Active Recon & Web Enumeration

Objective: To Identify vulnerabilities using active recon

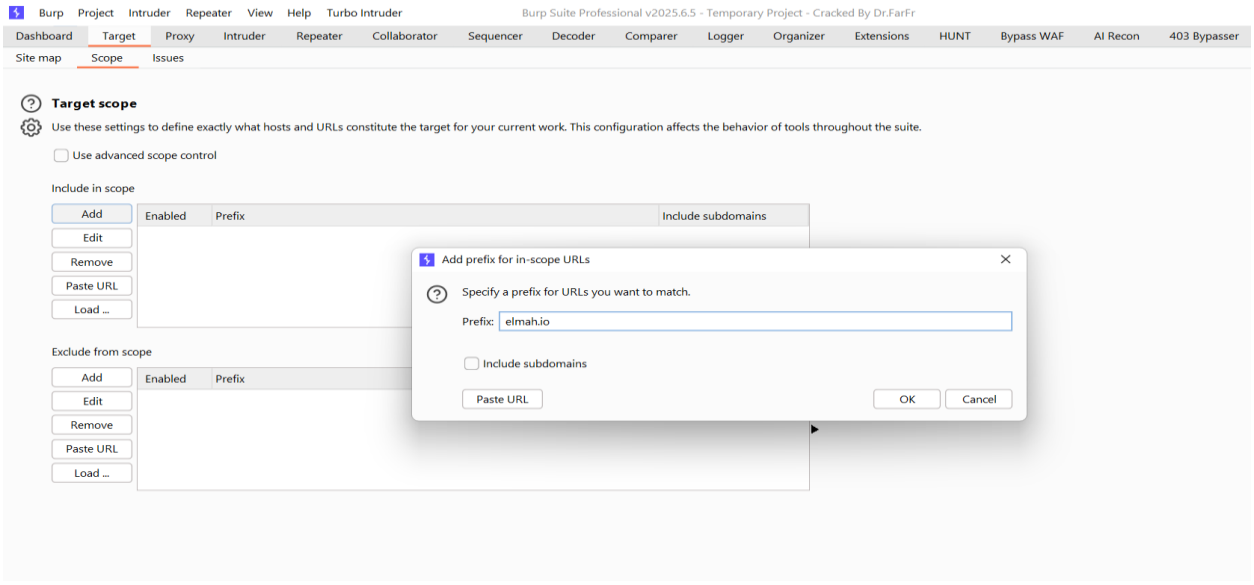
Target: elmah.io

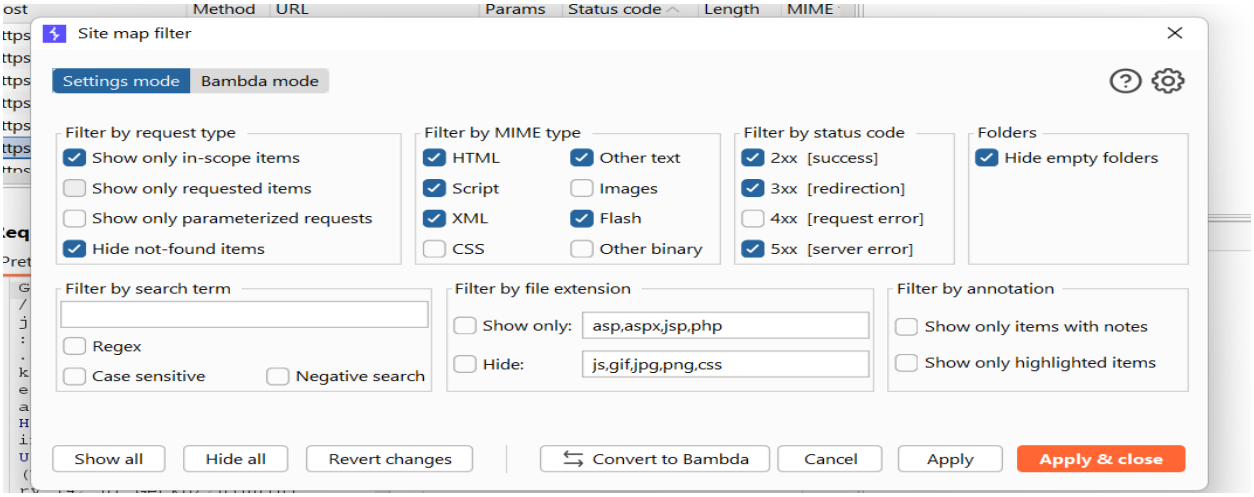
Scope: self-hosted bug bounty program

Submitted by: Prashant sengar

To: skill-horizon

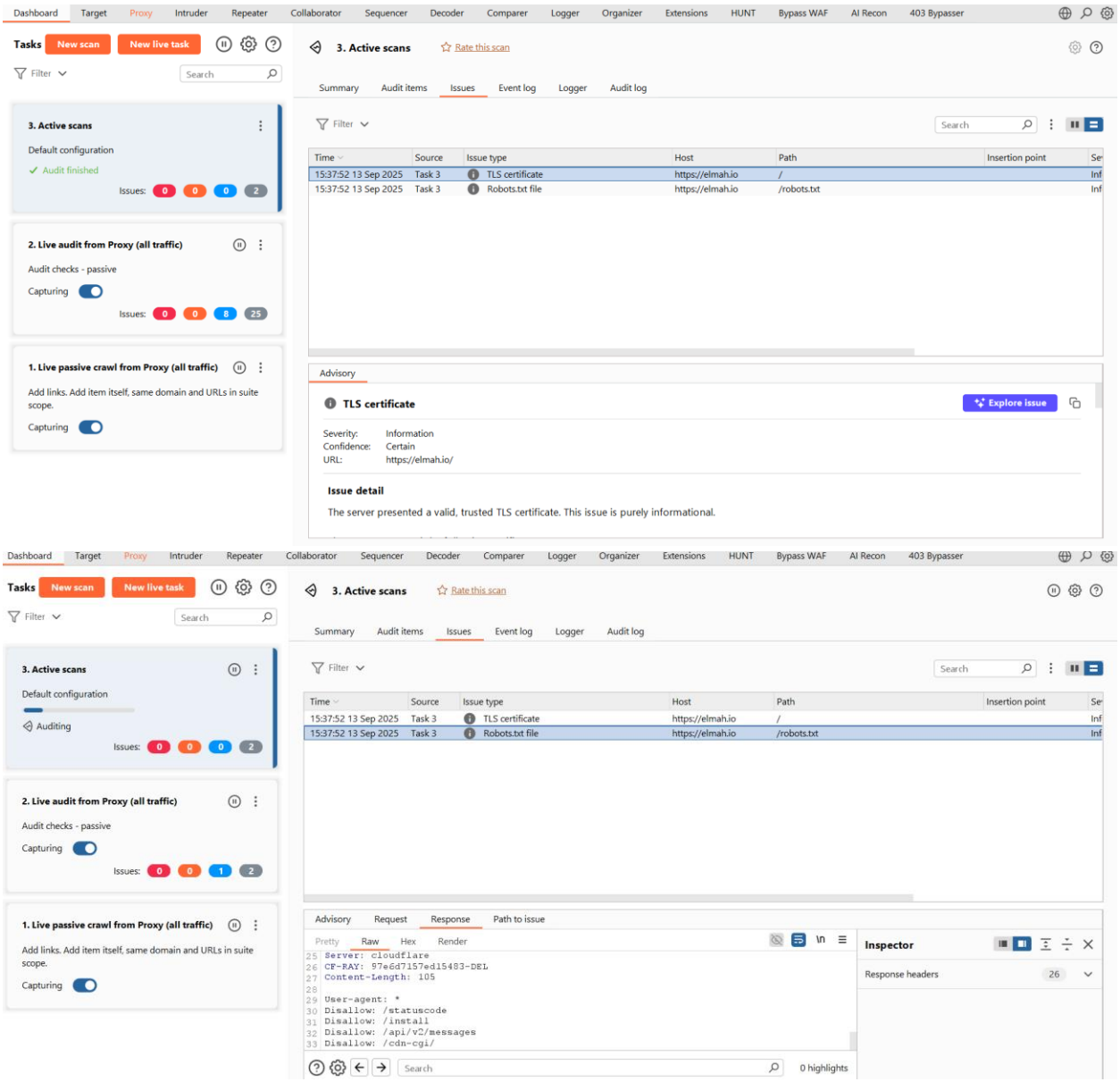
1. Defining Scope in Burp suite





:-FILTERING SCOPE SHOW ONLY ITEM IN SCOPE

:-Scanning target actively

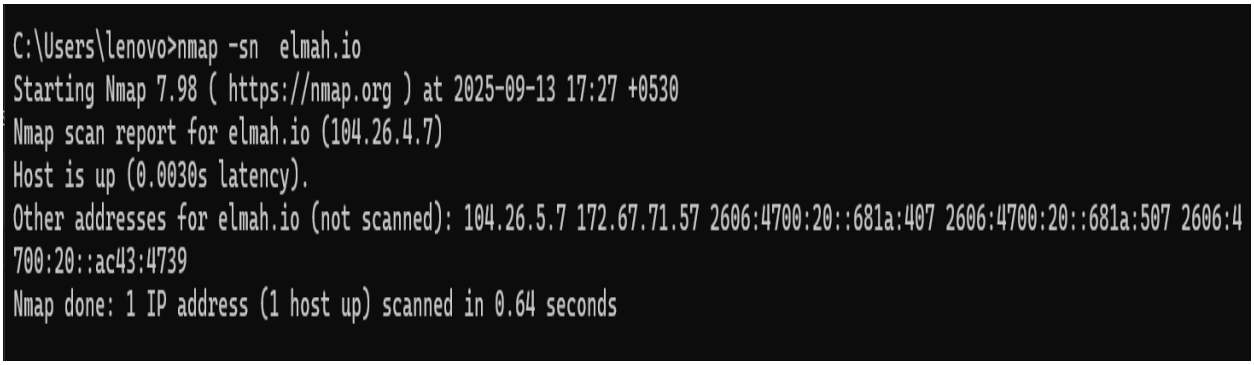


Findings:- didn't find any useful as is protected by cloud fare

2. Nmap findings

: -nmap is port scaning tool that is used to identify open ports and services that are running on ports and furthermore

: - Finding wheter the host is up or not using -sn



HOST IS UP

: - RUNNING TCP SCAN AND IDENTIFYING THE SERVICES AND RUNNING DEFAULT SCRIPT SCAN ON

```
PS C:\Users\lenovo> nmap -sS -sC -sV elmah.io
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-13 17:31 +0530
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.07% done; ETC: 17:32 (0:00:39 remaining)
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.33% done; ETC: 17:32 (0:00:38 remaining)
Nmap scan report for elmah.io (104.26.4.7)
Host is up (0.0048s latency).
Other addresses for elmah.io (not scanned): 172.67.71.57 104.26.5.7 2606:4700:20::681a:507 2606:4700:20::681a:407 2606:4700:20::ac43:4739
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
| dns-nsid:
|_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.10
80/tcp   open  http     Cloudflare http proxy
|_http-title: Did not follow redirect to https://elmah.io/
443/tcp  open  ssl/http Cloudflare http proxy
| ssl-cert: Subject: commonName=elmah.io
| Subject Alternative Name: DNS:elmah.io, DNS:*.elmah.io
| Not valid before: 2025-08-10T08:33:18
|_Not valid after:  2025-11-08T09:33:15
|_http-title: elmah.io - Error logging and Uptime monitoring for .NET
|_http-server-header: cloudflare
8080/tcp open  http     Cloudflare http proxy
|_http-title: Did not follow redirect to https://elmah.io:8080/
8443/tcp open  ssl/http Cloudflare http proxy
|_http-title: 400 The plain HTTP request was sent to HTTPS port
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.15 seconds
```

: - NSE-SCRIPT SCAN DEFAULT

```
PS C:\Users\lenovo> nmap --script=vuln elmah.io -T4
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-13 15:41 +0530
Nmap scan report for elmah.io (104.26.5.7)
Host is up (0.0042s latency).
Other addresses for elmah.io (not scanned): 172.67.71.57 104.26.4.7 2606:4700:20::681a:507 2606:4700:20::ac43:4739 2606:4700:20::681a:407
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp  open  https
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|_  /robots.txt: Robots file
8080/tcp open  http-proxy
8443/tcp open  https-alt
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
```

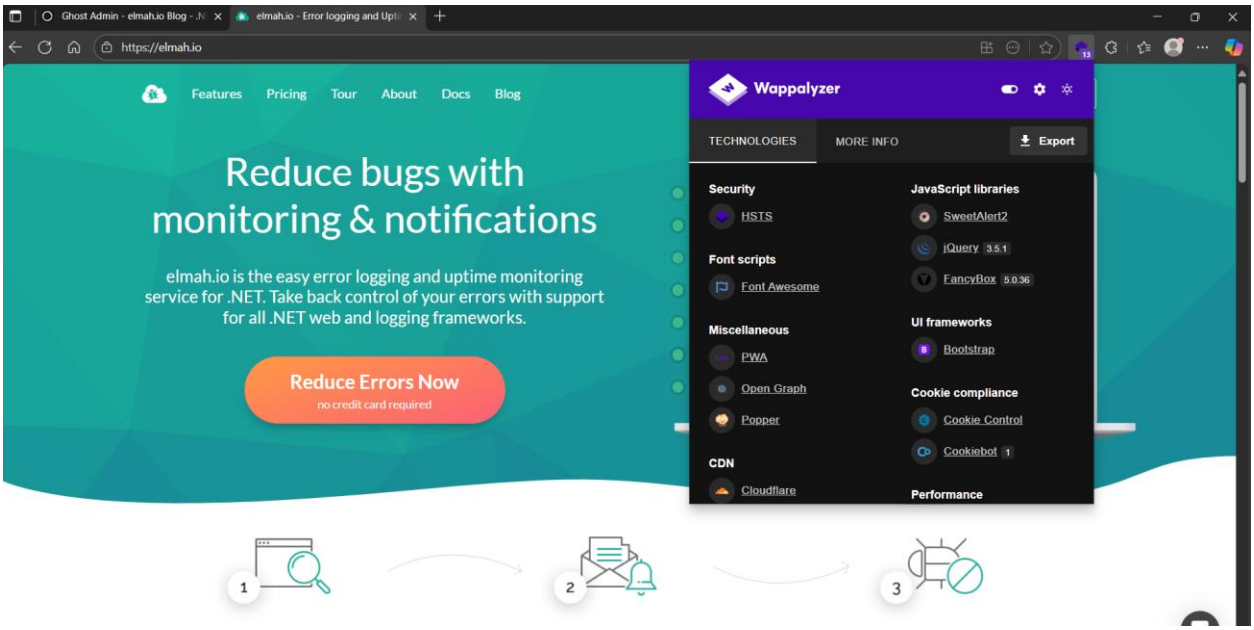
Didn't Find Any Vulnerabilities

Findings:- open port 80(http) ,port 51 domain

80,443,8080,8445 were open

Identifying web technologies

: - Using wappalyzer and whataweb




```
┌──(sengar㉿kali)-[~]
└─$ whatweb https://elmah.io/
https://elmah.io/ [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[cloudflare], IP[172.67.71.57], Open-Graph-Protocol[website][218008838347208], Script[text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[elmah.io - Error logging and Uptime monitoring for .NET], UncommonHeaders[report-to,x-content-type-options,referrer-policy,x-permitted-cross-domain-policies,permissions-policy,content-security-policy,cross-origin-resource-policy,cross-origin-opener-policy,cross-origin-embedder-policy,cf-cache-status,nel,cf-ray], X-Frame-Options[SAMEORIGIN]
```

USING NIKTO TO FIND WEB BASESD VUNREBILTY

```
┌──(sengar㉿kali)-[~]
└─$ nikto -h https://elmah.io/ -o output.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.26.4.7, 104.26.5.7, 172.67.71.57, 2606:4700:20::681a:507, 2606:4700:20::681a:407, 2606:4700:20::ac43:4739
+ Target IP:          104.26.4.7
+ Target Hostname:    elmah.io
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=elmah.io
                  Ciphers:  TLS_AES_256_GCM_SHA384
                  Issuer:   /C=US/O=Google Trust Services/CN=WE1
+ Start Time:         2025-09-13 15:54:13 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: Uncommon header 'cross-origin-embedder-policy' found, with contents: unsafe-none.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /api/v2/messages/: 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/
+ /robots.txt: contains 4 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/t
ls alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time:           2025-09-13 15:56:26 (GMT5.5) (133 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

CONTENT DISCOVERY

TOOLS USED: -

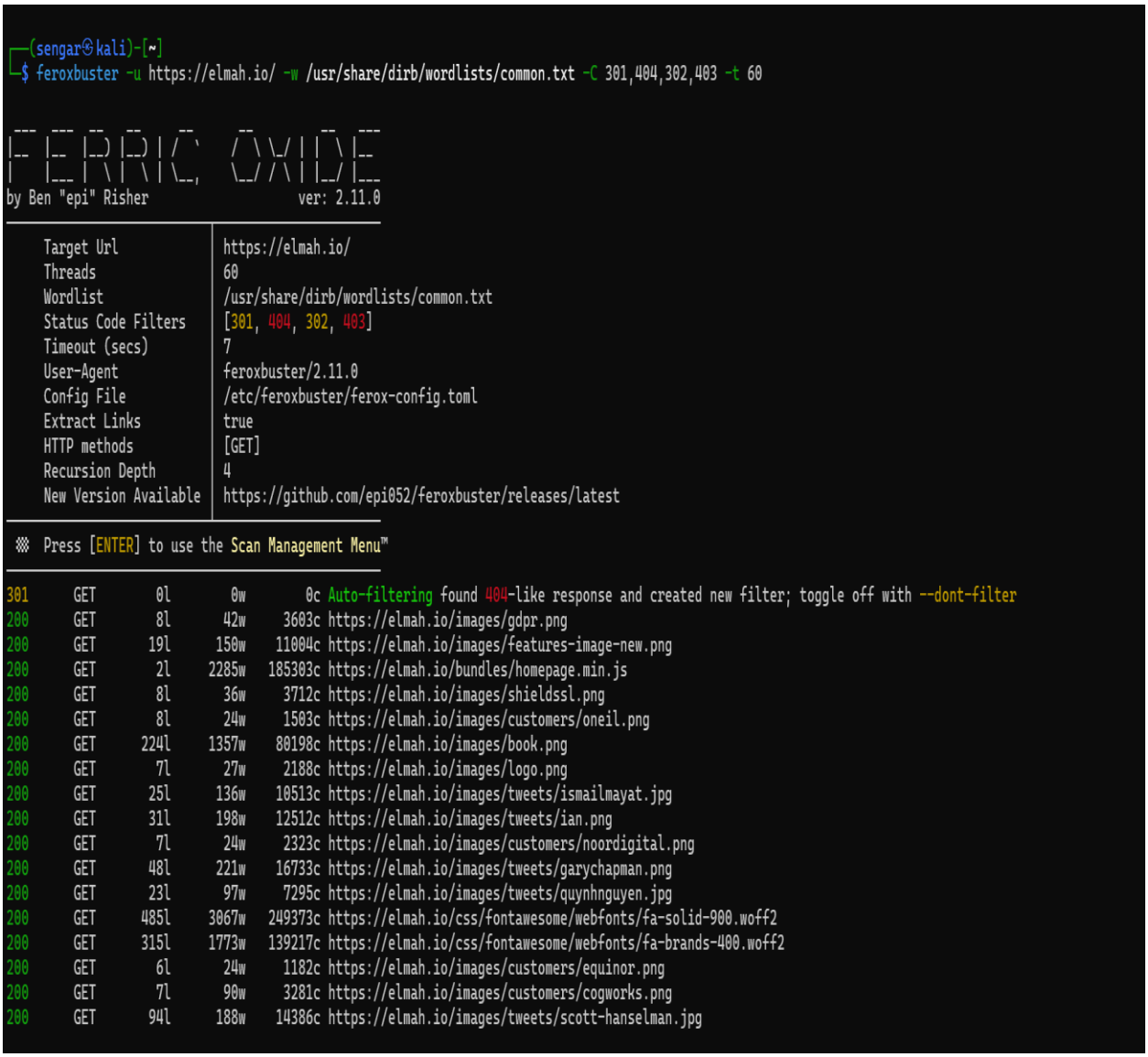
1.DIRB

2.DIRSEARCH

3.FEROXBUSTER

```
┌──(sengar㉿kali)-[~]
└─$ dirb  https://elmah.io -w /usr/share/dirb/wordlists/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Sep 13 16:02:28 2025
URL_BASE: https://elmah.io/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://elmah.io/ ----
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
    (Try using FineTunning: '-f')
+ https://elmah.io/.bash_history (CODE:301|SIZE:0)
+ https://elmah.io/.bashrc (CODE:301|SIZE:0)
+ https://elmah.io/.cache (CODE:301|SIZE:0)
+ https://elmah.io/.cvs (CODE:301|SIZE:0)
+ https://elmah.io/.cvsignore (CODE:301|SIZE:0)
+ https://elmah.io/.forward (CODE:301|SIZE:0)
+ https://elmah.io/.git/HEAD (CODE:301|SIZE:0)
+ https://elmah.io/.history (CODE:301|SIZE:0)
+ https://elmah.io/.hta (CODE:301|SIZE:0)
+ https://elmah.io/.htaccess (CODE:301|SIZE:0)
+ https://elmah.io/.htpasswd (CODE:301|SIZE:0)
+ https://elmah.io/.listing (CODE:301|SIZE:0)
+ https://elmah.io/.listings (CODE:301|SIZE:0)
+ https://elmah.io/.mysql_history (CODE:301|SIZE:0)
+ https://elmah.io/.passwd (CODE:301|SIZE:0)
+ https://elmah.io/.perf (CODE:301|SIZE:0)
+ https://elmah.io/.profile (CODE:301|SIZE:0)
+ https://elmah.io/.rhosts (CODE:301|SIZE:0)
+ https://elmah.io/.sh_history (CODE:301|SIZE:0)
+ https://elmah.io/.ssh (CODE:301|SIZE:0)
```

```
┌──(sengar㉿kali)-[~]
└─$ dirsearch -u https://elmah.io/ -w /usr/share/dirb/wordlists/common.txt -x 403,404,500
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 4613

Output File: /home/sengar/reports/https_elmah.io/__25-09-13_15-56-47.txt

Target: https://elmah.io/

[15:56:47] Starting:
[15:57:12] 200 -    9KB - /favicon.ico
[15:57:33] 200 -  105B  - /robots.txt

Task Completed
```



Findings: - didnt find any sensitive directory most the directory were 403 cloud fare blocking the request to access from client side