz).

3. SSL Certificate Details:

   - Validity: March 20, 2024, to April 17, 2025.
   - TLS Randomness: Issue detected.

4. Device Type:

    - Bridge or general-purpose.

5. Possible Operating Systems:

    - Oracle Virtualbox (96%)
    - QEMU (90%)

6. Traceroute:

    - Network Distance: 2 hops.

7. OS and Service Detection:

    - OS Guesses: Oracle Virtualbox or QEMU.
    - Web Server: Nginx.

8. Warning:

    - OSScan results may be unreliable.

Chapter 4 – Searching for vulnerabilities.

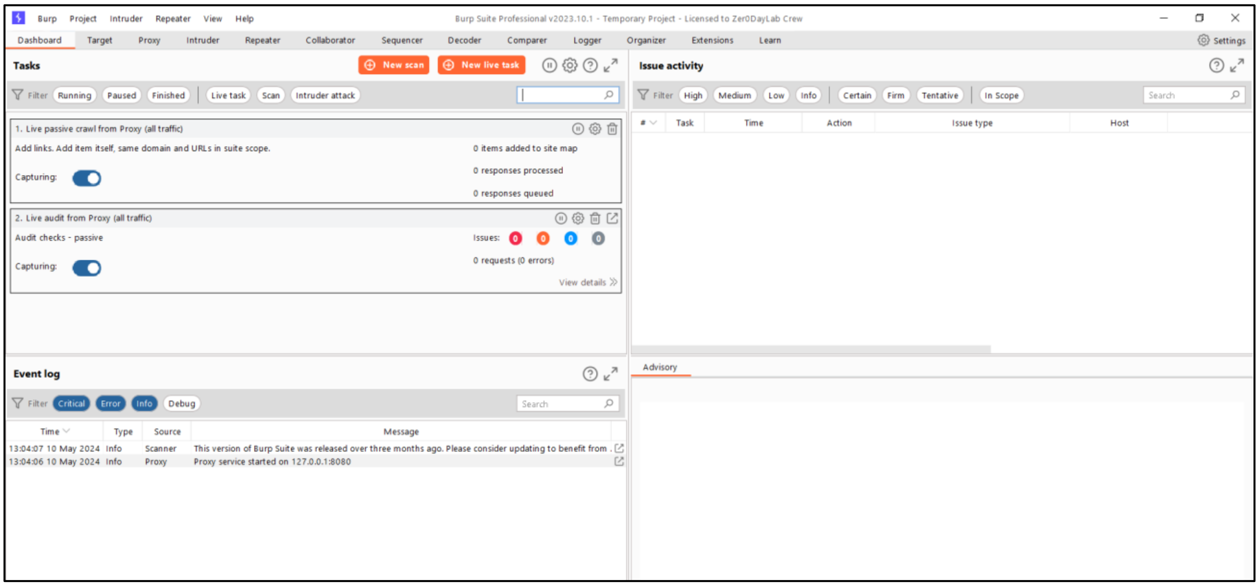
Day 7-8-9 and 10

This chapter is dedicated to vulnerability scanning phase of my bug bounty journey.for this first of all i had to decide what are the tools that I can use with this phase.as I do my research I found out there are bunch of tools available for this task.few tools caught my attention.they are

1) Burp Suite
2) Zap (previously known as OWASP Zap)
3) Nikto

Burp Suite

Burp Suite is a software that developed by the company PortSwigger.it is a security application used for penetration testing of web applications. Both a free and a paid version of the software are available. Burp Suite is a powerful tool when it comes to scanning for vulnerabilities.



1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

0 items added to site map

0 responses processed

0 responses queued

2. Live audit from Proxy (all traffic)

Audit checks - passive

Capturing:

Issues: 0 0 0 0

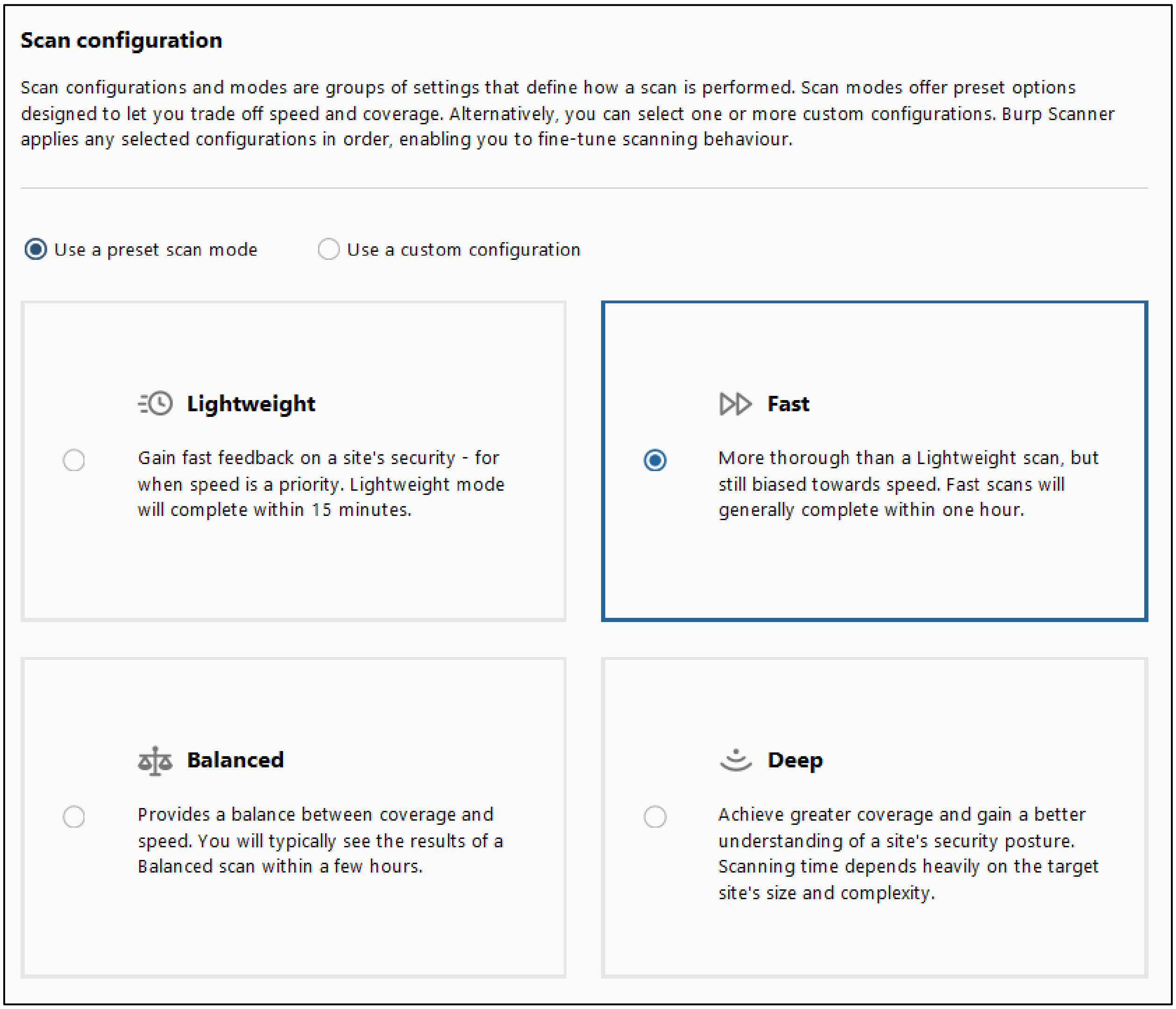
0 requests (0 errors)

View details

#	Task	Time	Action	Issue type	Host

Time	Type	Source	Message
13:04:07 10 May 2024	Info	Scanner	This version of Burp Suite was released over three months ago. Please consider updating to benefit from .
13:04:06 10 May 2024	Info	Proxy	Proxy service started on 127.0.0.1:8080

There are 4 available preset scan modes in burp suite.



Scan configuration

Scan configurations and modes are groups of settings that define how a scan is performed. Scan modes offer preset options designed to let you trade off speed and coverage. Alternatively, you can select one or more custom configurations. Burp Scanner applies any selected configurations in order, enabling you to fine-tune scanning behaviour.

● Use a preset scan mode ○ Use a custom configuration

○ **Lightweight**

Gain fast feedback on a site's security - for when speed is a priority. Lightweight mode will complete within 15 minutes.

● **Fast**

More thorough than a Lightweight scan, but still biased towards speed. Fast scans will generally complete within one hour.

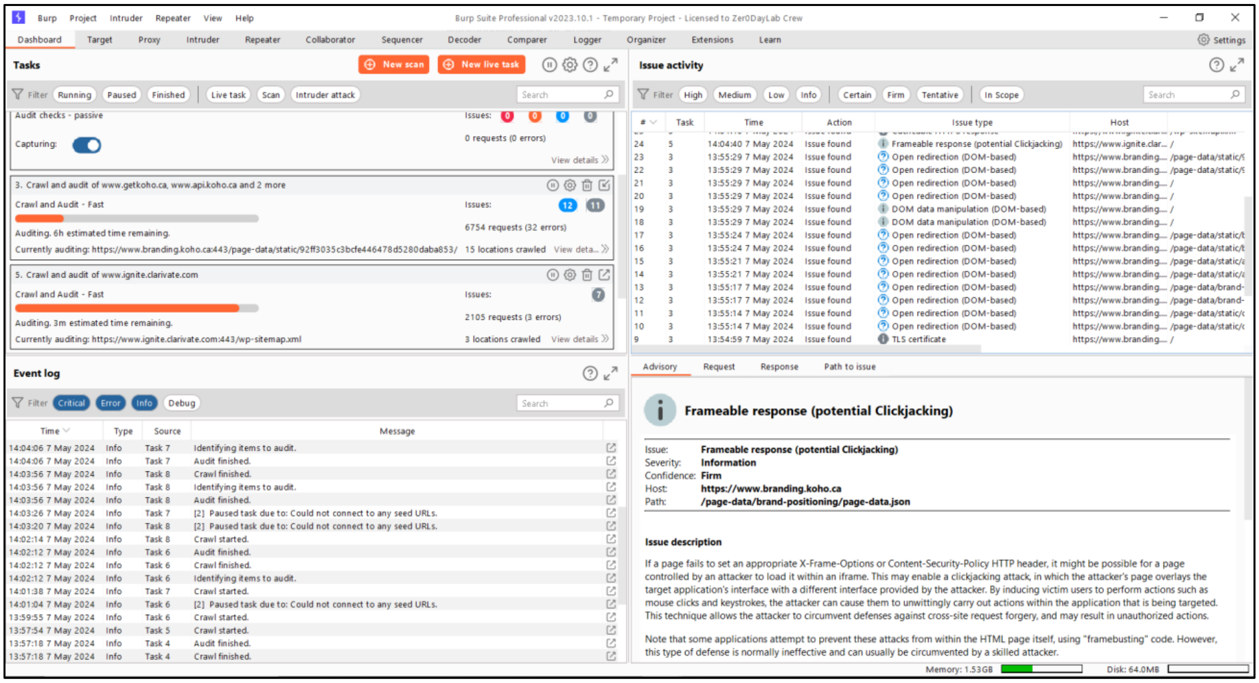
○ **Balanced**

Provides a balance between coverage and speed. You will typically see the results of a Balanced scan within a few hours.

○ **Deep**

Achieve greater coverage and gain a better understanding of a site's security posture. Scanning time depends heavily on the target site's size and complexity.

We can select one of those 4 options and just add a url and Burp will do the rest..i preferred the fast mode.



Burp Suite Professional v2023.10.1 - Temporary Project - Licensed to Zer0DayLab Crew

Tasks

Audit checks - passive
Issues: 0 0 0 0
Capturing:
0 requests (0 errors)
View details

3. Crawl and audit of www.getkoho.ca, www.api.koho.ca and 2 more
Crawl and Audit - Fast
Issues: 12 11
Auditing. 6h estimated time remaining.
6754 requests (32 errors)
Currently auditing: https://www.branding.koho.ca:443/page-data/static/92ff3035c3bcfe446478d5280daba853/
15 locations crawled
View deta...

5. Crawl and audit of www.ignite.clarivate.com
Crawl and Audit - Fast
Issues: 7
Auditing. 3m estimated time remaining.
2105 requests (3 errors)
Currently auditing: https://www.ignite.clarivate.com:443/wp-sitemap.xml
3 locations crawled
View details

Issue activity

#	Task	Time	Action	Issue type	Host	
24	5	14:04:40 7 May 2024	Issue found	Frameable response (potential Clickjacking)	https://www.ignite.clar...	/
23	3	13:55:29 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/page-data/static/9
22	3	13:55:29 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/page-data/static/9
21	3	13:55:29 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/
20	3	13:55:29 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/
19	3	13:55:29 7 May 2024	Issue found	DOM data manipulation (DOM-based)	https://www.branding....	/
18	3	13:55:29 7 May 2024	Issue found	DOM data manipulation (DOM-based)	https://www.branding....	/
17	3	13:55:24 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/page-data/static/t
16	3	13:55:24 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/page-data/static/t
15	3	13:55:21 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/page-data/static/a
14	3	13:55:21 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/page-data/static/a
13	3	13:55:17 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/page-data/brand-
12	3	13:55:17 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/page-data/brand-
11	3	13:55:14 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/page-data/static/c
10	3	13:55:14 7 May 2024	Issue found	Open redirection (DOM-based)	https://www.branding....	/page-data/static/c
9	3	13:54:59 7 May 2024	Issue found	TLS certificate	https://www.branding....	/

Event log

Time	Type	Source	Message
14:04:06 7 May 2024	Info	Task 7	Identifying items to audit.
14:04:06 7 May 2024	Info	Task 7	Audit finished.
14:03:56 7 May 2024	Info	Task 8	Crawl finished.
14:03:56 7 May 2024	Info	Task 8	Identifying items to audit.
14:03:56 7 May 2024	Info	Task 8	Audit finished.
14:03:26 7 May 2024	Info	Task 7	[2] Paused task due to: Could not connect to any seed URLs.
14:03:20 7 May 2024	Info	Task 8	[2] Paused task due to: Could not connect to any seed URLs.
14:02:14 7 May 2024	Info	Task 8	Crawl started.
14:02:12 7 May 2024	Info	Task 6	Audit finished.
14:02:12 7 May 2024	Info	Task 6	Crawl finished.
14:02:12 7 May 2024	Info	Task 6	Identifying items to audit.
14:01:38 7 May 2024	Info	Task 7	Crawl started.
14:01:04 7 May 2024	Info	Task 6	[2] Paused task due to: Could not connect to any seed URLs.
13:59:55 7 May 2024	Info	Task 6	Crawl started.
13:57:54 7 May 2024	Info	Task 5	Crawl started.
13:57:18 7 May 2024	Info	Task 4	Audit finished.
13:57:18 7 May 2024	Info	Task 4	Crawl finished.

Frameable response (potential Clickjacking)

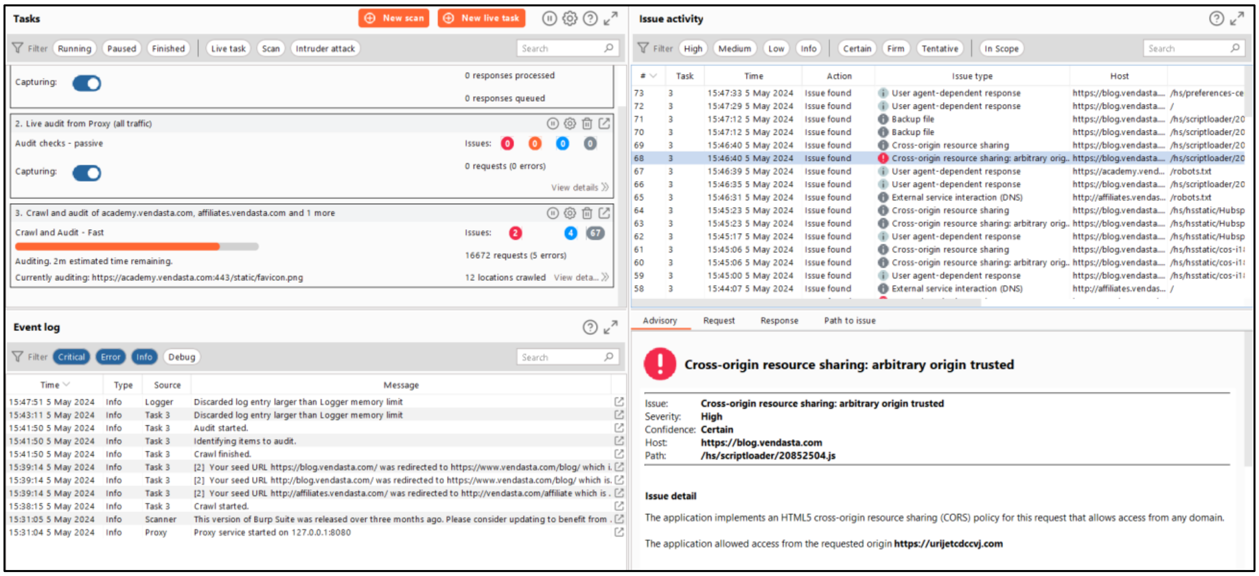
Issue: **Frameable response (potential Clickjacking)**
Severity: **Information**
Confidence: **Firm**
Host: **https://www.branding.koho.ca**
Path: **/page-data/brand-positioning/page-data.json**

Issue description

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

Memory: 1.53GB Disk: 64.0MB



Tasks

Capturing:
0 responses processed
0 responses queued

2. Live audit from Proxy (all traffic)
Audit checks - passive
Issues: 0 0 0 0
Capturing:
0 requests (0 errors)
View details

3. Crawl and audit of academy.vendasta.com, affiliates.vendasta.com and 1 more
Crawl and Audit - Fast
Issues: 2 4 67
Auditing. 2m estimated time remaining.
16672 requests (5 errors)
Currently auditing: https://academy.vendasta.com:443/static/favicon.png
12 locations crawled
View deta...

Issue activity

#	Task	Time	Action	Issue type	Host	
73	3	15:47:33 5 May 2024	Issue found	User agent-dependent response	https://blog.vendasta....	/hs/preferences-ce
72	3	15:47:29 5 May 2024	Issue found	User agent-dependent response	https://blog.vendasta....	/
71	3	15:47:12 5 May 2024	Issue found	Backup file	https://blog.vendasta....	/hs/scriptloader/20
70	3	15:47:12 5 May 2024	Issue found	Backup file	https://blog.vendasta....	/hs/scriptloader/20
69	3	15:46:40 5 May 2024	Issue found	Cross-origin resource sharing	https://blog.vendasta....	/hs/scriptloader/20
68	3	15:46:40 5 May 2024	Issue found	Cross-origin resource sharing: arbitrary orig..	https://blog.vendasta....	/hs/scriptloader/20
67	3	15:46:39 5 May 2024	Issue found	User agent-dependent response	https://academy.vend...	/robots.txt
66	3	15:46:35 5 May 2024	Issue found	User agent-dependent response	https://blog.vendasta....	/hs/scriptloader/20
65	3	15:46:31 5 May 2024	Issue found	External service interaction (DNS)	http://affiliates.vendas...	/robots.txt
64	3	15:45:23 5 May 2024	Issue found	Cross-origin resource sharing	https://blog.vendasta....	/hs/hsstatic/Hubsp
63	3	15:45:23 5 May 2024	Issue found	Cross-origin resource sharing: arbitrary orig..	https://blog.vendasta....	/hs/hsstatic/Hubsp
62	3	15:45:17 5 May 2024	Issue found	User agent-dependent response	https://blog.vendasta....	/hs/hsstatic/Hubsp
61	3	15:45:06 5 May 2024	Issue found	Cross-origin resource sharing	https://blog.vendasta....	/hs/hsstatic/cos-i1
60	3	15:45:06 5 May 2024	Issue found	Cross-origin resource sharing: arbitrary orig..	https://blog.vendasta....	/hs/hsstatic/cos-i1
59	3	15:45:00 5 May 2024	Issue found	User agent-dependent response	https://blog.vendasta....	/hs/hsstatic/cos-i1
58	3	15:44:07 5 May 2024	Issue found	External service interaction (DNS)	http://affiliates.vendas...	/

Event log

Time	Type	Source	Message
15:47:51 5 May 2024	Info	Logger	Discarded log entry larger than Logger memory limit
15:43:11 5 May 2024	Info	Task 3	Discarded log entry larger than Logger memory limit
15:41:50 5 May 2024	Info	Task 3	Audit started.
15:41:50 5 May 2024	Info	Task 3	Identifying items to audit.
15:41:50 5 May 2024	Info	Task 3	Crawl finished.
15:39:14 5 May 2024	Info	Task 3	[2] Your seed URL https://blog.vendasta.com/ was redirected to https://www.vendasta.com/blog/ which i.
15:39:14 5 May 2024	Info	Task 3	[2] Your seed URL http://blog.vendasta.com/ was redirected to https://www.vendasta.com/blog/ which is.
15:39:14 5 May 2024	Info	Task 3	[2] Your seed URL http://affiliates.vendasta.com/ was redirected to http://vendasta.com/affiliate which is .
15:38:15 5 May 2024	Info	Task 3	Crawl started.
15:31:05 5 May 2024	Info	Scanner	This version of Burp Suite was released over three months ago. Please consider updating to benefit from .
15:31:04 5 May 2024	Info	Proxy	Proxy service started on 127.0.0.1:8080

Cross-origin resource sharing: arbitrary origin trusted

Issue: **Cross-origin resource sharing: arbitrary origin trusted**
Severity: **High**
Confidence: **Certain**
Host: **https://blog.vendasta.com**
Path: **/hs/scriptloader/20852504.js**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://urijetcdccvj.com**

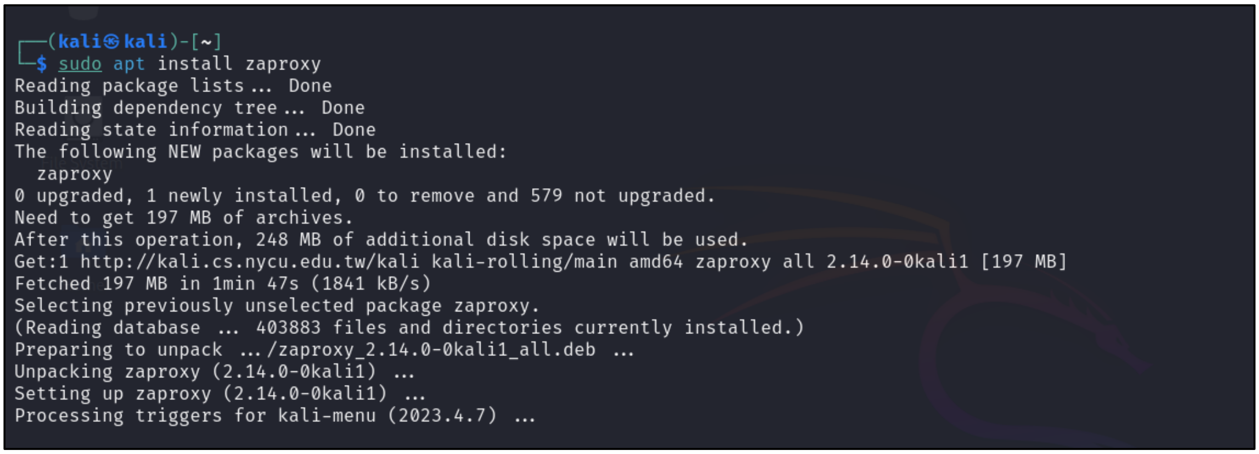
With the help of burp suite I could find some of the critical vulnerabilities like

- Cross-origin resource sharing (CORS)
- Cross site request forgery (CSRF)
- Ajax request header manipulation   etc.

Zap

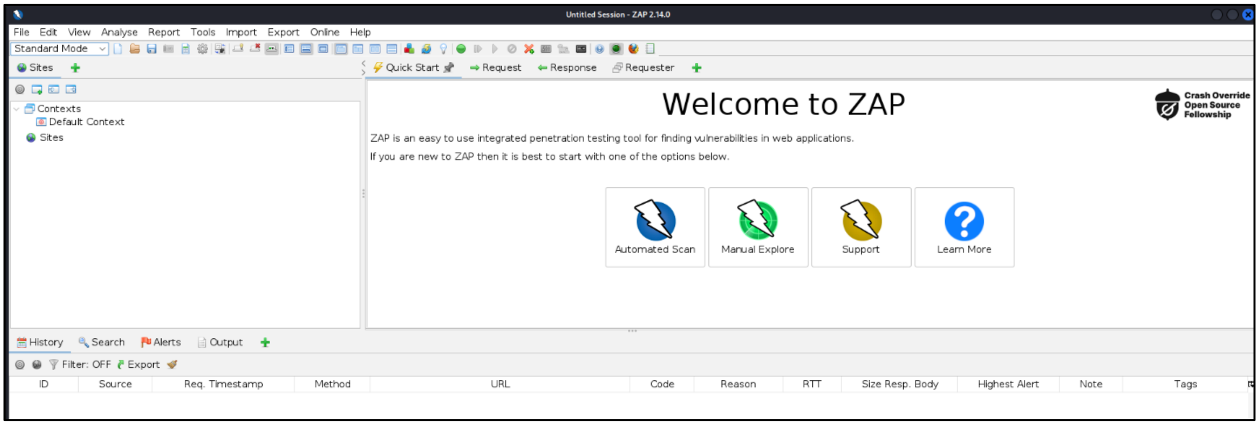
Zap(Zed Attack Proxy), previously known as OWASP Zap is a widely used free and open source powerful automated tool for vulnerability scanning

Since zap was not available in my kali Linux environment, I had to install it first.



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install zaproxy
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  zaproxy
0 upgraded, 1 newly installed, 0 to remove and 579 not upgraded.
Need to get 197 MB of archives.
After this operation, 248 MB of additional disk space will be used.
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 zaproxy all 2.14.0-0kali1 [197 MB]
Fetched 197 MB in 1min 47s (1841 kB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 403883 files and directories currently installed.)
Preparing to unpack .../zaproxy_2.14.0-0kali1_all.deb ...
Unpacking zaproxy (2.14.0-0kali1) ...
Setting up zaproxy (2.14.0-0kali1) ...
Processing triggers for kali-menu (2023.4.7) ...
```

This is how zap looks like

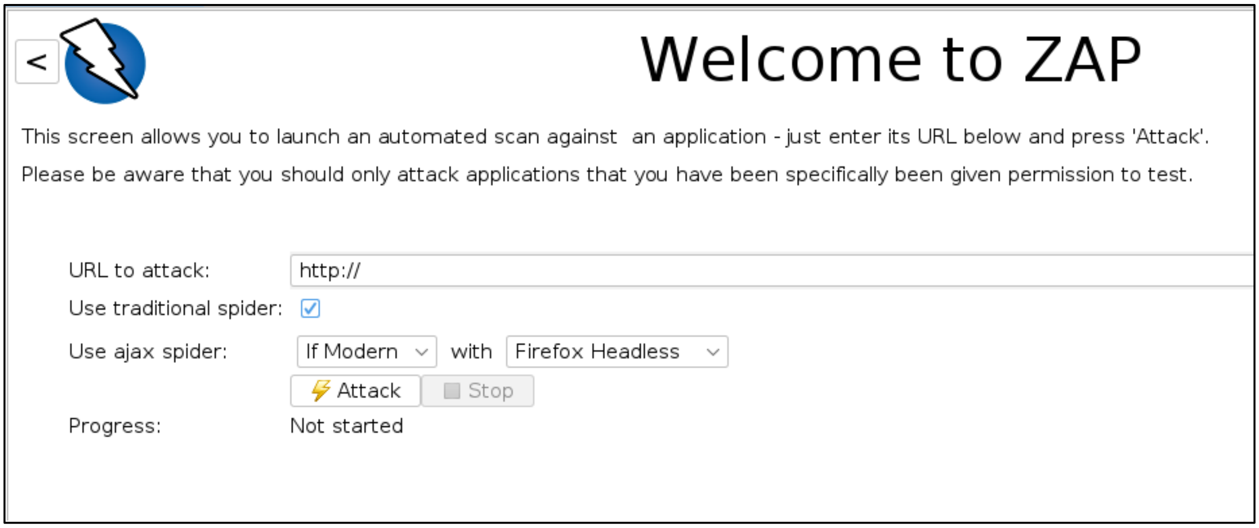


Welcome to ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

For me the preferred scan mode is Automated scan.there we have to just enter a url and scan for it.



Welcome to ZAP

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.

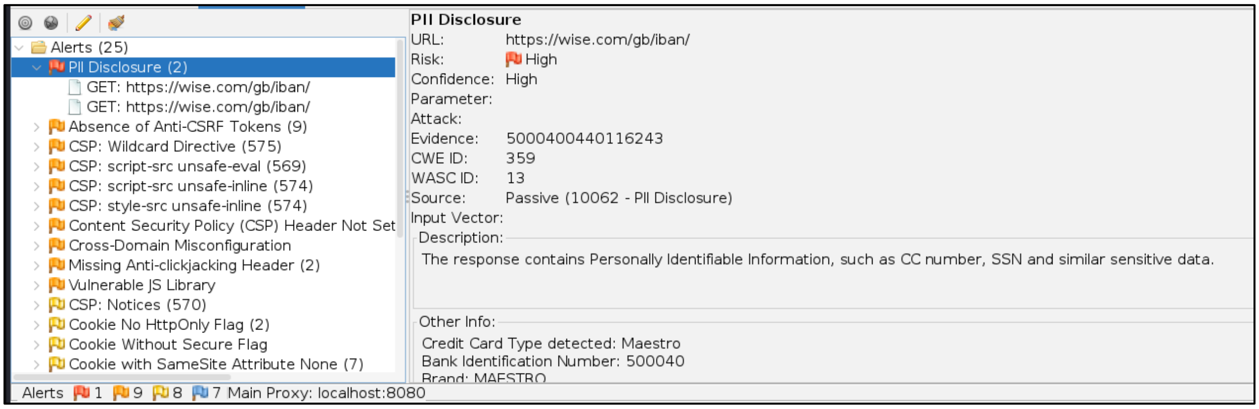
URL to attack: http://

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox Headless

Progress: Not started

Throughout my scanning with zap I discovered many vulnerabilities.



- Alerts (25)
  - PII Disclosure (2)
    - GET: https://wise.com/gb/iban/
    - GET: https://wise.com/gb/iban/
  - Absence of Anti-CSRF Tokens (9)
  - CSP: Wildcard Directive (575)
  - CSP: script-src unsafe-eval (569)
  - CSP: script-src unsafe-inline (574)
  - CSP: style-src unsafe-inline (574)
  - Content Security Policy (CSP) Header Not Set
  - Cross-Domain Misconfiguration
  - Missing Anti-clickjacking Header (2)
  - Vulnerable JS Library
  - CSP: Notices (570)
  - Cookie No HttpOnly Flag (2)
  - Cookie Without Secure Flag
  - Cookie with SameSite Attribute None (7)

PII Disclosure

URL: https://wise.com/gb/iban/
Risk: High
Confidence: High
Parameter:
Attack:
Evidence: 5000400440116243
CWE ID: 359
WASC ID: 13
Source: Passive (10062 - PII Disclosure)
Input Vector:

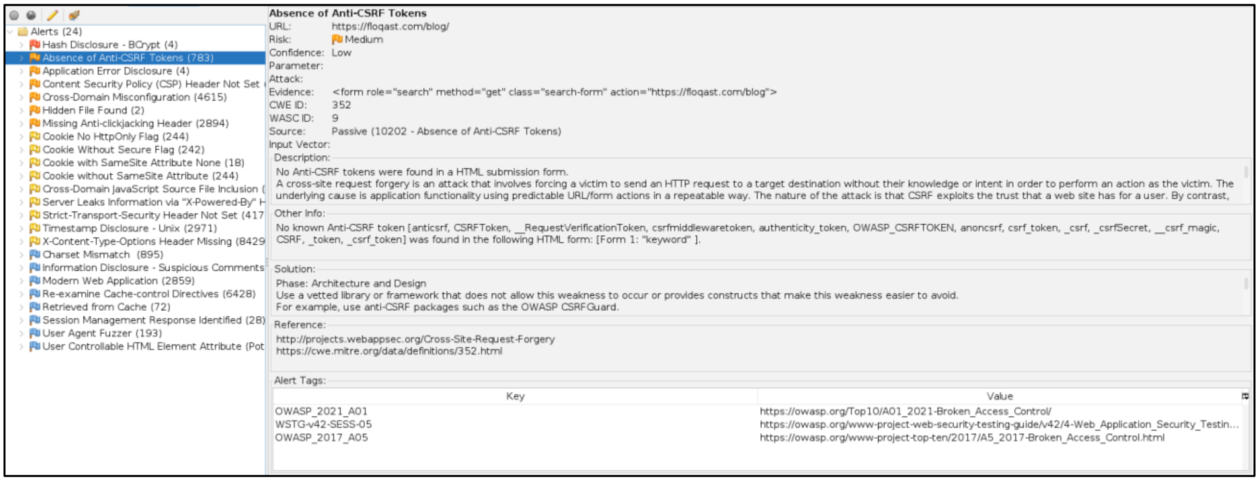
Description:

The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

Other Info:

Credit Card Type detected: Maestro
Bank Identification Number: 500040
Brand: MAESTRO

Alerts 🟥 1 🟧 9 🟨 8 🟦 7 Main Proxy: localhost:8080



- Alerts (24)
  - Hash Disclosure - BCrypt (4)
  - Absence of Anti-CSRF Tokens (783)
  - Application Error Disclosure (4)
  - Content Security Policy (CSP) Header Not Set (
  - Cross-Domain Misconfiguration (4615)
  - Hidden File Found (2)
  - Missing Anti-clickjacking Header (2894)
  - Cookie No HttpOnly Flag (244)
  - Cookie Without Secure Flag (242)
  - Cookie with SameSite Attribute None (18)
  - Cookie without SameSite Attribute (244)
  - Cross-Domain JavaScript Source File Inclusion (
  - Server Leaks Information via "X-Powered-By" H
  - Strict-Transport-Security Header Not Set (417
  - Timestamp Disclosure - Unix (2971)
  - X-Content-Type-Options Header Missing (8429
  - Charset Mismatch (895)
  - Information Disclosure - Suspicious Comments
  - Modern Web Application (2859)
  - Re-examine Cache-control Directives (6428)
  - Retrieved from Cache (72)
  - Session Management Response Identified (28)
  - User Agent Fuzzer (193)
  - User Controllable HTML Element Attribute (Pot

Absence of Anti-CSRF Tokens

URL: https://floqast.com/blog/
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form role="search" method="get" class="search-form" action="https://floqast.com/blog">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:

Description:

No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,

Other Info:

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "keyword"].

Solution:

Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Reference:

http://projects.webappsec.org/Cross-Site-Request-Forgery
https://cwe.mitre.org/data/definitions/352.html

Alert Tags:

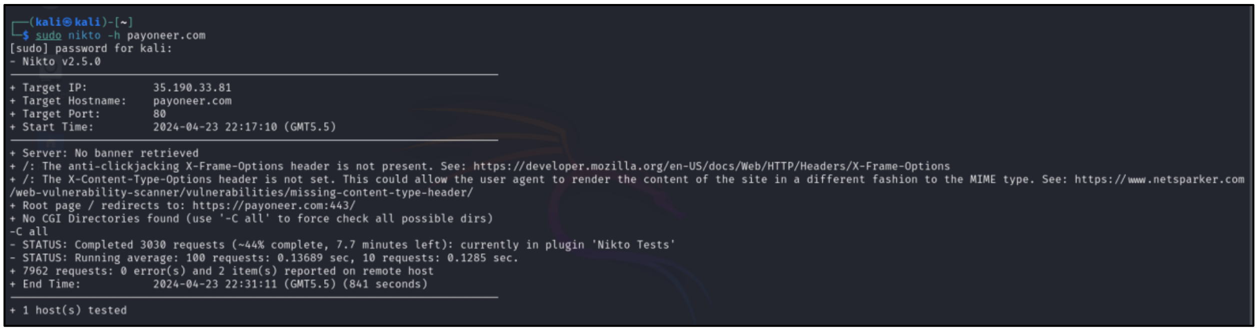
Key	Value
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/
WSTG-v42-SESS-05	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testin...
OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html

I was able to find the following vulnerabilities with Zap

- PII Disclosure
- Hash Disclosure
- Cloud Metadata potentially exposed
- Absence of Anti CSRF tokens
- Content Security Policy (CSP) Header not set
- CSP : wildcard directive
- CSP : script-src unsafe-eval
- CSP : style-src unsafe-eval
- Cross- Domain Misconfiguration
- Missing anti Clickjacking Header
- Vulnerable JS library
- HTTP to HTTPS insecure Transition in the for post Etc.

Nikto

Nikto is a free web server scanner used for detecting vulnerabilities in web servers and applications.Nikto checks for potentially dangerous files, outdated server versions, and configuration issues.As of my understanding nikto is not as powerful as both Burp Suite and Zap.but it is a comprehensive tool when it comes to vulnerability scanning.



```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h payoneer.com
[sudo] password for kali:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          35.190.33.81
+ Target Hostname:    payoneer.com
+ Target Port:        80
+ Start Time:         2024-04-23 22:17:10 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: 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 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/
+ Root page / redirects to: https://payoneer.com:443/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
-C all
- STATUS: Completed 3030 requests (~44% complete, 7.7 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.13689 sec, 10 requests: 0.1285 sec.
+ 7962 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2024-04-23 22:31:11 (GMT5.5) (841 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

With Nikto scans I was able to identify some of the vulnerabilities as following.

- The anti-clickjacking X-Frame-Options header is not present
- The X-Content-Type-Options header is not set
- Uncommon header 'accept-ch' found
- Uncommon header 'akamai-grn' found

Throughout this phase I referred so many resources like Blogs,Youtube videos etc and this was the most time consuming stage of this assignment.

Chapter 5 – Documenting

Day 11-12-13 and 14

Documenting

After days and days of searching for vulnerabilities, next step of this bug bounty journey is to Start documenting the whole report.before that I planned the way I wanted to make my report. for that I made a sketch.as of the sketch I started to make the report.first part of the report was dedicated to what bug bounty is,what are the tools I used, and the reconnaissance phase.then the vulnerability hunting phase.there in each domain I attached screenshots of the scans I did,scope of the target and the vulnerabilities I found.in the report I only included about 2 (3 max) descriptions about the vulnerabilities because I found some of them in many domains.i did that to keep the report simple and clean.but each vulnerability is described at least one time.ie the vulnerability “Absence of Anti CSRF Tokens” was present in many domains.but I didn’t describe it everywhere.but I mentioned that I found it. Documentation process took me 3-4 days to get completed.

Chapter 6 : Challenges

My bug bounty journey was full of challenges and obstacles.

In the first few days I had to overcome things like how to select the tools I want to use, what are the domains I can check for vulnerabilities.as I doing some search online it was clear to me what tools I could use to do the process.and with some more search I was able to identify the 10 domains I wanted to test for my bug bounty assignment.

Furthermore, I had to face to a problem where the targets have limited scope in the eligible criteria. With the limited scope there was not much to test on some websites.in addition of that some of the findings was a bit unclear to me at first. I had to do some research to find out what some things were.

Regarding Burp Suite, Burp has two edition.Free and Professional.we can not do vulnerability scans with the Free version.So I had to find a cracked version of the Burp Suite Professional and install it in my pc.Since a one copy of Burp suite professional version costs $449 per year.And another problem I had to face was some of the tools I used didn't work properly sometimes.once when in a middle of a scan Zap just frozed.sometimes subfinder didn't work properly.and also nikto had some issues.to resolve these issues I had to do things like restarts,reinstall the tools and update them.

Another challenge I had to overcome was the limited time frame. Especially when searching for the targets, I had to do find subdomains of each site. And I had to go through those one by one carefully.That was time consuming.and also I had to manage time between this assignment and other academic work which was kind of a challenge in some situations.

Chapter 7 : Conclusion

In a span of two weeks,I gain so much knowledge about the realm of bug bounty and ran into many obstacles in the process.starting with a little knowledge I am certain that I got a considerable amount of knowledge with this assignment.

In the beginning I started with searching for what OWASP Top 10 is.step by step the process evolved.with the tools like subfinder,sublist3r I was able to gain some crucial information about the targets.and with Nmap scans I was able to gain much more info.

Then from the automated tools like Burp Suite,Zap I was able to find some crucial vulnerabilities such as CSRF,CORS,PII DIsclorsure,Cloud Metadata potentially exposed,Absence of Anti-CSRF tokens,CSP Header not set and much more.

Documentation process came next.i had to go through so many different resources and make sure to include most relevant things including what are those vulnerabilities,how impactful they can be,and how to prevent them from harming the organizations.

To conclude this I should mention that this journey was not a easy one.but I gain so much knowledge with this.it was full of discovering new things.and learning many new things.for all of those I am very grateful.

As this journey comes to a end I am certain that the knowledge I got for this will affect my future in cyber security in a very healthy manner.

End.