Sri Lanka Institute of Information Technology

Specialized in Cyber Security

Year 2, Semester 2

IE2062 – Web Security

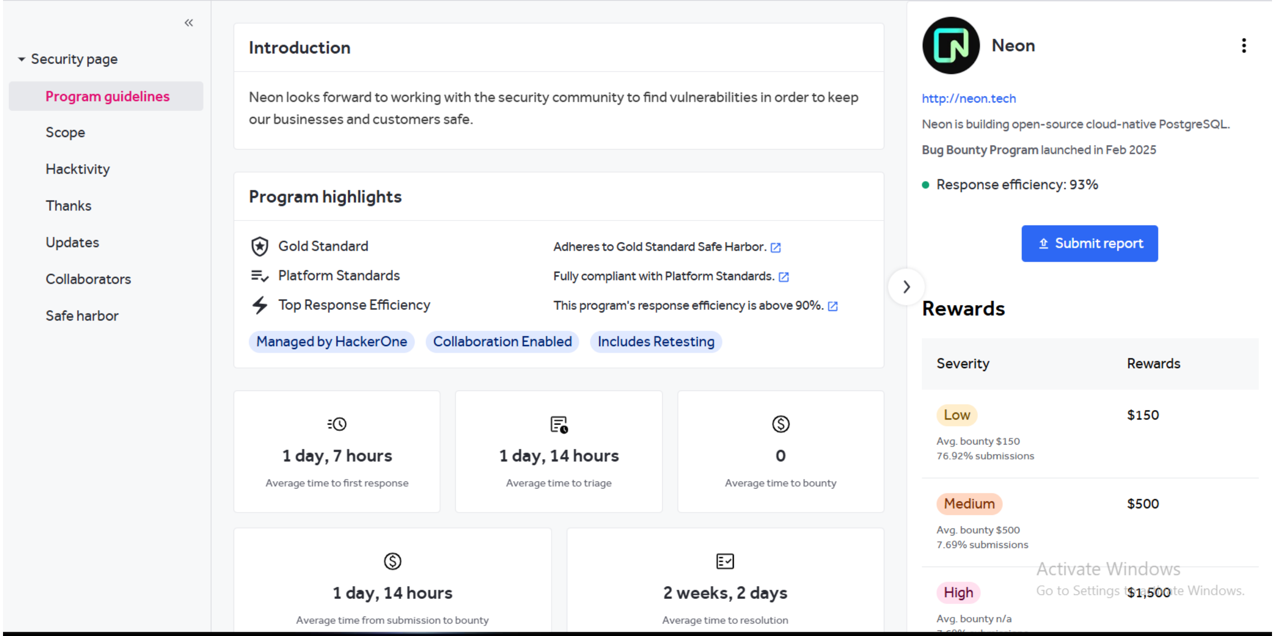
Bug Bounty – Report 02

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

Table of Contents

1. Website Overview

Neon Tech – Company offering a **serverless, cloud-native PostgreSQL database service**
HackerOne Link: Neon | Bug Bounty Program Policy | HackerOne



Introduction

Neon looks forward to working with the security community to find vulnerabilities in order to keep our businesses and customers safe.

Program highlights

Gold Standard	Adheres to Gold Standard Safe Harbor.
Platform Standards	Fully compliant with Platform Standards.
Top Response Efficiency	This program's response efficiency is above 90%.

1 day, 7 hours
Average time to first response

1 day, 14 hours
Average time to triage

0
Average time to bounty

1 day, 14 hours
Average time from submission to bounty

2 weeks, 2 days
Average time to resolution

Neon

http://neon.tech

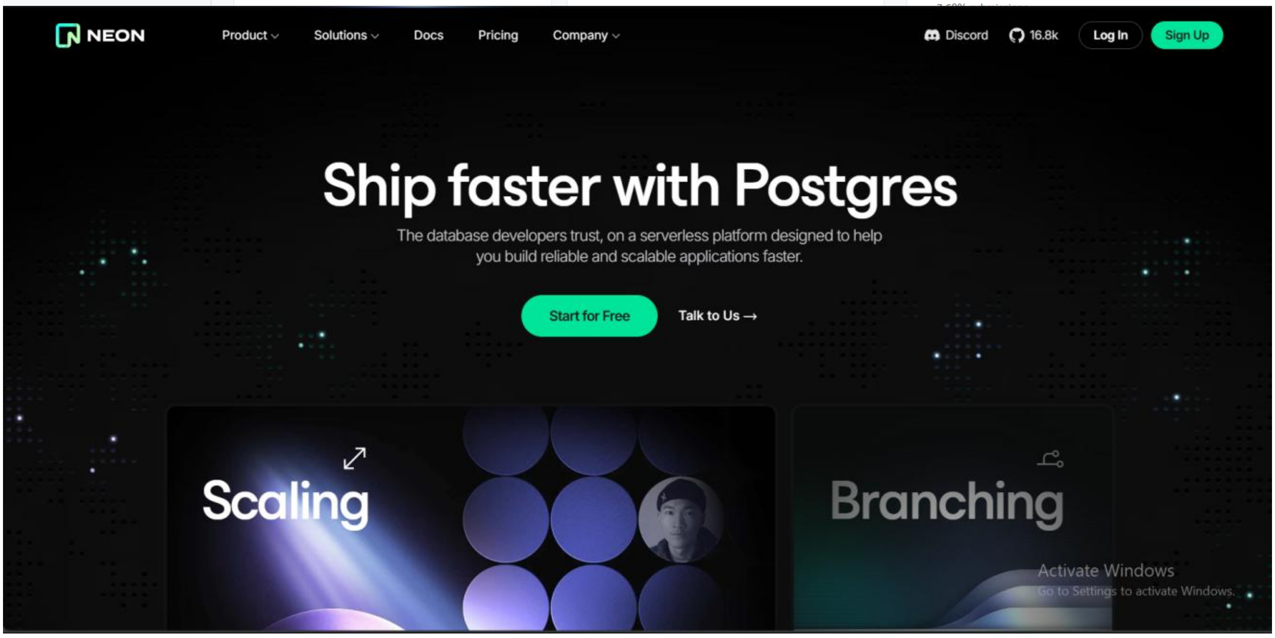
Neon is building open-source cloud-native PostgreSQL.

Bug Bounty Program launched in Feb 2025

● Response efficiency: 93%

Rewards

Severity	Rewards
Low Avg. bounty $150 76.92% submissions	$150
Medium Avg. bounty $500 7.69% submissions	$500
High Avg. bounty n/a	$1,500



Ship faster with Postgres

The database developers trust, on a serverless platform designed to help you build reliable and scalable applications faster.

Step 01: Gather Information.

a. Sub-domain Discovery

i. Sublist3r: Sublist3r Results.txt

Tool : Sublist3r

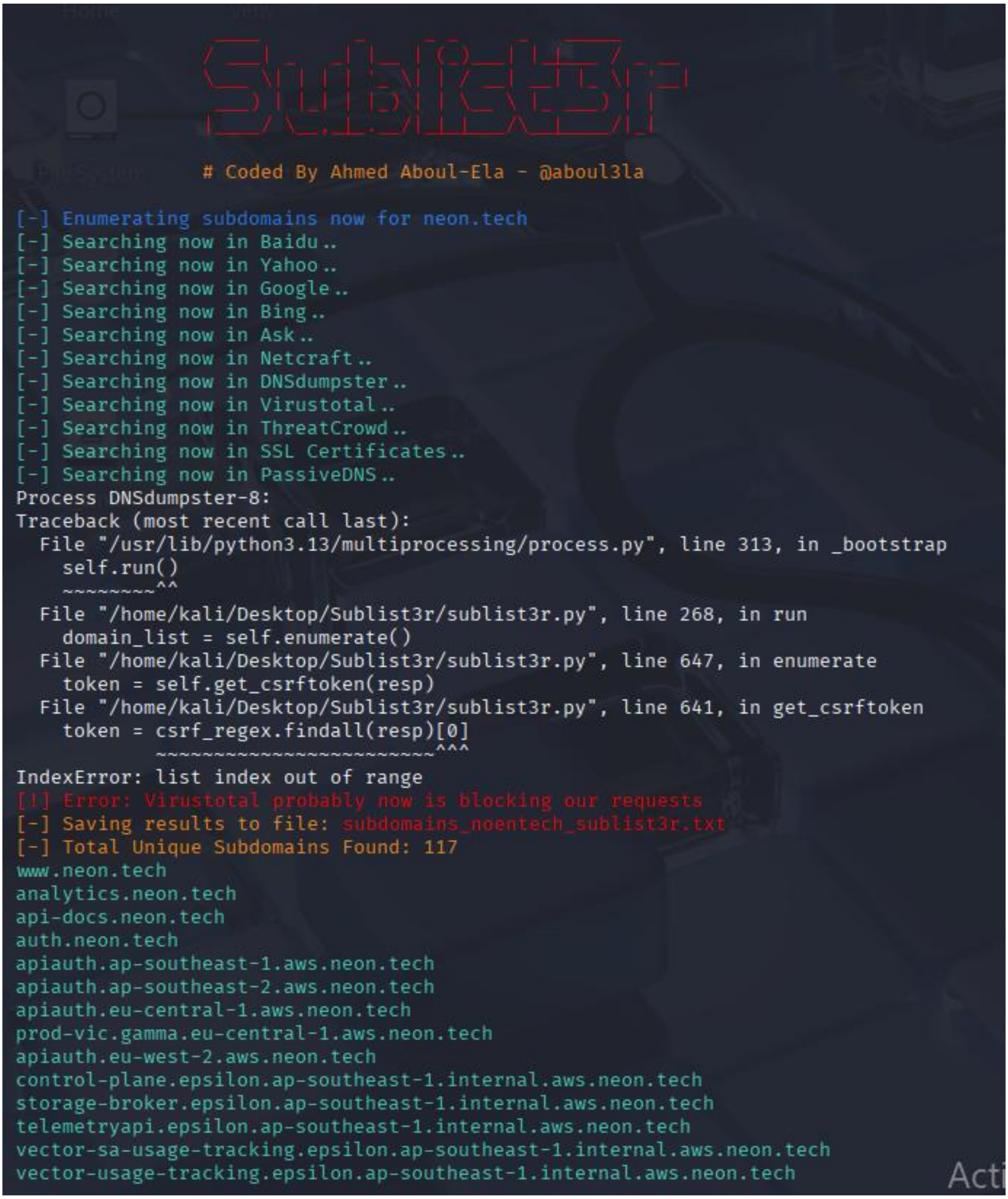
Code : python3 sublist3r.py -d neon.tech -o subdomains_neontech_sublist3r.txt

Explanation:

python3 sublist3r.py - Run the script using python

-d neon.tech - Target domain

-o subdomains_neontech_sublist3r.txt – Output file where the result is saved

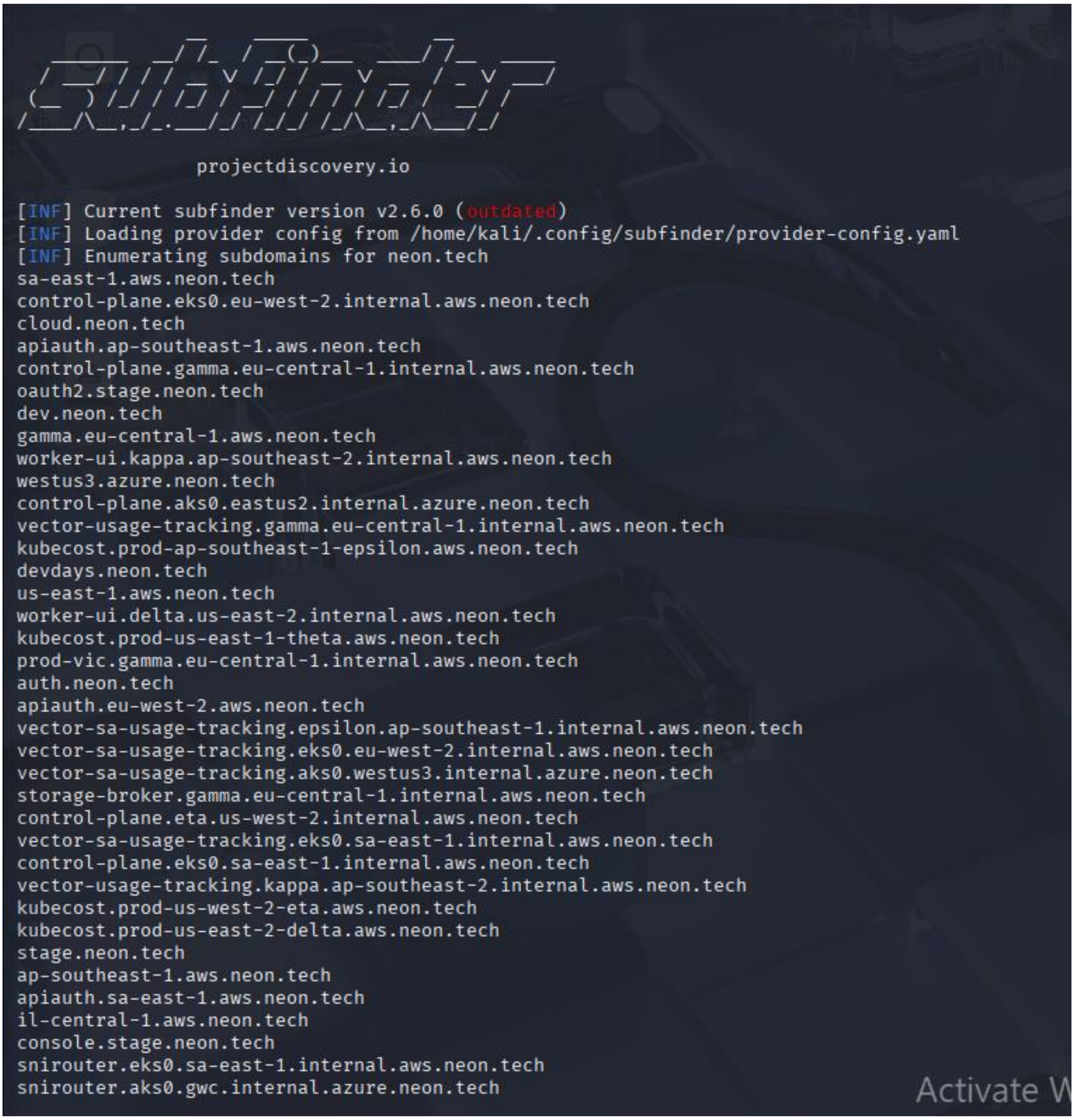


```
                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for neon.tech
[-] 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..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
    ~~~~~~~~^^
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 647, in enumerate
    token = self.get_csrftoken(resp)
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 641, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
            ~~~~~~~~~~~~~~~~~~~~~~~~^^^
IndexError: list index out of range
[!] Error: Virustotal probably now is blocking our requests
[-] Saving results to file: subdomains_noentech_sublist3r.txt
[-] Total Unique Subdomains Found: 117
www.neon.tech
analytics.neon.tech
api-docs.neon.tech
auth.neon.tech
apiauth.ap-southeast-1.aws.neon.tech
apiauth.ap-southeast-2.aws.neon.tech
apiauth.eu-central-1.aws.neon.tech
prod-vic.gamma.eu-central-1.aws.neon.tech
apiauth.eu-west-2.aws.neon.tech
control-plane.epsilon.ap-southeast-1.internal.aws.neon.tech
storage-broker.epsilon.ap-southeast-1.internal.aws.neon.tech
telemetryapi.epsilon.ap-southeast-1.internal.aws.neon.tech
vector-sa-usage-tracking.epsilon.ap-southeast-1.internal.aws.neon.tech
vector-usage-tracking.epsilon.ap-southeast-1.internal.aws.neon.tech
```

```
www.neon.tech
analytics.neon.tech
api-docs.neon.tech
auth.neon.tech
apiauth.ap-southeast-1.aws.neon.tech
apiauth.ap-southeast-2.aws.neon.tech
apiauth.eu-central-1.aws.neon.tech
prod-vic.gamma.eu-central-1.aws.neon.tech
apiauth.eu-west-2.aws.neon.tech
control-plane.epsilon.ap-southeast-1.internal.aws.neon.tech
storage-broker.epsilon.ap-southeast-1.internal.aws.neon.tech
telemetryapi.epsilon.ap-southeast-1.internal.aws.neon.tech
vector-sa-usage-tracking.epsilon.ap-southeast-1.internal.aws.neon.tech
vector-usage-tracking.epsilon.ap-southeast-1.internal.aws.neon.tech
worker-ui.epsilon.ap-southeast-1.internal.aws.neon.tech
control-plane.kappa.ap-southeast-2.internal.aws.neon.tech
telemetryapi.kappa.ap-southeast-2.internal.aws.neon.tech
vector-sa-usage-tracking.kappa.ap-southeast-2.internal.aws.neon.tech
vector-usage-tracking.kappa.ap-southeast-2.internal.aws.neon.tech
worker-ui.kappa.ap-southeast-2.internal.aws.neon.tech
control-plane.gamma.eu-central-1.internal.aws.neon.tech
prod-vic.gamma.eu-central-1.internal.aws.neon.tech
storage-broker.gamma.eu-central-1.internal.aws.neon.tech
telemetryapi.gamma.eu-central-1.internal.aws.neon.tech
vector-sa-usage-tracking.gamma.eu-central-1.internal.aws.neon.tech
vector-usage-tracking.gamma.eu-central-1.internal.aws.neon.tech
worker-ui.gamma.eu-central-1.internal.aws.neon.tech
control-plane.theta.eu-east-1.internal.aws.neon.tech
control-plane.eks0.eu-west-2.internal.aws.neon.tech
telemetryapi.eks0.eu-west-2.internal.aws.neon.tech
vector-sa-usage-tracking.eks0.eu-west-2.internal.aws.neon.tech
worker-ui.eks0.eu-west-2.internal.aws.neon.tech
control-plane.iota.il-central-1.internal.aws.neon.tech
vector-sa-usage-tracking.iota.il-central-1.internal.aws.neon.tech
vector-usage-tracking.iota.il-central-1.internal.aws.neon.tech
control-plane.eks0.sa-east-1.internal.aws.neon.tech
telemetryapi.eks0.sa-east-1.internal.aws.neon.tech
vector-sa-usage-tracking.eks0.sa-east-1.internal.aws.neon.tech
worker-ui.eks0.sa-east-1.internal.aws.neon.tech
control-plane.theta.us-east-1.internal.aws.neon.tech
telemetryapi.theta.us-east-1.internal.aws.neon.tech
vector-sa-usage-tracking.theta.us-east-1.internal.aws.neon.tech
vector-usage-tracking.theta.us-east-1.internal.aws.neon.tech
worker-ui.theta.us-east-1.internal.aws.neon.tech
control-plane.delta.us-east-2.internal.aws.neon.tech
storage-broker.delta.us-east-2.internal.aws.neon.tech
telemetryapi.delta.us-east-2.internal.aws.neon.tech
vector-sa-usage-tracking.delta.us-east-2.internal.aws.neon.tech
vector-usage-tracking.delta.us-east-2.internal.aws.neon.tech
worker-ui.delta.us-east-2.internal.aws.neon.tech
ext-metrics.infra.us-east-2.internal.aws.neon.tech
int-metrics-write.infra.us-east-2.internal.aws.neon.tech
vector-sa-console.service.us-east-2.internal.aws.neon.tech
vector-usage-tracking.service.us-east-2.internal.aws.neon.tech
vector-usage-tracking-sa.service.us-east-2.internal.aws.neon.tech
control-plane.eta.us-west-2.internal.aws.neon.tech
storage-broker.eta.us-west-2.internal.aws.neon.tech
```

ii. Subfindre: Subfinder_Result.txt

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



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

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for neon.tech
sa-east-1.aws.neon.tech
control-plane.eks0.eu-west-2.internal.aws.neon.tech
cloud.neon.tech
apiauth.ap-southeast-1.aws.neon.tech
control-plane.gamma.eu-central-1.internal.aws.neon.tech
oauth2.stage.neon.tech
dev.neon.tech
gamma.eu-central-1.aws.neon.tech
worker-ui.kappa.ap-southeast-2.internal.aws.neon.tech
westus3.azure.neon.tech
control-plane.aks0.eastus2.internal.azure.neon.tech
vector-usage-tracking.gamma.eu-central-1.internal.aws.neon.tech
kubecost.prod-ap-southeast-1-epsilon.aws.neon.tech
devdays.neon.tech
us-east-1.aws.neon.tech
worker-ui.delta.us-east-2.internal.aws.neon.tech
kubecost.prod-us-east-1-theta.aws.neon.tech
prod-vic.gamma.eu-central-1.internal.aws.neon.tech
auth.neon.tech
apiauth.eu-west-2.aws.neon.tech
vector-sa-usage-tracking.epsilon.ap-southeast-1.internal.aws.neon.tech
vector-sa-usage-tracking.eks0.eu-west-2.internal.aws.neon.tech
vector-sa-usage-tracking.aks0.westus3.internal.azure.neon.tech
storage-broker.gamma.eu-central-1.internal.aws.neon.tech
control-plane.eta.us-west-2.internal.aws.neon.tech
vector-sa-usage-tracking.eks0.sa-east-1.internal.aws.neon.tech
control-plane.eks0.sa-east-1.internal.aws.neon.tech
vector-usage-tracking.kappa.ap-southeast-2.internal.aws.neon.tech
kubecost.prod-us-west-2-eta.aws.neon.tech
kubecost.prod-us-east-2-delta.aws.neon.tech
stage.neon.tech
ap-southeast-1.aws.neon.tech
apiauth.sa-east-1.aws.neon.tech
il-central-1.aws.neon.tech
console.stage.neon.tech
snirouter.eks0.sa-east-1.internal.aws.neon.tech
snirouter.aks0.gwc.internal.azure.neon.tech
```

sa-east-1.aws.neon.tech
control-plane.eks0.eu-west-2.internal.aws.neon.tech
cloud.neon.tech
apiauth.ap-southeast-1.aws.neon.tech
control-plane.gamma.eu-central-1.internal.aws.neon.tech
oauth2.stage.neon.tech
dev.neon.tech
gamma.eu-central-1.aws.neon.tech
worker-ui.kappa.ap-southeast-2.internal.aws.neon.tech
westus3.azure.neon.tech

```
control-plane.aks0.eastus2.internal.azure.neon.tech
vector-usage-tracking.gamma.eu-central-1.internal.aws.neon.tech
kubecost.prod-ap-southeast-1-epsilon.aws.neon.tech
devdays.neon.tech
us-east-1.aws.neon.tech
worker-ui.delta.us-east-2.internal.aws.neon.tech
kubecost.prod-us-east-1-theta.aws.neon.tech
prod-vic.gamma.eu-central-1.internal.aws.neon.tech
auth.neon.tech
apiauth.eu-west-2.aws.neon.tech
vector-sa-usage-tracking.epsilon.ap-southeast-1.internal.aws.neon.tech
vector-sa-usage-tracking.eks0.eu-west-2.internal.aws.neon.tech
vector-sa-usage-tracking.aks0.westus3.internal.azure.neon.tech
storage-broker.gamma.eu-central-1.internal.aws.neon.tech
control-plane.eta.us-west-2.internal.aws.neon.tech
vector-sa-usage-tracking.eks0.sa-east-1.internal.aws.neon.tech
control-plane.eks0.sa-east-1.internal.aws.neon.tech
vector-usage-tracking.kappa.ap-southeast-2.internal.aws.neon.tech
kubecost.prod-us-west-2-eta.aws.neon.tech
kubecost.prod-us-east-2-delta.aws.neon.tech
stage.neon.tech
ap-southeast-1.aws.neon.tech
apiauth.sa-east-1.aws.neon.tech
il-central-1.aws.neon.tech
console.stage.neon.tech
snirouter.eks0.sa-east-1.internal.aws.neon.tech
snirouter.aks0.gwc.internal.azure.neon.tech
vector-usage-tracking.service.us-east-2.internal.aws.neon.tech
telemetryapi.eks0.sa-east-1.internal.aws.neon.tech
worker-ui.epsilon.ap-southeast-1.internal.aws.neon.tech
us-east-2.aws.neon.tech
storage-broker.eta.us-west-2.internal.aws.neon.tech
stress.neon.tech
epsilon.ap-southeast-1.aws.neon.tech
gamma.us-east-2.aws.neon.tech
worker-ui.eks0.eu-west-2.internal.aws.neon.tech
api-docs.neon.tech
```

b. Live Subdomain Discovery

Tool **:** httpx: Livesub_Results.txt

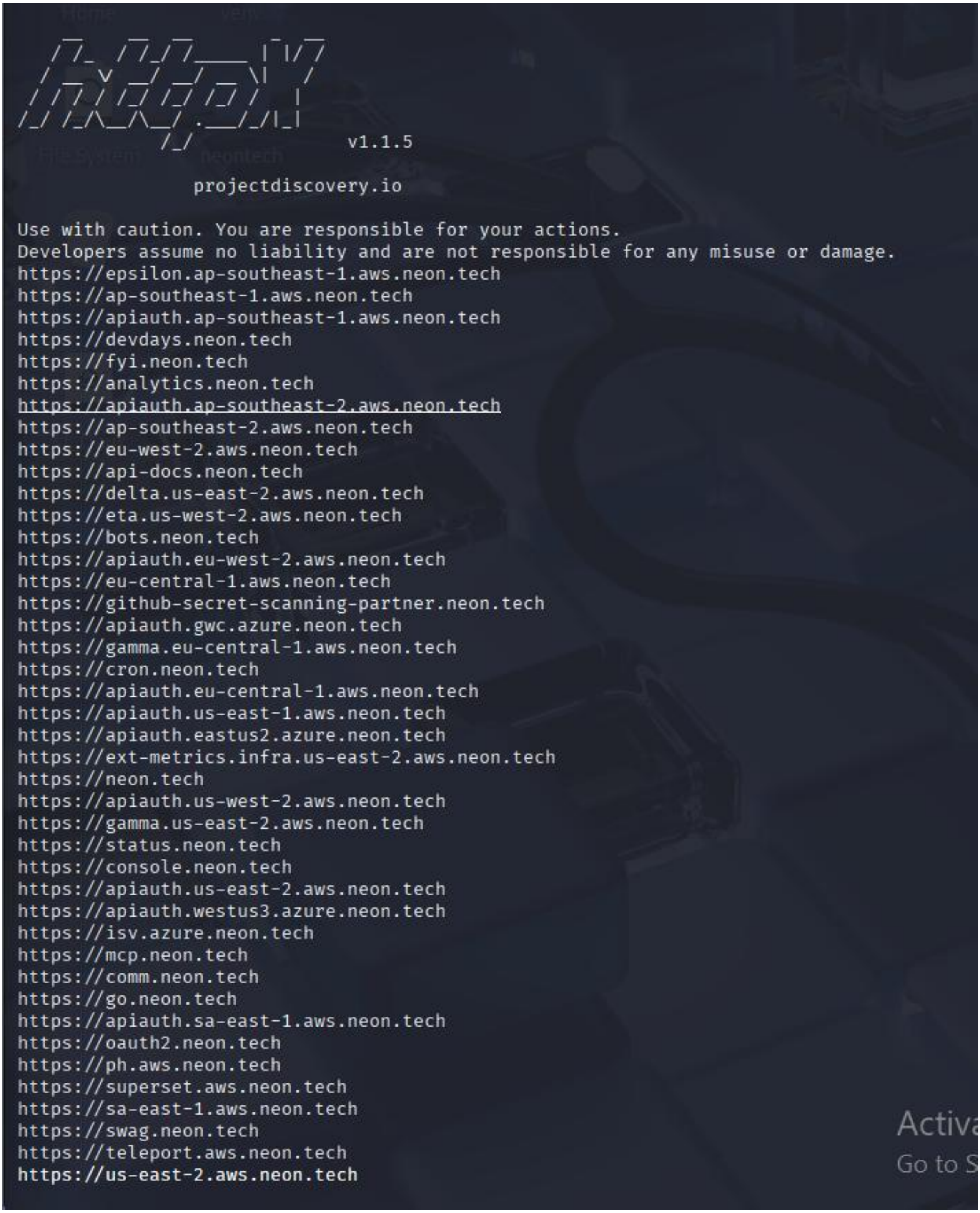
Code **:** httpx-toolkit -l subfinder_result.txt -o livesub_results.txt

Explanation:

httpx-toolkit - run the httpx tool

-*l subfinder_result.txt* – mention the file containing input

-*o livesub_results.txt* – mention the file which should write the output



```
    __    __  __       _  __
   / /_  / /_/ /_____ | |/ /
  / __ \/ __/ __/ __ \|   /
 / / / / /_/ /_/ /_/ /   |
/_/ /_/\__/\__/ .___/_/|_|
             /_/              v1.1.5

                projectdiscovery.io

Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible for any misuse or damage.
https://epsilon.ap-southeast-1.aws.neon.tech
https://ap-southeast-1.aws.neon.tech
https://apiauth.ap-southeast-1.aws.neon.tech
https://devdays.neon.tech
https://fyi.neon.tech
https://analytics.neon.tech
https://apiauth.ap-southeast-2.aws.neon.tech
https://ap-southeast-2.aws.neon.tech
https://eu-west-2.aws.neon.tech
https://api-docs.neon.tech
https://delta.us-east-2.aws.neon.tech
https://eta.us-west-2.aws.neon.tech
https://bots.neon.tech
https://apiauth.eu-west-2.aws.neon.tech
https://eu-central-1.aws.neon.tech
https://github-secret-scanning-partner.neon.tech
https://apiauth.gwc.azure.neon.tech
https://gamma.eu-central-1.aws.neon.tech
https://cron.neon.tech
https://apiauth.eu-central-1.aws.neon.tech
https://apiauth.us-east-1.aws.neon.tech
https://apiauth.eastus2.azure.neon.tech
https://ext-metrics.infra.us-east-2.aws.neon.tech
https://neon.tech
https://apiauth.us-west-2.aws.neon.tech
https://gamma.us-east-2.aws.neon.tech
https://status.neon.tech
https://console.neon.tech
https://apiauth.us-east-2.aws.neon.tech
https://apiauth.westus3.azure.neon.tech
https://isv.azure.neon.tech
https://mcp.neon.tech
https://comm.neon.tech
https://go.neon.tech
https://apiauth.sa-east-1.aws.neon.tech
https://oauth2.neon.tech
https://ph.aws.neon.tech
https://superset.aws.neon.tech
https://sa-east-1.aws.neon.tech
https://swag.neon.tech
https://teleport.aws.neon.tech
https://us-east-2.aws.neon.tech
```

https://epsilon.ap-southeast-1.aws.neon.tech
https://ap-southeast-1.aws.neon.tech
https://apiauth.ap-southeast-1.aws.neon.tech
https://devdays.neon.tech
https://fyi.neon.tech
https://analytics.neon.tech
https://apiauth.ap-southeast-2.aws.neon.tech
https://ap-southeast-2.aws.neon.tech
https://eu-west-2.aws.neon.tech
https://api-docs.neon.tech
https://delta.us-east-2.aws.neon.tech
https://eta.us-west-2.aws.neon.tech
https://bots.neon.tech
https://apiauth.eu-west-2.aws.neon.tech
https://eu-central-1.aws.neon.tech
https://github-secret-scanning-partner.neon.tech
https://apiauth.gwc.azure.neon.tech
https://gamma.eu-central-1.aws.neon.tech
https://cron.neon.tech
https://apiauth.eu-central-1.aws.neon.tech
https://apiauth.us-east-1.aws.neon.tech
https://apiauth.eastus2.azure.neon.tech
https://ext-metrics.infra.us-east-2.aws.neon.tech
https://neon.tech
https://apiauth.us-west-2.aws.neon.tech
https://gamma.us-east-2.aws.neon.tech
https://status.neon.tech
https://console.neon.tech
https://apiauth.us-east-2.aws.neon.tech
https://apiauth.westus3.azure.neon.tech
https://isv.azure.neon.tech
https://mcp.neon.tech
https://comm.neon.tech
https://go.neon.tech
https://apiauth.sa-east-1.aws.neon.tech
https://oauth2.neon.tech
https://ph.aws.neon.tech
https://superset.aws.neon.tech
https://sa-east-1.aws.neon.tech
https://swag.neon.tech
https://teleport.aws.neon.tech
https://us-east-2.aws.neon.tech
https://us-east-1.aws.neon.tech
https://us-west-2.aws.neon.tech
https://track.neon.tech
https://vpce.ap-southeast-1.aws.neon.tech
https://vpce.eu-central-1.aws.neon.tech
https://vpce.ap-southeast-2.aws.neon.tech
https://trust.neon.tech
https://vpce.us-east-1.aws.neon.tech
https://vpce.us-east-2.aws.neon.tech
https://vpce.us-west-2.aws.neon.tech
https://www.neon.tech

c. IP Discovery

Tool: nslookup: nslookup_Results.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: $sub" >> ips.txt
  nslookup "$sub" | awk '/^Name:|^Address:/' >> ips.txt
  echo "-----------------------" >> ips.txt
done < livesub_results.txt
```

Explanation:

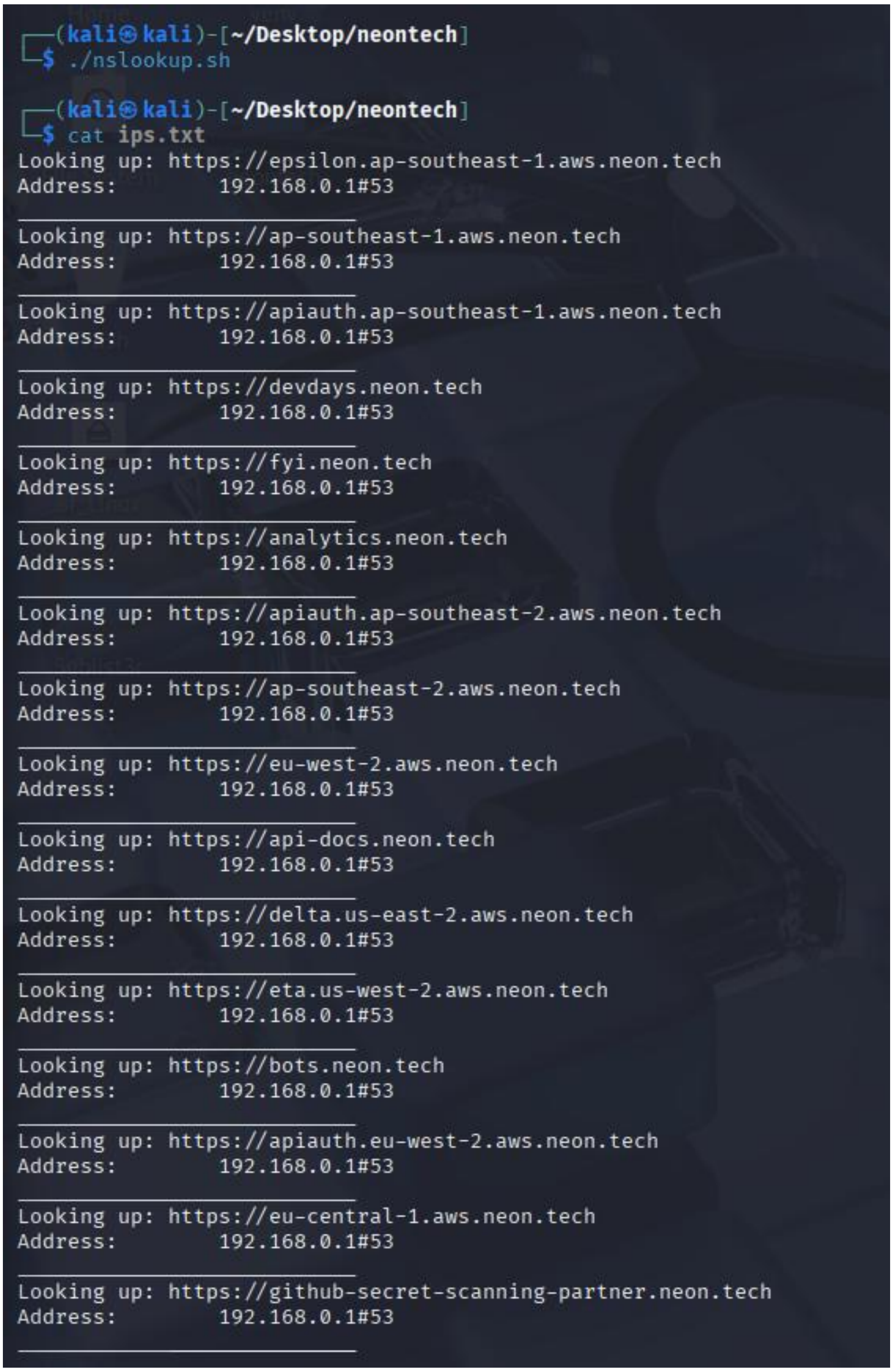
While read sub; do - start of the loop

Echo “Looking up: $sub”>>ips.txt - print message “Looking up: subdomain” into the file “ips.txt”

nslookup “$sub” | awk ‘/^Name:|^Address:/’ >> ips.txt - run the nslookup command

echo “__________________” >> ips.txt - separate one subdomain details from another

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



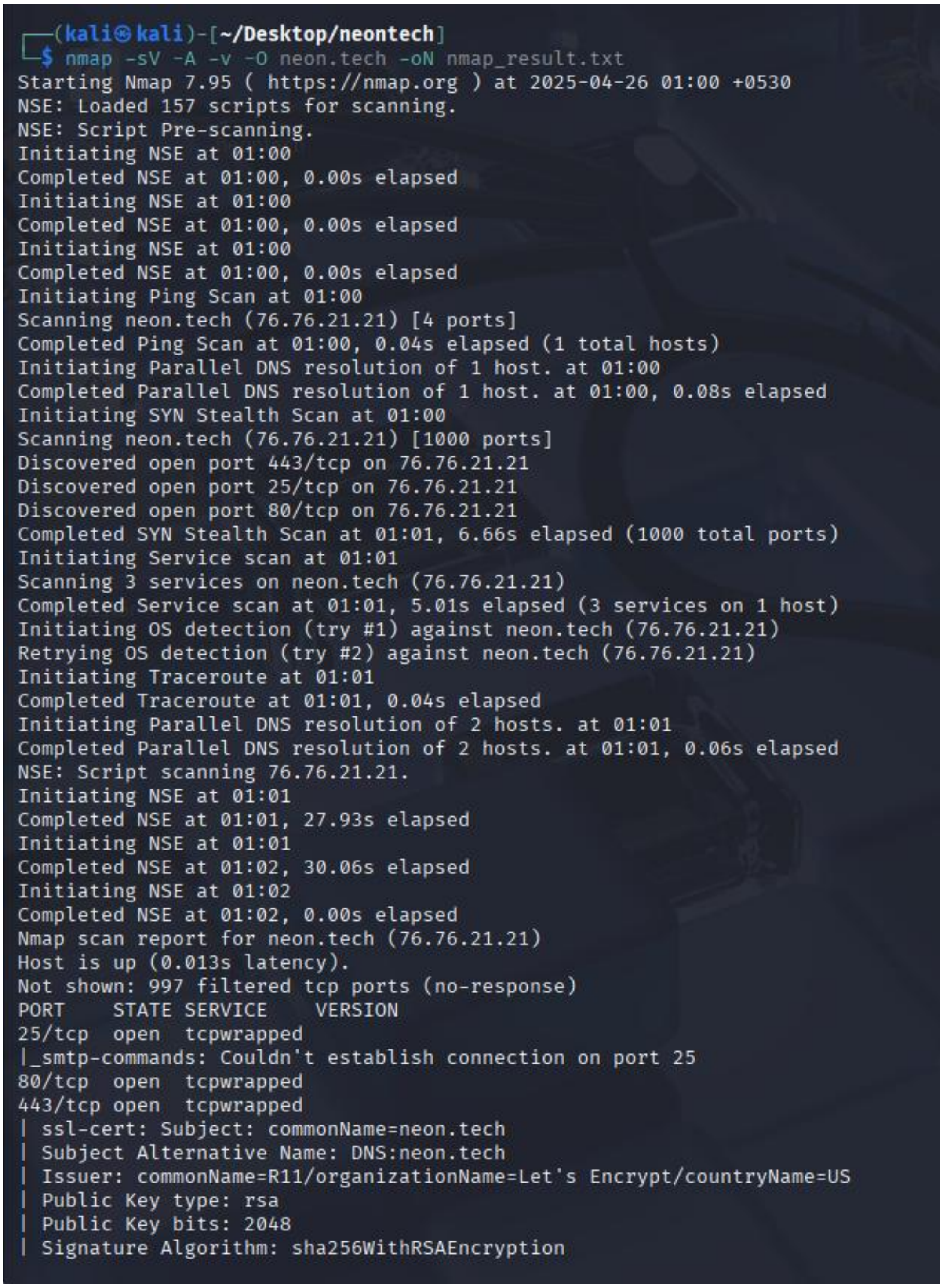
```
┌──(kali㉿kali)-[~/Desktop/neontech]
└─$ ./nslookup.sh

┌──(kali㉿kali)-[~/Desktop/neontech]
└─$ cat ips.txt
Looking up: https://epsilon.ap-southeast-1.aws.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://ap-southeast-1.aws.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://apiauth.ap-southeast-1.aws.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://devdays.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://fyi.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://analytics.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://apiauth.ap-southeast-2.aws.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://ap-southeast-2.aws.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://eu-west-2.aws.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://api-docs.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://delta.us-east-2.aws.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://eta.us-west-2.aws.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://bots.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://apiauth.eu-west-2.aws.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://eu-central-1.aws.neon.tech
Address:        192.168.0.1#53
___________________________
Looking up: https://github-secret-scanning-partner.neon.tech
Address:        192.168.0.1#53
___________________________
```

IP list:

```
Looking up: https://epsilon.ap-southeast-1.aws.neon.tech
Address:       192.168.0.1#53

Looking up: https://ap-southeast-1.aws.neon.tech
Address:       192.168.0.1#53

Looking up: https://apiauth.ap-southeast-1.aws.neon.tech
Address:       192.168.0.1#53

Looking up: https://devdays.neon.tech
Address:       192.168.0.1#53

Looking up: https://fyi.neon.tech
Address:       192.168.0.1#53

Looking up: https://analytics.neon.tech
Address:       192.168.0.1#53

Looking up: https://apiauth.ap-southeast-2.aws.neon.tech
Address:       192.168.0.1#53

Looking up: https://ap-southeast-2.aws.neon.tech
Address:       192.168.0.1#53

Looking up: https://eu-west-2.aws.neon.tech
Address:       192.168.0.1#53

Looking up: https://api-docs.neon.tech
Address:       192.168.0.1#53

Looking up: https://delta.us-east-2.aws.neon.tech
Address:       192.168.0.1#53

Looking up: https://eta.us-west-2.aws.neon.tech
Address:       192.168.0.1#53

Looking up: https://bots.neon.tech
Address:       192.168.0.1#53

Looking up: https://apiauth.eu-west-2.aws.neon.tech
Address:       192.168.0.1#53

Looking up: https://eu-central-1.aws.neon.tech
Address:       192.168.0.1#53

Looking up: https://github-secret-scanning-partner.neon.tech
Address:       192.168.0.1#53
```

d. Open Ports

Tool: nmap: nmap_Result.txt
Code: nmap -sV -A -v -O neon.tech -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
- neon.tech - target website
-oN nmap_results.txt - result in an output text file



```
┌──(kali㉿kali)-[~/Desktop/neontech]
└─$ nmap -sV -A -v -O neon.tech -oN nmap_result.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 01:00 +0530
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:00
Completed NSE at 01:00, 0.00s elapsed
Initiating NSE at 01:00
Completed NSE at 01:00, 0.00s elapsed
Initiating NSE at 01:00
Completed NSE at 01:00, 0.00s elapsed
Initiating Ping Scan at 01:00
Scanning neon.tech (76.76.21.21) [4 ports]
Completed Ping Scan at 01:00, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:00
Completed Parallel DNS resolution of 1 host. at 01:00, 0.08s elapsed
Initiating SYN Stealth Scan at 01:00
Scanning neon.tech (76.76.21.21) [1000 ports]
Discovered open port 443/tcp on 76.76.21.21
Discovered open port 25/tcp on 76.76.21.21
Discovered open port 80/tcp on 76.76.21.21
Completed SYN Stealth Scan at 01:01, 6.66s elapsed (1000 total ports)
Initiating Service scan at 01:01
Scanning 3 services on neon.tech (76.76.21.21)
Completed Service scan at 01:01, 5.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against neon.tech (76.76.21.21)
Retrying OS detection (try #2) against neon.tech (76.76.21.21)
Initiating Traceroute at 01:01
Completed Traceroute at 01:01, 0.04s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 01:01
Completed Parallel DNS resolution of 2 hosts. at 01:01, 0.06s elapsed
NSE: Script scanning 76.76.21.21.
Initiating NSE at 01:01
Completed NSE at 01:01, 27.93s elapsed
Initiating NSE at 01:01
Completed NSE at 01:02, 30.06s elapsed
Initiating NSE at 01:02
Completed NSE at 01:02, 0.00s elapsed
Nmap scan report for neon.tech (76.76.21.21)
Host is up (0.013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
25/tcp  open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=neon.tech
| Subject Alternative Name: DNS:neon.tech
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
```

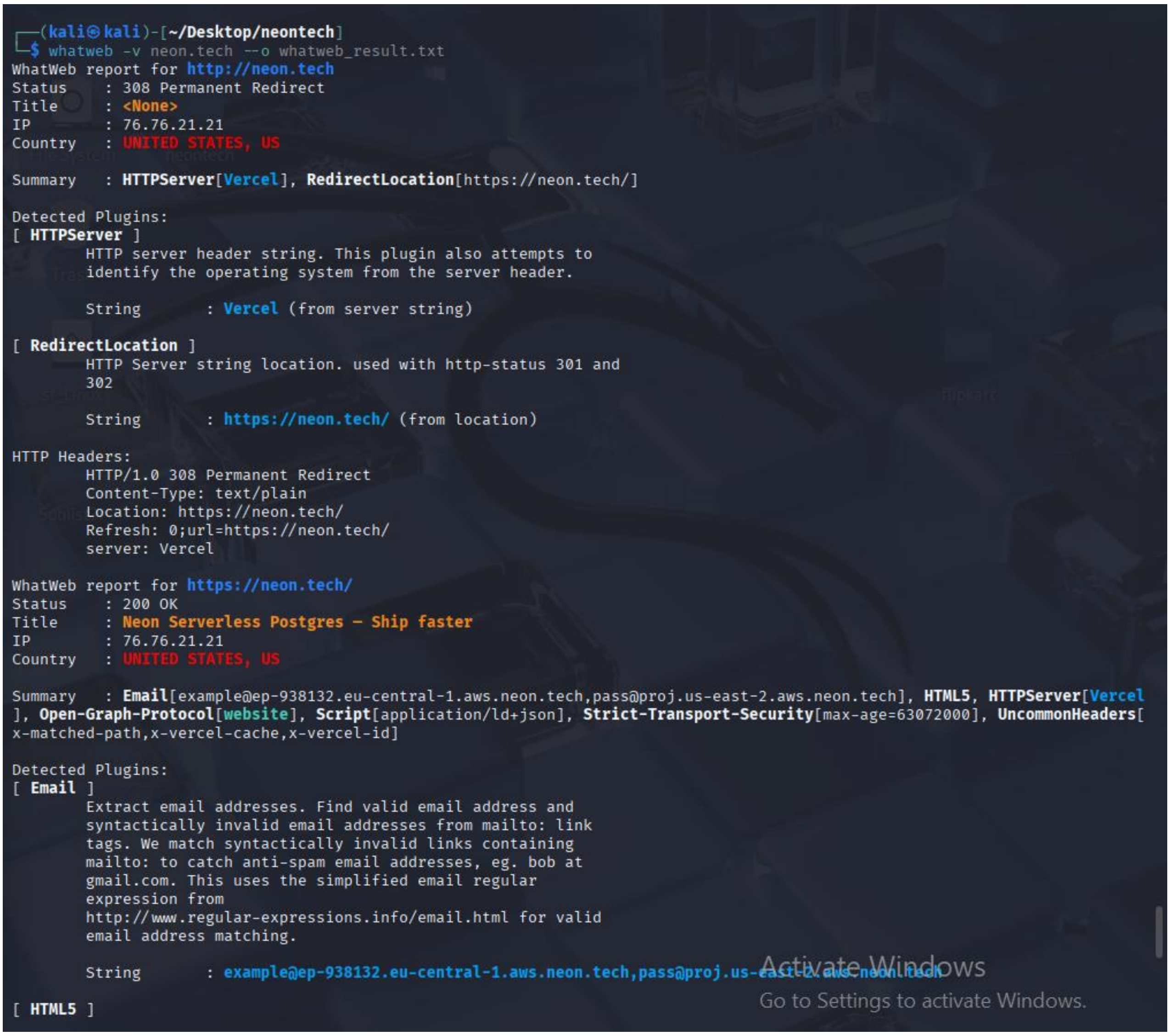
e. Used Technologies

Tool: whatweb - Whatweb_Result.txt

Code: whatweb -v neon.tech > whatweb_result.txt

Explanation:

whatweb - start whatweb tool
-v - verbose
Neon.tech - target website
> *whatweb_result.txt* - file with the output



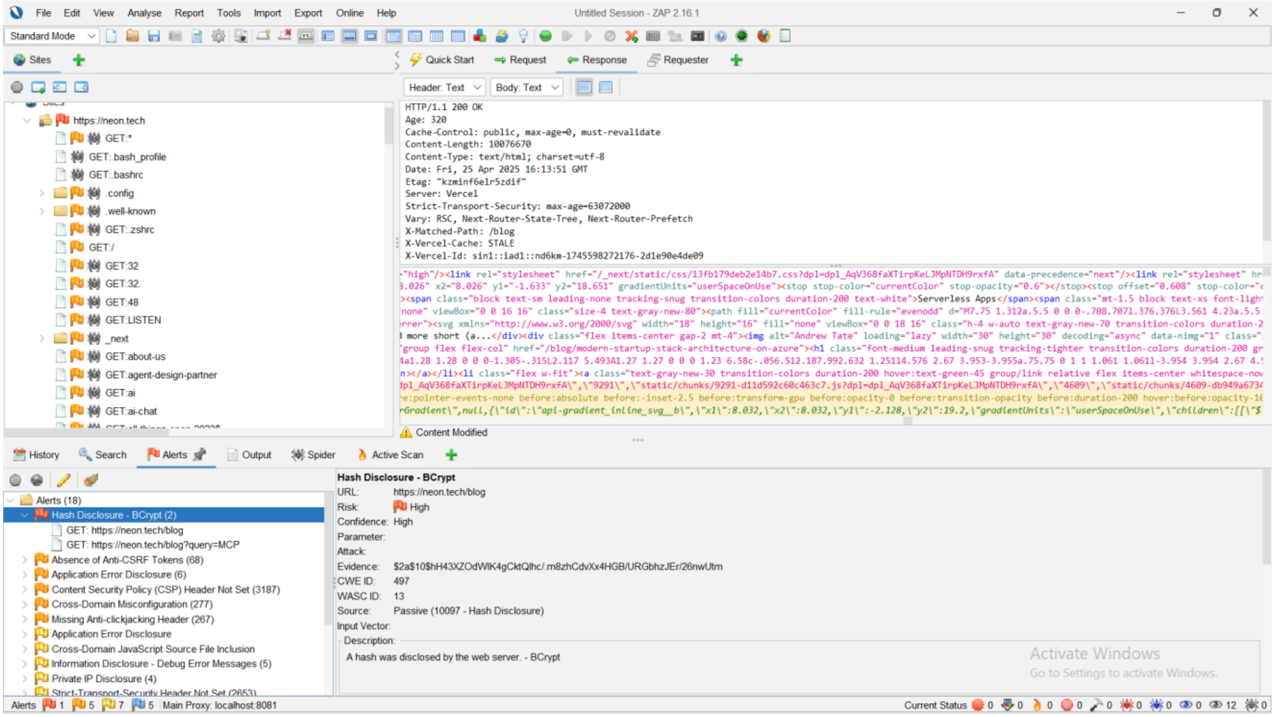
```
┌──(kali㉿kali)-[~/Desktop/neontech]
└─$ whatweb -v neon.tech --o whatweb_result.txt
WhatWeb report for http://neon.tech
Status    : 308 Permanent Redirect
Title     : <None>
IP        : 76.76.21.21
Country   : UNITED STATES, US

Summary   : HTTPServer[Vercel], RedirectLocation[https://neon.tech/]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Vercel (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://neon.tech/ (from location)

HTTP Headers:
        HTTP/1.0 308 Permanent Redirect
        Content-Type: text/plain
        Location: https://neon.tech/
        Refresh: 0;url=https://neon.tech/
        server: Vercel

WhatWeb report for https://neon.tech/
Status    : 200 OK
Title     : Neon Serverless Postgres — Ship faster
IP        : 76.76.21.21
Country   : UNITED STATES, US

Summary   : Email[example@ep-938132.eu-central-1.aws.neon.tech,pass@proj.us-east-2.aws.neon.tech], HTML5, HTTPServer[Vercel
], Open-Graph-Protocol[website], Script[application/ld+json], Strict-Transport-Security[max-age=63072000], UncommonHeaders[
x-matched-path,x-vercel-cache,x-vercel-id]

Detected Plugins:
[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
        tags. We match syntactically invalid links containing
        mailto: to catch anti-spam email addresses, eg. bob at
        gmail.com. This uses the simplified email regular
        expression from
        http://www.regular-expressions.info/email.html for valid
        email address matching.

        String       : example@ep-938132.eu-central-1.aws.neon.tech,pass@proj.us-east-2.aws.neon.tech

[ HTML5 ]
```

3. Step 02: Scanning and vulnerability identification

a. Identify Potential Vulnerabilities

Tool : OWASP ZAP

Vulnerability : HASH Disclosure



```
HTTP/1.1 200 OK
Age: 320
Cache-Control: public, max-age=0, must-revalidate
Content-Length: 10076670
Content-Type: text/html; charset=utf-8
Date: Fri, 25 Apr 2025 16:13:51 GMT
Etag: "kzminf6elr5zdif"
Server: Vercel
Strict-Transport-Security: max-age=63072000
Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch
X-Matched-Path: /blog
X-Vercel-Cache: STALE
X-Vercel-Id: sin1::iad1::nd6km-1745598272176-2d1e90e4de09
```

Alerts (18)
- Hash Disclosure - BCrypt (2)
  - GET: https://neon.tech/blog
  - GET: https://neon.tech/blog?query=MCP
- Absence of Anti-CSRF Tokens (68)
- Application Error Disclosure (6)
- Content Security Policy (CSP) Header Not Set (3187)
- Cross-Domain Misconfiguration (277)
- Missing Anti-clickjacking Header (267)
- Application Error Disclosure
- Cross-Domain JavaScript Source File Inclusion
- Information Disclosure - Debug Error Messages (5)
- Private IP Disclosure (4)
- Strict-Transport-Security Header Not Set (2653)

Hash Disclosure - BCrypt
URL: https://neon.tech/blog
Risk: High
Confidence: High
Parameter:
Attack:
Evidence: $2a$10$hH43XZOdWIK4gCktQlhc/.m8zhCdvXx4HGB/URGbhzJEr/26nwUtm
CWE ID: 497
WASC ID: 13
Source: Passive (10097 - Hash Disclosure)
Input Vector:
Description:
A hash was disclosed by the web server. - BCrypt

Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
https://neon.tech
Content Modified
History
Search
Alerts
Output
Spider
Active Scan
Activate Windows
Go to Settings to activate Windows.
Alerts 1 5 7 5 Main Proxy: localhost:8081
Current Status 0 0 0 0 0 0 0 0 12 0

Hash Disclosure:

URL: https://neon.tech/blog

Risk: High

Confidential: High

Parameter:

Attack:

Evidence: $2a$10$hH43XZOdWlK4gCktQlhc/.m8zhCdvXx4HGB/URGbhzJEr/26nwUtm

CWE ID: 497

WASC ID: 13

Source: Passive (10097 - Hash Disclosure)

Input Vector:

- Description: A hash was disclosed by the web server. - BCrypt.
- Other Info:
- Solution: Ensure that hashes that are used to protect credentials or other resources are not leaked by the web server or database. There is typically no requirement for password hashes to be accessible to the web browser.
- Reference: https://openwall.info/wiki/john/sample-hashes
- Alert Tags:
  - OWASP_2021_A04: https://owasp.org/Top10/A04_2021-Insecure_Design/
  - OWASP_2017_A03: https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html
  - CWE-497: https://cwe.mitre.org/data/definitions/497.html

b. Hash Disclosure

Hash disclosure refers to the exposure of hashed values—especially of sensitive data like passwords—through web pages, APIs, headers, or source code. While hashes are not plaintext, if they're leaked and weak hashing algorithms are used (like MD5 or SHA-1), they can potentially be cracked using dictionary attacks or rainbow tables. This can compromise user credentials and expose systems to further attacks such as credential stuffing.

Cause of PII in website:

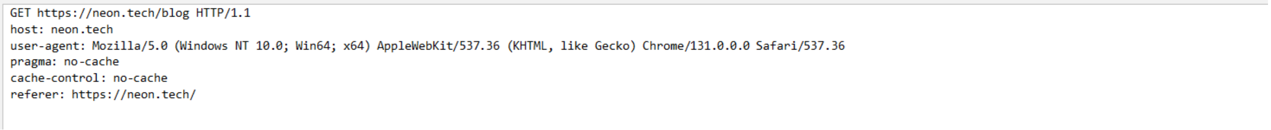
- Exposing hashed passwords or tokens in client-side code or responses
- Displaying hashed values in URLs, error messages, or debug outputs
- Logging hashed credentials insecurely in server logs
- Weak or outdated hashing algorithms (e.g., MD5, SHA-1)
- No salting of hashes, making them vulnerable to precomputed attacks
- Misconfigured debugging tools or development environments pushed to production

Propositions to Mitigation or Fix:

- Use Strong Hashing Algorithms: Use secure, modern algorithms like bcrypt, scrypt, or Argon2
- Implement Salting: Add a unique salt to each hash to prevent precomputed attacks
- Avoid Client-Side Hashing: Perform all sensitive hashing on the server side only
- Secure Logging Practices: Avoid logging sensitive hashed data, especially in plaintext logs
- Do Not Leak Hashes in Responses: Ensure hash values are not included in API responses, headers, or error messages
- Use HTTPS Everywhere: Prevent man-in-the-middle attacks that could capture hashes during transmission
- Regular Security Reviews: Audit code, logs, and network traffic for accidental hash disclosures

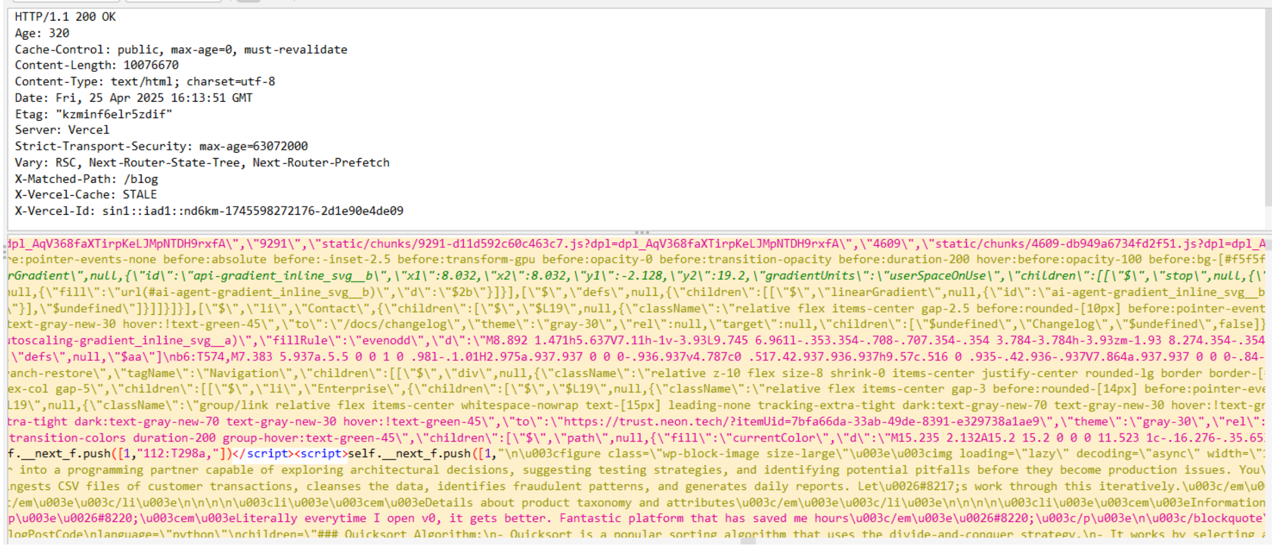
4. Step 03: Exploitation and Validation

Request:



```
GET https://neon.tech/blog HTTP/1.1
host: neon.tech
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
referer: https://neon.tech/
```

Response:



```
HTTP/1.1 200 OK
Age: 320
Cache-Control: public, max-age=0, must-revalidate
Content-Length: 10076670
Content-Type: text/html; charset=utf-8
Date: Fri, 25 Apr 2025 16:13:51 GMT
Etag: "kzminf6elr5zdif"
Server: Vercel
Strict-Transport-Security: max-age=63072000
Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch
X-Matched-Path: /blog
X-Vercel-Cache: STALE
X-Vercel-Id: sin1::iad1::nd6km-1745598272176-2d1e90e4de09
```

```
dpl_AqV368faXTirpKeLJMpNTDH9rxfA\",\"9291\",\"static/chunks/9291-d11d592c60c463c7.js?dpl=dpl_AqV368faXTirpKeLJMpNTDH9rxfA\",\"4609\",\"static/chunks/4609-db949a6734fd2f51.js?dpl=dpl_A
e:pointer-events-none before:absolute before:-inset-2.5 before:transform-gpu before:opacity-0 before:transition-opacity before:duration-200 hover:before:opacity-100 before:bg-[#f5f5f
rGradient\",null,{\"id\":\"api-gradient_inline_svg__b\",\"x1\":8.032,\"x2\":8.032,\"y1\":-2.128,\"y2\":19.2,\"gradientUnits\":\"userSpaceOnUse\",\"children\":[[\"$\",\"stop\",null,{\
ull,{\"fill\":\"url(#ai-agent-gradient_inline_svg__b)\",\"d\":\"$2b\"}]}],[\"$\",\"defs\",null,{\"children\":[[\"$\",\"linearGradient\",null,{\"id\":\"ai-agent-gradient_inline_svg__b
\"}],\"$undefined\"]}]]}]}],[\"$\",\"li\",\"Contact\",{\"children\":[\"$\",\"$L19\",null,{\"className\":\"relative flex items-center gap-2.5 before:rounded-[10px] before:pointer-event
text-gray-new-30 hover:!text-green-45\",\"to\":\"/docs/changelog\",\"theme\":\"gray-30\",\"rel\":null,\"target\":null,\"children\":[\"$undefined\",\"Changelog\",\"$undefined\",false]}
toscaling-gradient_inline_svg__a)\",\"fillRule\":\"evenodd\",\"d\":\"M8.892 1.471h5.637V7.11h-1v-3.93L9.745 6.961l-.353.354-.708-.707.354-.354 3.784-3.784h-3.93zm-1.93 8.274.354-.354
\"defs\",null,\"$aa\"]\nb6:T574,M7.383 5.937a.5.5 0 0 1 0 .981-.1.01H2.975a.937.937 0 0 0-.936.937v4.787c0 .517.42.937.936.937h9.57c.516 0 .935-.42.936-.937V7.864a.937.937 0 0 0-.84-
anch-restore\",\"tagName\":\"Navigation\",\"children\":[[\"$\",\"div\",null,{\"className\":\"relative z-10 flex size-8 shrink-0 items-center justify-center rounded-lg border border-[
ex-col gap-5\",\"children\":[[\"$\",\"li\",\"Enterprise\",{\"children\":[\"$\",\"$L19\",null,{\"className\":\"relative flex items-center gap-3 before:rounded-[14px] before:pointer-eve
L19\",null,{\"className\":\"group/link relative flex items-center whitespace-nowrap text-[15px] leading-none tracking-extra-tight dark:text-gray-new-70 text-gray-new-30 hover:!text-gr
tra-tight dark:text-gray-new-70 text-gray-new-30 hover:!text-green-45\",\"to\":\"https://trust.neon.tech/?itemUid=7bfa66da-33ab-49de-8391-e329738a1ae9\",\"theme\":\"gray-30\",\"rel\":
transition-colors duration-200 group-hover:text-green-45\",\"children\":[\"$\",\"path\",null,{\"fill\":\"currentColor\",\"d\":\"M15.235 2.132A15.2 15.2 0 0 0 11.523 1c-.16.276-.35.65
f.__next_f.push([1,"112:T298a,"])</script><script>self.__next_f.push([1,"\n\u003cfigure class=\"wp-block-image size-large\"\u003e\u003cimg loading=\"lazy\" decoding=\"async\" width=\"
 into a programming partner capable of exploring architectural decisions, suggesting testing strategies, and identifying potential pitfalls before they become production issues. You\
ngests CSV files of customer transactions, cleanses the data, identifies fraudulent patterns, and generates daily reports. Let\u0026#8217;s work through this iteratively.\u003c/em\u0
/em\u003e\u003c/li\u003e\n\n\n\n\u003cli\u003e\u003cem\u003eDetails about product taxonomy and attributes\u003c/em\u003e\u003c/li\u003e\n\n\n\n\u003cli\u003e\u003cem\u003eInformation
p\u003e\u0026#8220;\u003cem\u003eLiterally everytime I open v0, it gets better. Fantastic platform that has saved me hours\u003c/em\u003e\u0026#8220;\u003c/p\u003e\n\u003c/blockquote
logPostCode\nlanguage=\"python\"\nchildren=\"### Quicksort Algorithm:\n- Quicksort is a popular sorting algorithm that uses the divide-and-conquer strategy.\n- It works by selecting a
```

5. Step 04: Mitigation / Fix

Immediate Mitigation Actions:

1. Remove the hash from public access. – Check if the hash appears in HTML, API responses or logs and disable error messages I production.
2. Invalidate the exposed Hash – Force a password reset for the affected user.

Secure Coding Practices:

1. Never return password hashes in API/HTML responses
2. Use Data Transfer Objects (objects used to transfer data between different parts of a software application) to filter sensitive fields.

Long Term Prevention:

1. Automated Security Testing.
2. Educate the Team / Employees.