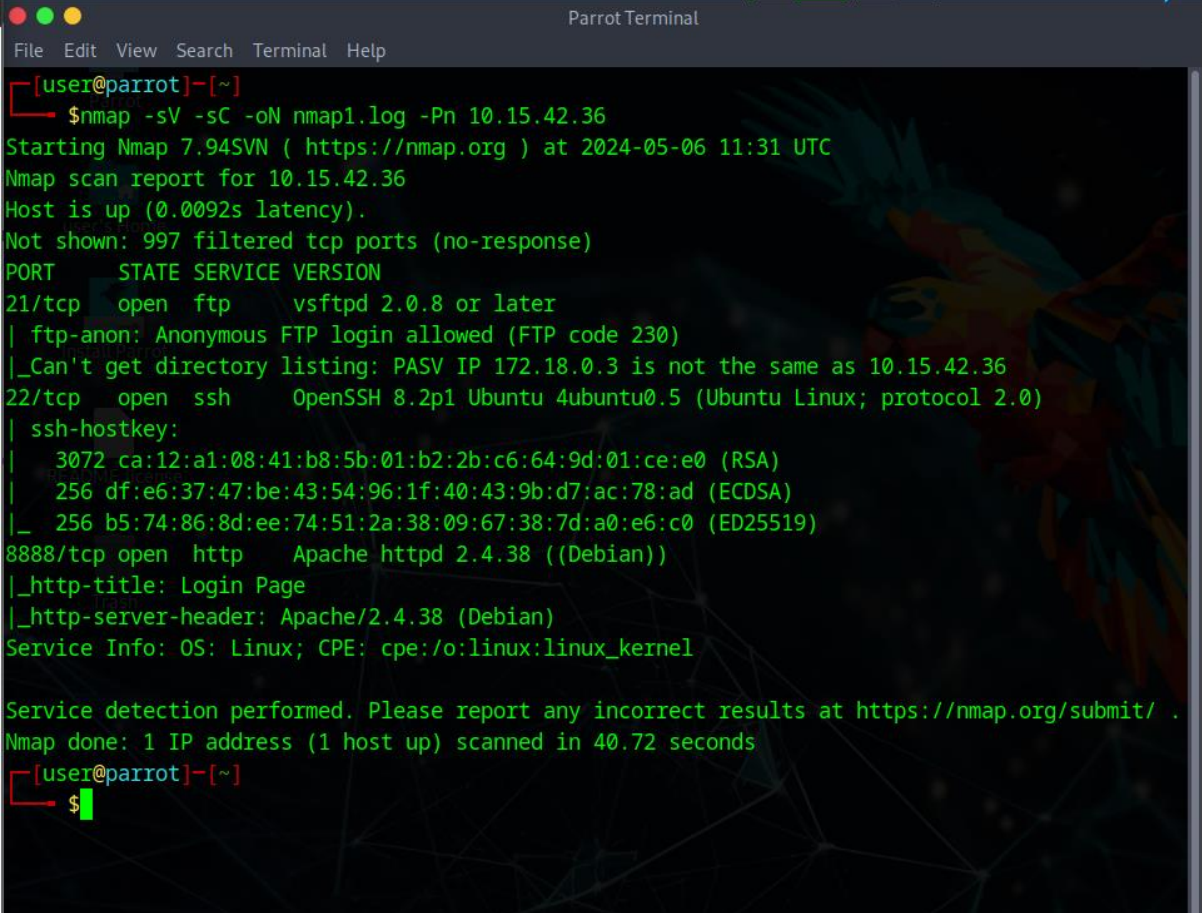


Bagian ip 10.15.42.36

1. Menjalankan nmap -sV -sC -oN nmap1.log -Pn 10.15.42.36 untuk mendapatkan informasi



```
[user@parrot]-[~]
$ nmap -sV -sC -oN nmap1.log -Pn 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 11:31 UTC
Nmap scan report for 10.15.42.36
Host is up (0.0092s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: PASV IP 172.18.0.3 is not the same as 10.15.42.36
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RSA)
|   256  df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
|_  256  b5:74:86:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25519)
8888/tcp  open  http     Apache httpd 2.4.38 ((Debian))
|_ http-title: Login Page
|_ http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.72 seconds
[user@parrot]-[~]
$
```

Dari sini kita mendapatkan :

- Server HTTP: Sistem target menjalankan server web Apache versi 2.4.38 pada Debian Linux. Informasi ini dapat membantu Anda meneliti kerentanan potensial yang spesifik untuk versi Apache tersebut.
- Sistem Operasi: Sistem target menjalankan beberapa versi Linux, seperti yang ditunjukkan oleh entri "OS: Linux" dan "CPE: cpe:/o:linux:linux_kernel". Distribusi Linux spesifik tidak diidentifikasi, tetapi informasi ini mempersempit pencarian Anda untuk kerentanan dan eksploitasi potensial.
- Aplikasi Web: Entri "http-title: halaman login" menunjukkan bahwa sistem target meng-host aplikasi web dengan halaman login. Ini bisa menjadi vektor serangan menarik jika Anda diizinkan untuk menguji kerentanan aplikasi web seperti injeksi SQL, cross-site scripting (XSS), atau cara melewati otentikasi.
- Server SSH: Sistem target memiliki server OpenSSH yang berjalan pada versi 8.2p1 pada Ubuntu 4ubuntu0.5. Informasi ini dapat membantu Anda meneliti kerentanan potensial pada versi OpenSSH tersebut, serta kerentanan yang spesifik untuk Ubuntu.

```

[~]-[user@parrot]-[~]
$ nmap -p 8888 -T1 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 11:57 UTC
Nmap scan report for 10.15.42.36
Host is up (1.8s latency).

PORT      STATE SERVICE
8888/tcp  open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 45.10 seconds

```

Dapat bahwa service dari port 8888 adalah sun-answerbook. Ini dapat dilihat pada **CVE: 2002-2425** terkait Sun AnswerBook2 1.x - Unauthorized Administrative Script Access

2. Mencoba mencari informasi terkait server dan dipatkankan http servernya merupakan apache 2.4.38 yang termask versi yang outdated dan ini

```

Parrot Terminal
File Edit View Search Terminal Help

[imamnurhadi@parrot]-[~]
$ nikto -host 10.15.42.36:8888
- Nikto v2.5.0

-----
+ Target IP:          10.15.42.36
+ Target Hostname:    10.15.42.36
+ Target Port:        8888
+ Start Time:         2024-05-07 04:41:32 (GMT-4)
-----
+ Server: Apache/2.4.38 (Debian)
+ /: Retrieved x-powered-by header: PHP/7.2.34.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/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 response in an unexpected fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misused-x-content-type-options-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the current version.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-icons/
+ 8102 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2024-05-07 04:45:59 (GMT-4) (267 seconds)
-----
+ 1 host(s) tested

[imamnurhadi@parrot]-[~]
$ nc -lsvp 10.15.42.36
nc: forward host lookup failed: Unknown host
[imamnurhadi@parrot]-[~]
$ nc -lsvp 10.15.42.36
nc: forward host lookup failed: Unknown host

```

Mencoba mencari kerentanan web server apache yang outdated

1. Dengan didapatkan kerentanan **CVE-2019-0211** dikarenakan versi web server apache yang outdated

2. Lalu didapatkan versi php 7.2.34 yang memiliki kerentanan berdasarkan [CVE-2020-7069](#), [CVE-2020-7070](#)
<https://www.tenable.com/plugins/was/112604>

3. Mencari web content pada http://10.15.42.36 :8888 untuk mencari file pada web server nya dengan hasil sebagai berikut

dirb http://10.15.42.36:8888 -X .php

DIRB v2.22

By The Dark Raver

START_TIME: Tue May 7 11:31:03 2024

URL_BASE: http://10.15.42.36:8888/

WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

GENERATED WORDS: 4612

---- Scanning URL: http://10.15.42.36:8888/ ----

+ http://10.15.42.36:8888/dashboard.php

(CODE:302|SIZE:0)

+ http://10.15.42.36:8888/index.php (CODE:200|SIZE:603)

END_TIME: Tue May 7 11:31:42 2024

DOWNLOADED: 4612 - FOUND: 2

```
$dirb http://10.15.42.36:8888
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Tue May  7 11:15:48 2024
URL_BASE: http://10.15.42.36:8888/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.15.42.36:8888/ ----
+ http://10.15.42.36:8888/index.php (CODE:200|SIZE:603)
+ http://10.15.42.36:8888/server-status (CODE:403|SIZE:278)
-----
END_TIME: Tue May  7 11:17:14 2024
```

```
By The Dark Raver http://10.15.42.36:8888/dashboard
Parrot OS Hack The Box OSINT Services Vuln DB

Not Found
START_TIME: Tue May  7 11:31:03 2024
URL_BASE: http://10.15.42.36:8888/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]
Apache/2.4.38 (Debian) Server at 10.15.42.36 Port 8888

-----

GENERATED WORDS: 4612

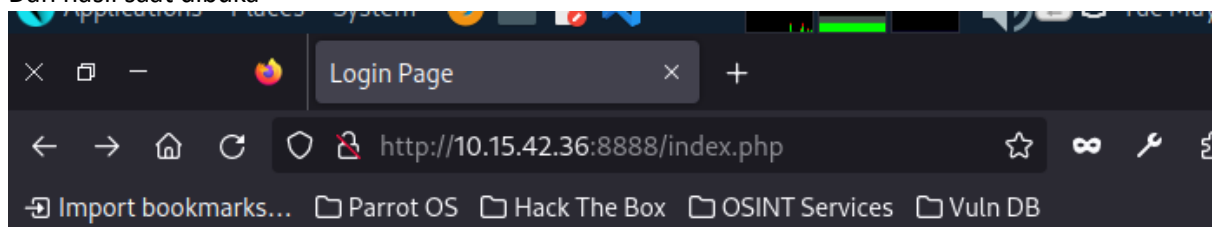
---- Scanning URL: http://10.15.42.36:8888/ ----

+ http://10.15.42.36:8888/dashboard.php (CODE:302|SIZE:0)
+ http://10.15.42.36:8888/index.php (CODE:200|SIZE:603)

-----

END_TIME: Tue May  7 11:31:42 2024
DOWNLOADED: 4612 - FOUND: 2
```

Dan hasil saat dibuka



Login

Username:

Password:

Login

dan tidak ditemukan shell.php

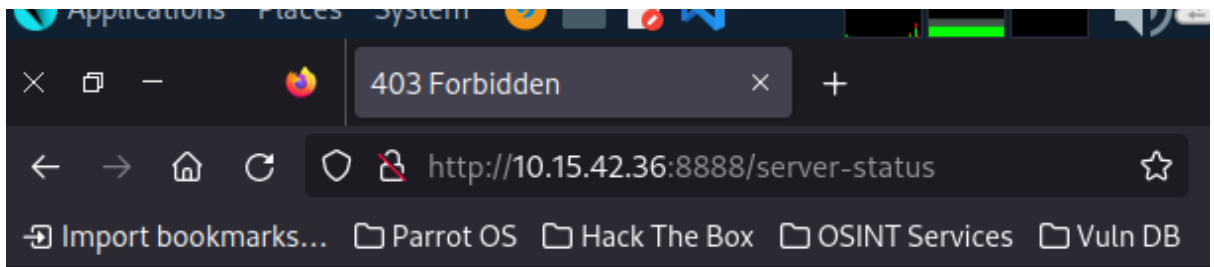
```

[imamnurhadi@parrot]~[~]tps://nmap.org ) at 2024-05-07 11:28 EDT
$dirb http://10.15.42.36:8888a-Xyshell:phplocking our ping probes, t
y -Pn
-----P--address (0 hosts up) scanned in 3.28 seconds
DIRBv2.22hadi@parrot]~[~]
By The Dark Raver 15.42.36
-----ing-----7-94SVN ( https://nmap.org ) at 2024-05-07 11:28 EDT
nmap scan report for 10.15.42.36
START_TIME: (Tue May 7 11:49:01 2024
URL_BASE: http://10.15.42.36:8888/(no-response)
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (shell.php) | (shell.php) [NUM = 1]
12/tcp open ssh
-----n-answerbook

nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
GENERATED WORDS: 4612]~[~]
→ $nc -lvnp 8888
-i-eScanning URL: http://10.15.42.36:8888/ ----
C
-[*]-[imamnurhadi@parrot]~[~]
→ $nc -lvnp 4242
-i-eing-----[---] 4242 ...
END_TIME: Tue May 7 11:49:39 2024
[-] Handler failed to bind to 10.15.42.36:8888:- -
[*] Started reverse TCP handler on 0.0.0.0:8888
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> Interr
upt: use the 'exit' command to quit
[msf](Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> █

```

sehingga tidak bisa dilakukan reverse shell exploit



Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at 10.15.42.36 Port 8888

4. Mengetahui versi php yang digunakan pada webserver ip 10.15.42.36

```
[imamnurhadi@parrot]~$ nmap -p 80,443 --script=http-php-version 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 11:59 EDT
Nmap scan report for 10.15.42.36
Host is up (0.0000s latency)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   filtered https
listening on [any] 8888 ...
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 3.20 seconds
```

dengan versi 10.1

5. Mencoba masuk ke ftp port 21

```
[imamnurhadi@parrot]~$ nmap -p 21 10.15.42.36
Nmap scan report for 10.15.42.36
host up) scanned in 136.52 seconds
$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server begins with '-'. Try '-oN ./-Pn' if you really want it to
Name (10.15.42.36:imamnurhadi): login
530 This FTP server is anonymous only.
ftp: Login failed.
ftp> exit
221 Goodbye.
[imamnurhadi@parrot]~$ nmap -p 21 10.15.42.36
Nmap scan report for 10.15.42.36
host up) scanned in 172.17 seconds
$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server filtered tcp ports (no-response), 10 filtered tcp ports (f
Name (10.15.42.36:imamnurhadi): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Dengan menjalankan ftp dan mencoba mendapatkan salah satu filenya yaitu backup.sql


```

230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files. report any incorrect results at https://nmap.org/submit/.
ftp> ls org/submit/
229 Entering Extended Passive Mode (|||65503|) 136.52 seconds
150 Here comes the directory listing.
-rwxrwxr-x -sC1 ftp -Pn 1ftp5.42.7 1997 May 04 15:40 backup.sql
226 Directory send OK. with '-'. Try '-oN ./-Pn' if you really want it to
ftp> put backup.sql
local: backup.sql remote: backup.sql
ftp: Can't open backup.sql: No such file or directory
ftp> cd ftp-sCV -Pn 10.15.42.7
550 Failed to change directory! (/nmap.org ) at 2024-05-07 12:20 EDT
ftp> tree report for 10.15.42.7
?Invalid command? (s latency).
ftp> get backup.sql
rts on 10.15.42.7 are in ignored states.
local: backup.sql remote: backup.sql b-response), 10 filtered tcp ports (ho
229 Entering Extended Passive Mode (|||65512|)
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% |*****|re1997 any 1173.64 KiB/sults00:00ETA
226 Transfer complete.
1997 bytes received in 00:00 (108.85 KiB/s) in 172.17 seconds
ftp> exit rhadi@parrot]~[~]
221 Goodbye

```

Dan melakukan untuk menunjukkan isi dari backup.sql

Desktop Downloads Music Pictures Templates

```

[imamnurhadi@parrot]~$ cat backup.sql
Service detected. Please report any incorrect results at https://nmap.org
-- MySQL dump 10.13 Distrib 8.0.36, for Linux (x86_64)
-- map done: 1 IP address (1 host up) scanned in 136.52 seconds
-- Host: localhost Database: db
-- Server version: 8.0.36-0ubuntu0.22.04.1
-- Table structure for table `users` scanned in 172.17 seconds
DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int NOT NULL,0) exploit(multi/http/php_cgi_arg_injection) >> Interrupt: use th
  `username` varchar(255) DEFAULT NULL;tp/php_cgi_arg_injection) >>

```

```

DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client      = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int NOT NULL,
  `username` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`id`),
  ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;
-- Dumping data for table `users`
-- Dump scan report for 10.15.42.7
Host is up (0.029s latency).
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmYscv9UyfuRDleF8ML0tjn.Ft51UKwTWiavJOJhM56d0K');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
-- Dump completed on 2024-05-01 19:49:02

```

Bagian ip 10.42.7

1. Mencari data yang bisa didapatkan dengan nmap -sCV -Pn 10.15.42.7 dengan hasil sebagai berikut Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-05-08 11:50 EDT

Nmap scan report for 10.15.42.7

Host is up (0.0076s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 9a:ed:52:a9:08:9d:71:6f:d1:24:8f:0b:4a:5b:7a:42 (RSA)

| 256 00:9c:a8:13:91:9f:4f:74:fb:9e:15:a2:36:6b:c5:ba (ECDSA)

|_ 256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:37 (ED25519)

80/tcp open http Apache httpd 2.4.59 ((Debian))

| http-robots.txt: 1 disallowed entry

|_ /wp-admin/

|_http-title: Hello World

|_http-generator: WordPress 6.5.2

|_http-server-header: Apache/2.4.59 (Debian)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
File Edit View Search Terminal Help
└─$ nmap -sCV -Pn 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 12:34 EDT
Nmap scan report for 10.15.42.7
Host is up (0.0080s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 9a:ed:52:a9:08:9d:71:6f:d1:24:8f:0b:4a:5b:7a:42 (RSA)
|_ 256 00:9c:a8:13:91:9f:4f:74:fb:9e:15:a2:36:6b:c5:ba (ECDSA)
|_ 256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:37 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds
└─[imamnurhadi@parrot]-[~]
```

```
└─$ nmap -sV -sC -oN nmap1.log -Pn 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 11:44 EDT
Nmap scan report for 10.15.42.7
Host is up (0.0087s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 9a:ed:52:a9:08:9d:71:6f:d1:24:8f:0b:4a:5b:7a:42 (RSA)
|_ 256 00:9c:a8:13:91:9f:4f:74:fb:9e:15:a2:36:6b:c5:ba (ECDSA)
|_ 256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:37 (ED25519)
80/tcp    open  http     Apache httpd 2.4.59 ((Debian))
|_ _http-title: Hello World
|_ http-robots.txt: 1 disallowed entry
|_ _/wp-admin/
|_ _http-server-header: Apache/2.4.59 (Debian)
|_ _http-generator: WordPress 6.5.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 23.73 seconds
└─[imamnurhadi@parrot]-[~/thunor-403]
```

Didapatkan informasi versi 2.4.59 web server Apache dan menggunakan wordpress versi 6.5.2

Yang bisa dikatakan termasuk dari informasi pada

1. **moderate: Apache HTTP Server: HTTP response splitting ([CVE-2023-38709](#)) ->**

https://httpd.apache.org/security/vulnerabilities_24.html

2. WordPress Core < 6.5.2 - Unauthenticated & Authenticated (Contributor+) Stored Cross-Site Scripting via Avatar Block [CVE-2024-4439](#)

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-core/wordpress-core-652-authenticated-contributor-stored-cross-site-scripting-via-avatar-block?asset_slug=wordpress

2.