Sri Lanka Institute of Information Technology

Specialized in Cyber Security

Year 2, Semester 2

IE2062 – Web Security

Bug Bounty – Report 07

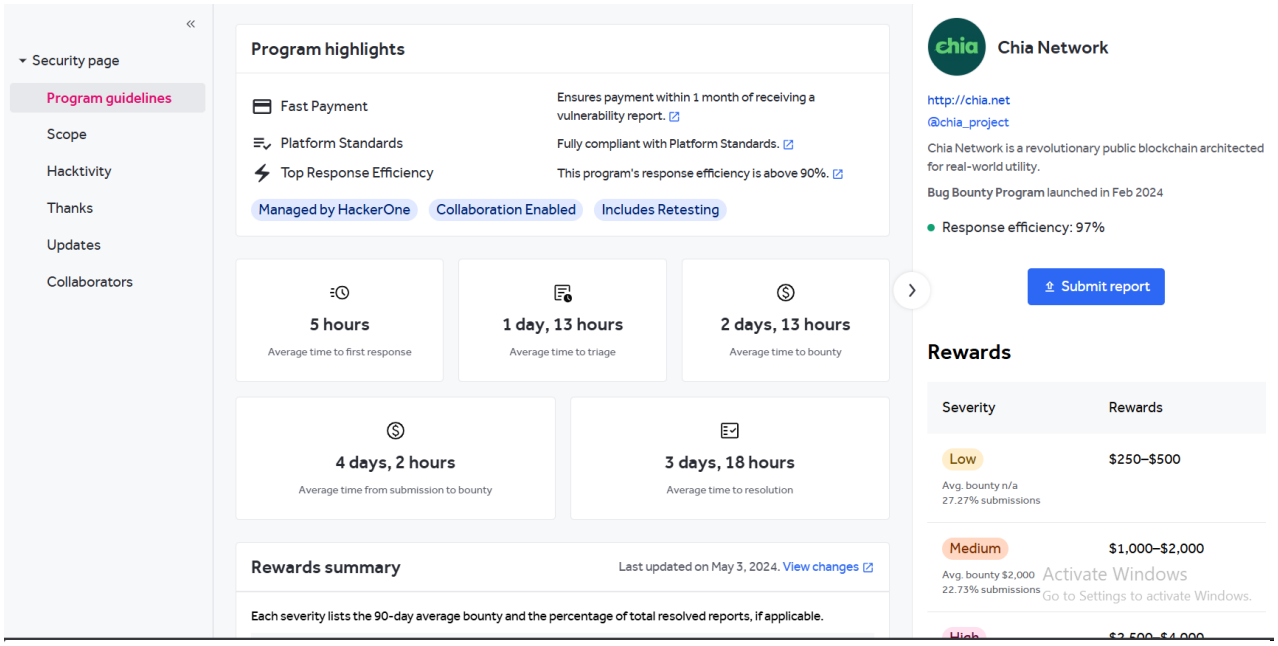
Student ID No.	Name
IT23136106	D.M.M. Pasindu Supushmika

Table of Contents

1. Website Overview

[Chia Network – Tokenize any asset]

HackerOne Link: [Chia Network | Bug Bounty Program Policy | HackerOne]

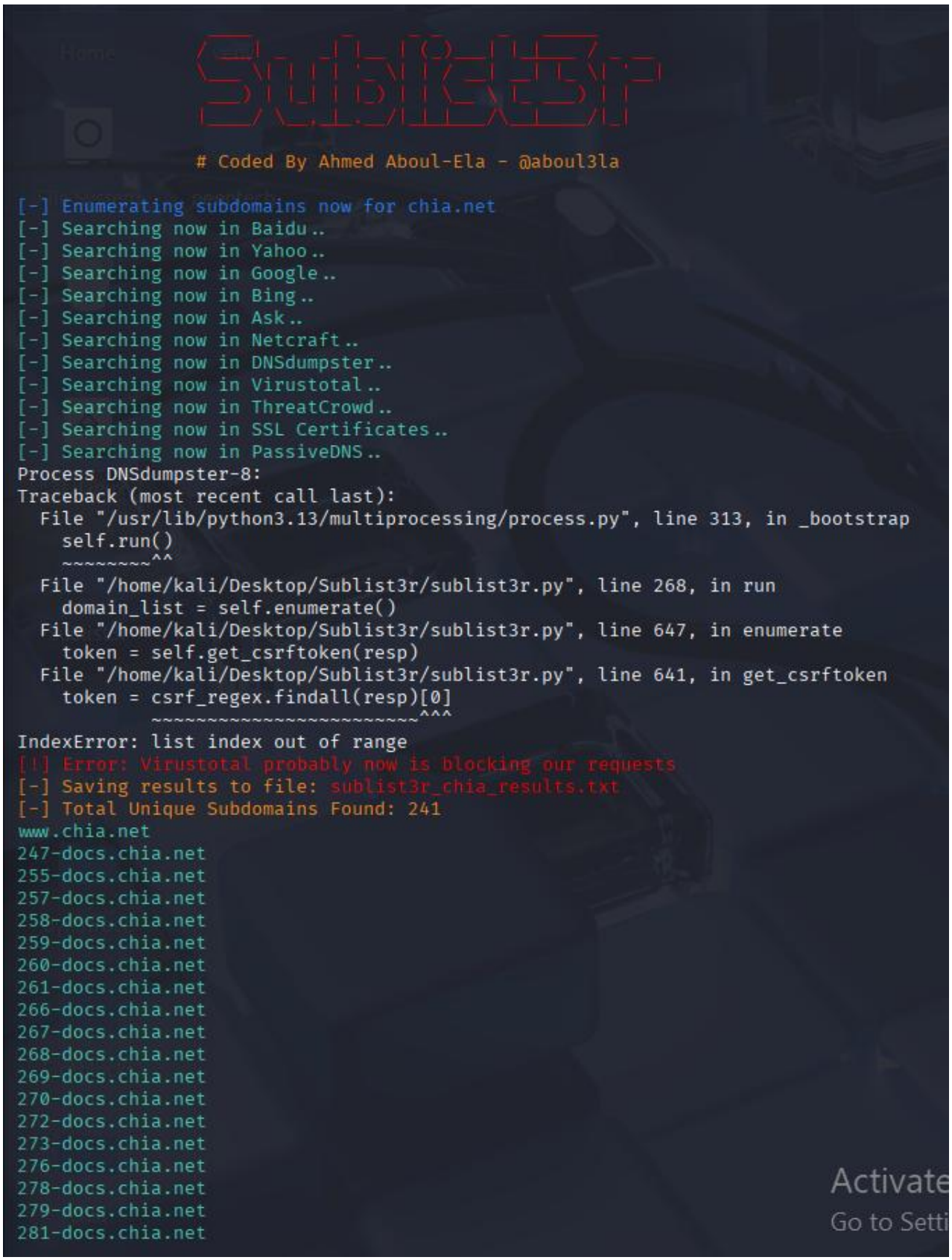


Step 01: Gather Information.

a. Sub-domain Discovery

i. Sublist3r: sublist3r_chia_results.txt

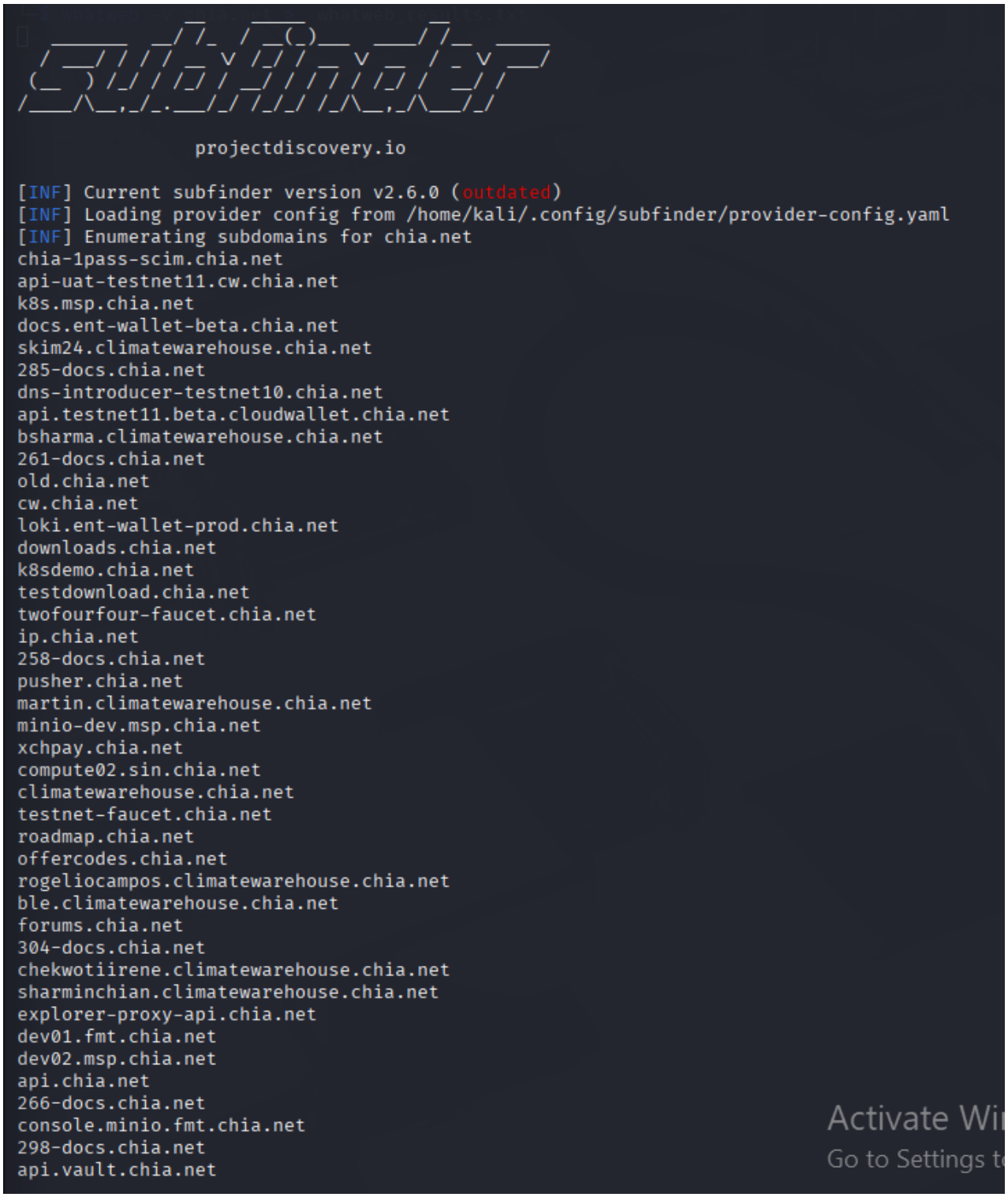
Tool **:** Sublist3r
Code **:** python3 sublist3r.py -d chia.net -o sublist3r_chai_results.txt
Explanation:
python3 sublist3r.py - Run the script using python
-d chia.net - Target domain
-o sublist3r_chai_results.txt – Output file where the result is saved



www.chia.net
247-docs.chia.net
255-docs.chia.net
257-docs.chia.net
258-docs.chia.net
259-docs.chia.net
260-docs.chia.net
261-docs.chia.net
266-docs.chia.net
267-docs.chia.net
268-docs.chia.net
269-docs.chia.net
270-docs.chia.net
272-docs.chia.net
273-docs.chia.net
276-docs.chia.net
278-docs.chia.net
279-docs.chia.net
281-docs.chia.net
283-docs.chia.net
285-docs.chia.net
288-docs.chia.net
289-docs.chia.net
292-docs.chia.net
293-docs.chia.net
295-docs.chia.net
296-docs.chia.net
297-docs.chia.net
298-docs.chia.net
300-docs.chia.net
301-docs.chia.net
302-docs.chia.net
304-docs.chia.net
305-docs.chia.net
308-docs.chia.net
310-docs.chia.net
312-docs.chia.net
router1.44monty.chia.net
api.chia.net
backup.chia.net
cat1.chia.net
cat1-stage.chia.net
ch21.chia.net
chat.chia.net
chia-1pass-scim.chia.net
chiamainnet2023.chia.net
abrahambartolome.climatewarehouse.chia.net
aferrantorres.climatewarehouse.chia.net
alexandrasoezer.climatewarehouse.chia.net
amitthusu.climatewarehouse.chia.net
angry-rooster.climatewarehouse.chia.net
api.climatewarehouse.chia.net
api-green.climatewarehouse.chia.net
api2.climatewarehouse.chia.net
app.climatewarehouse.chia.net
app2.climatewarehouse.chia.net
aureliacasarrubias.climatewarehouse.chia.net
blabber-duck.climatewarehouse.chia.net

ii. Subfindre: subfinder_result_chia.txt

Tool : Subfinder
Code : subfinder -d chia.net -o subfinder_result.txt
Explanation:
bfinder - run subfinder too
l -d chia.net - Mention the target website
-o subfinder_result.txt – Mention the output file



chia-1pass-scim.chia.net
api-uat-testnet11.cw.chia.net
k8s.msp.chia.net
docs.ent-wallet-beta.chia.net
skim24.climatewarehouse.chia.net

285-docs.chia.net
dns-introducer-testnet10.chia.net
api.testnet11.beta.cloudwallet.chia.net
bsharma.climatewarehouse.chia.net
261-docs.chia.net
old.chia.net
cw.chia.net
loki.ent-wallet-prod.chia.net
downloads.chia.net
k8sdemo.chia.net
testdownload.chia.net
twofourfour-faucet.chia.net
ip.chia.net
258-docs.chia.net
pusher.chia.net
martin.climatewarehouse.chia.net
minio-dev.msp.chia.net
xchpay.chia.net
compute02.sin.chia.net
climatewarehouse.chia.net
testnet-faucet.chia.net
roadmap.chia.net
offercodes.chia.net
rogeliocampos.climatewarehouse.chia.net
ble.climatewarehouse.chia.net
forums.chia.net
304-docs.chia.net
chekwotiirene.climatewarehouse.chia.net
sharminchian.climatewarehouse.chia.net
explorer-proxy-api.chia.net
dev01.fmt.chia.net
dev02.msp.chia.net
api.chia.net
266-docs.chia.net
console.minio.fmt.chia.net
298-docs.chia.net
api.vault.chia.net
ent-wallet-dev-testnet11.chia.net
twofivezerorc1-faucet.chia.net
stefanmeier.climatewarehouse.chia.net
uat-testnet11.cw.chia.net
compute03.msp.chia.net
276-docs.chia.net
k8s-public.fmt.chia.net
test-cadt-chia.climatewarehouse.chia.net
devs.chia.net
289-docs.chia.net
manuelgarciarossel.climatewarehouse.chia.net
ssrinivasan8.climatewarehouse.chia.net
content-rhino.climatewarehouse.chia.net
router1.44monty.chia.net
cat3compute03.ldn.chia.net

b. Live Subdomain Discovery

Tool : httpx:livesub_results.txt
Code : httpx-toolkit -l subfinder_result_chia.txt -o livesub_results.txt
Explanation:
httpx-toolkit - run the httpx tool
-l subfinder_result_chia.txt – mention the file containing input
-o livesub_results.txt – mention the file which should write the output

https://app.climatewarehouse.chia.net
https://api-dev-testnet11.cw.chia.net
https://chia.net
https://dev.chia.net
https://developers.chia.net
https://dashboard.chia.net
https://devs.chia.net

https://download.chia.net
https://chia-1pass-scim.chia.net
https://ch21.chia.net
https://console.minio.ldn.chia.net
https://console.minio.msp.chia.net
https://console.minio.fmt.chia.net
https://help.chia.net
https://api-uat-testnet11.cw.chia.net
https://console.minio.sin.chia.net
https://api.vault.chia.net
https://ip.chia.net
https://docs.chia.net
https://discord-bot.chia.net
https://docs.ent-wallet-dev.chia.net
https://explorer-proxy-api.chia.net
https://docs.ent-wallet-prod.chia.net
https://dev-testnet11.cw.chia.net
https://faucet.chia.net
https://github-webhooks.chia.net
https://github-glue.chia.net
https://k8s.ldn.chia.net
https://portal.chia.net
https://hosted.chia.net
https://k8s.fmt.chia.net
https://pypi.chia.net
https://k8s.msp.chia.net
https://roadmap.chia.net
https://minio.ldn.chia.net
https://loadtest.ent-wallet-prod.chia.net
https://minio.fmt.chia.net
https://loadtest.ent-wallet-dev.chia.net
https://minio.sin.chia.net
https://minio.msp.chia.net
https://matomo.chia.net
https://offercodes.chia.net
https://offers-api-sim.chia.net
https://downloads.chia.net
https://staging.docs.chia.net
https://warrantcanary.chia.net
https://torrents.chia.net
https://testnet11-faucet.chia.net
https://shop.chia.net
https://status.chia.net
https://xchpay.chia.net
https://vault.chia.net
https://uat-testnet11.cw.chia.net
https://www.chia.net

c. IP Discovery

Tool: nslookup: nslookup_result.txt

Code: since we whole file with subdomains, to find IP addresses using "nslookup" we need to make a loop until all the Ips of all the subdomains are found.

```
while read sub; do
 echo "Looking up: $sub" >> nslookup_result.txt
  nslookup "$sub" | awk '/^Name:|^Address:/' >> nslookup_result.txt
  echo "------------------------" >> nslookup_result.txt
done < livesub_results.txt
```

Explanation:

While read sub; do - start of the loop

Echo "Looking up: $sub">>nslookup_result.txt - print message "Looking up: subdomain" into the file "*nslookup_result*.txt"

nslookup "$sub" | awk '/^Name:|^Address:/' >> nslookup_result.txt - run the nslookup command

echo "_____" >> nslookup_result.txt - separate one subdomain details from another

done < livesub_results.txt - End the loop and continue until the lines in the livesub_results.txt

```
┌──(kali㉿kali)-[~/Desktop/chia]
└─$ ./nslookup_script.sh

┌──(kali㉿kali)-[~/Desktop/chia]
└─$ cat nslookup_result.txt
Looking up: https://app.climatewarehouse.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://api-dev-testnet11.cw.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://dev.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://developers.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://dashboard.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://devs.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://download.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://chia-1pass-scim.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://ch21.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://console.minio.ldn.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://console.minio.msp.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://console.minio.fmt.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://help.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://api-uat-testnet11.cw.chia.net
Address:        192.168.0.1#53
------------------------
Looking up: https://console.minio.sin.chia.net
Address:        192.168.0.1#53
------------------------
```

IP list:

Looking up: https://app.climatewarehouse.chia.net
Address: 192.168.0.1#53

Looking up: https://api-dev-testnet11.cw.chia.net
Address: 192.168.0.1#53

Looking up: https://chia.net
Address: 192.168.0.1#53

Looking up: https://dev.chia.net
Address: 192.168.0.1#53

Looking up: https://developers.chia.net
Address: 192.168.0.1#53

Looking up: https://dashboard.chia.net
Address: 192.168.0.1#53

Looking up: https://devs.chia.net
Address: 192.168.0.1#53

Looking up: https://download.chia.net
Address: 192.168.0.1#53

Looking up: https://chia-1pass-scim.chia.net
Address: 192.168.0.1#53

Looking up: https://ch21.chia.net
Address: 192.168.0.1#53

Looking up: https://console.minio.ldn.chia.net
Address: 192.168.0.1#53

Looking up: https://console.minio.msp.chia.net
Address: 192.168.0.1#53

Looking up: https://console.minio.fmt.chia.net
Address: 192.168.0.1#53

Looking up: https://help.chia.net
Address: 192.168.0.1#53

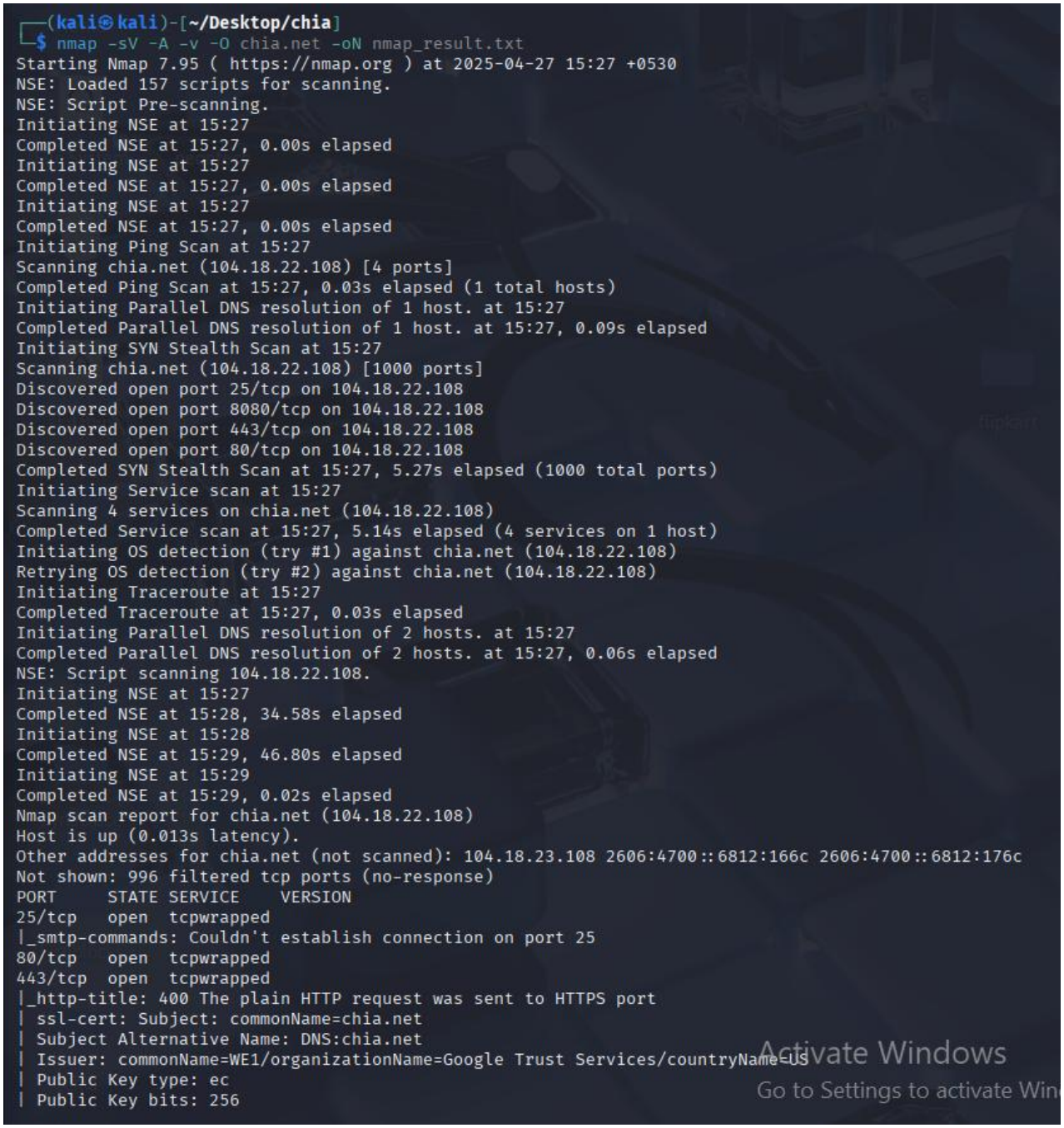
Looking up: https://api-uat-testnet11.cw.chia.net
Address: 192.168.0.1#53

Looking up: https://console.minio.sin.chia.net
Address: 192.168.0.1#53

Looking up: https://api.vault.chia.net
Address: 192.168.0.1#53
---

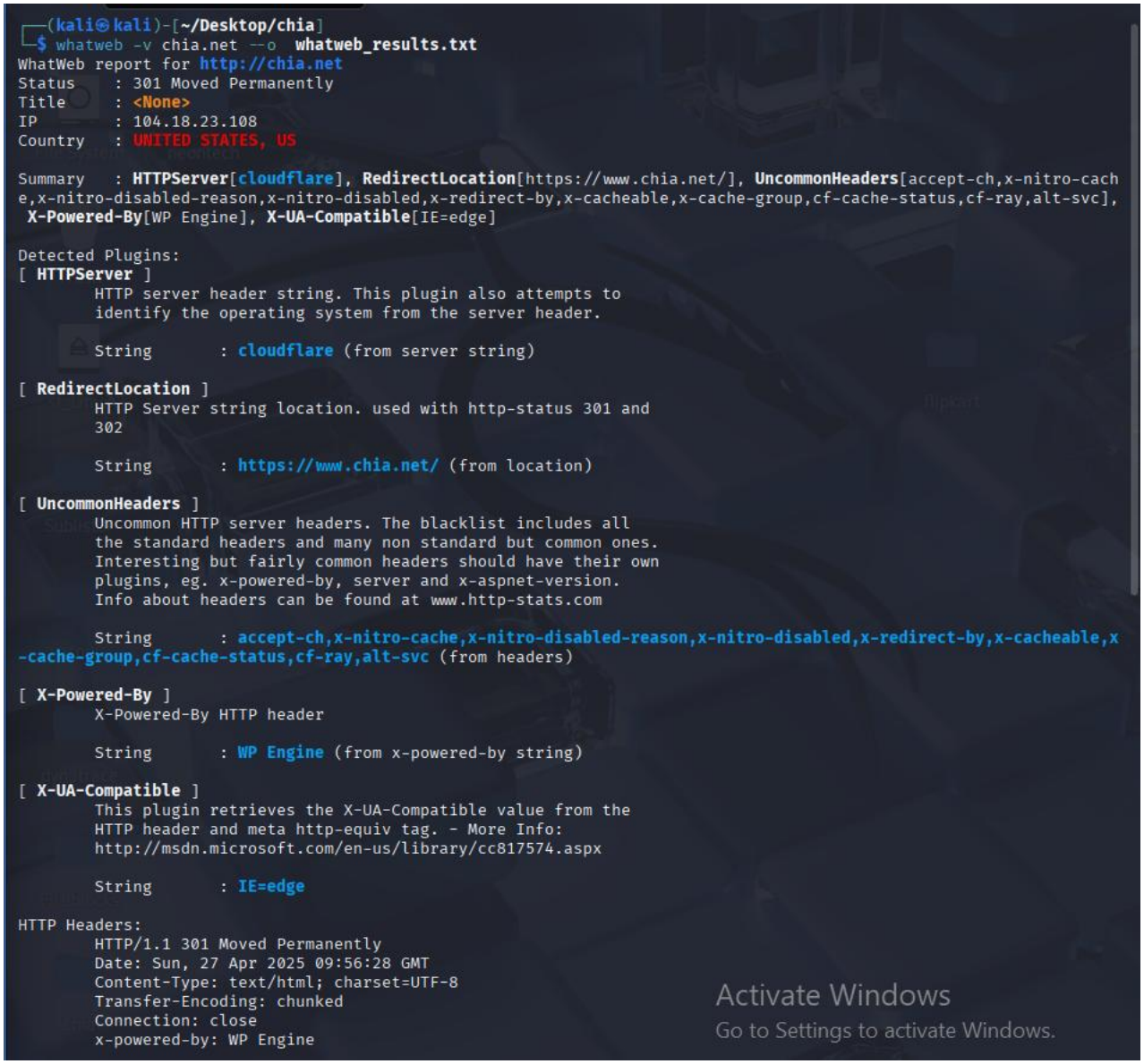
d. Open Ports

Tool: nmap: nmap_result.txt
Code: nmap -sV -A -v -O chia.net -oN nmap_results.txt
Explanation:
nmap - start the tool
-sV - Service and version detection
-A - OS detection, version detection, script scanning
-v - increase verbosity level
-O - Os detection
- *chia.net* - target website
-oN nmap_results.txt - result in an output text file



e. Used Technologies

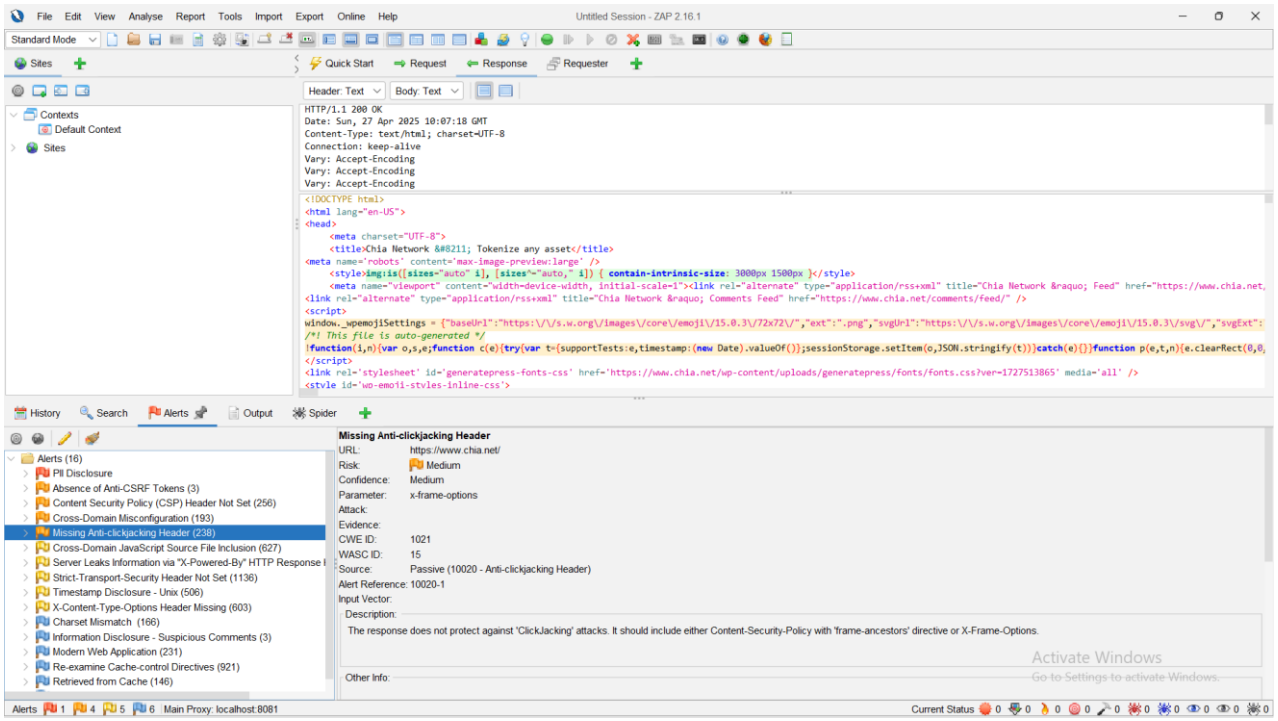
Tool: whatweb - whatweb_results.txt
Code: whatweb -v chia.net > whatweb_result.txt
Explanation:
whatweb - start whatweb tool
-v - verbose
Chia.net - target website
> whatweb_result.txt - file with the output



3. Step 02: Scanning and vulnerability identification

a. Identify Potential Vulnerabilities

Tool : OWASP ZAP
Vulnerability : Missing Anti-clickjacking Header



Missing Anti-clickjacking Header:

URL: https://www.chia.net/
Risk: Medium
Confidential: Medium
Parameter: x-frame-options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-1
Input Vector:

- Description: The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
- Other Info:
- Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
- Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
- Alert Tags:
    - WSTG-v42-CLNT-09: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking
    - OWASP_2021_A05: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
    - OWASP_2017_A06: https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
    - CWE-1021: https://cwe.mitre.org/data/definitions/1021.html

b. Missing Anti-Clickjacking Header

Anti-clickjacking headers are security mechanisms (like X-Frame-Options and Content-Security-Policy: frame-ancestors) used to prevent a website from being embedded inside an iframe on another domain. Without these protections, attackers can perform clickjacking attacks, tricking users into clicking on invisible or disguised elements that perform unintended actions, such as transferring money, changing settings, or granting permissions.

Cause of Missing Anti-clickjacking Header website:

- Failure to configure server responses with X-Frame-Options or CSP: frame-ancestors
- Outdated development practices relying only on client-side JavaScript for protection
- Misunderstanding or ignoring the threat of clickjacking during development
- Lack of security policies enforced in the web application infrastructure
- Using outdated server configurations or CMS platforms without frame protection

Propositions to Mitigation or Fix:

- Set X-Frame-Options Header: Use DENY to block all framing, or SAMEORIGIN to allow only from the same origin
- Use Content Security Policy (CSP) frame-ancestors Directive: A more flexible and modern approach to control allowed framing domains
- Avoid JavaScript-only Frame Busting: Rely on HTTP headers instead of client-side scripts for strong protection
- Secure Critical Pages First: Ensure login, payment, and admin panels are protected with anti-clickjacking headers
- Test Regularly: Use automated tools to detect missing or misconfigured anti-clickjacking headers
- Educate Development Teams: Train developers on the importance of proper frame protections during the secure coding lifecycle

4. Step 03: Exploitation and Validation

Request:

```
GET https://www.chia.net/ HTTP/1.1
host: www.chia.net
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
```

Response:

```
HTTP/1.1 200 OK
Date: Sun, 27 Apr 2025 10:07:18 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Accept-Encoding
```

```
<!DOCTYPE html>
<html lang="en-US">
<head>
    <meta charset="UTF-8">
    <title>Chia Network &#8211; Tokenize any asset</title>
<meta name='robots' content='max-image-preview:large' />
    <style>img:is([sizes="auto" i], [sizes^="auto," i]) { contain-intrinsic-size: 3000px 1500px }</style>
    <meta name="viewport" content="width=device-width, initial-scale=1"><link rel="alternate" type="application/rss+xml" title="Chia Network &raquo; Feed" href="https://www.chia.net/
<link rel="alternate" type="application/rss+xml" title="Chia Network &raquo; Comments Feed" href="https://www.chia.net/comments/feed/" />
<script>
window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/15.0.3\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/15.0.3\/svg\/","svgExt":
/*! This file is auto-generated */
!function(i,n){var o,s,e;function c(e){try{var t={supportTests:e,timestamp:(new Date).valueOf()};sessionStorage.setItem(o,JSON.stringify(t))}catch(e){}}function p(e,t,n){e.clearRect(0,0,
</script>
<link rel='stylesheet' id='generatepress-fonts-css' href='https://www.chia.net/wp-content/uploads/generatepress/fonts/fonts.css?ver=1727513865' media='all' />
<style id='wp-emoji-styles-inline-css'>
```

5. Step 04: Mitigation / Fix

Immediate Mitigation Actions:
1. Deny all framing – [*X-Frame-Options: DENY]*
2. Allow only same-origin framing
3. Block all framing or allow specific domains.

Long Term Prevention:
1. Use tools like *SecurityHeaders.com* or *OWASP ZAP* to scan for missing headers.
2. CI/CD integration.