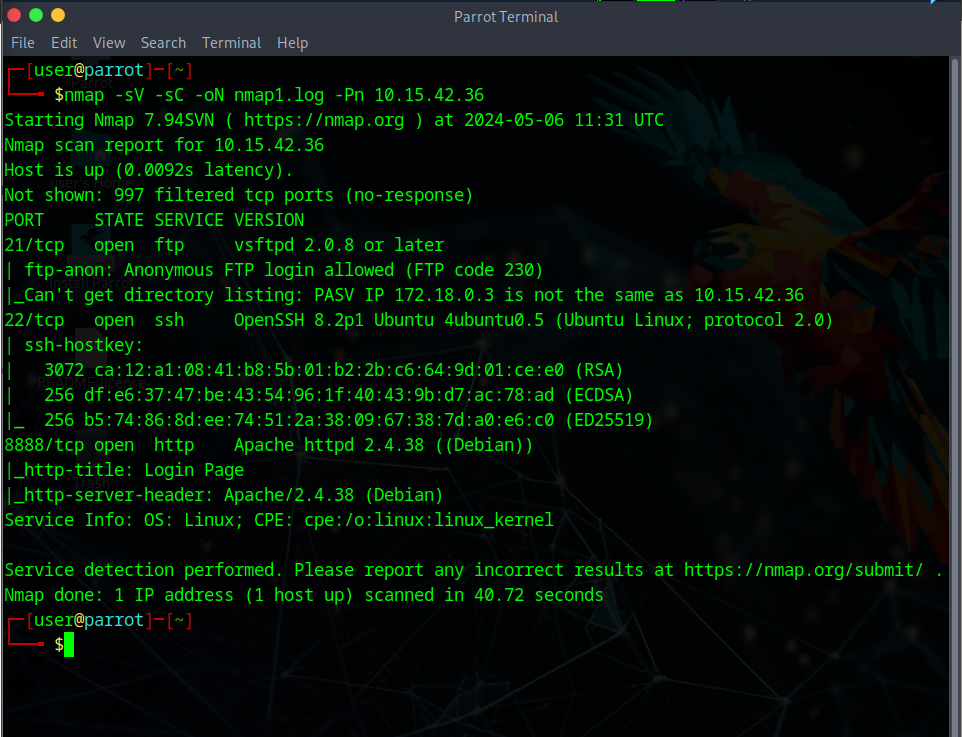
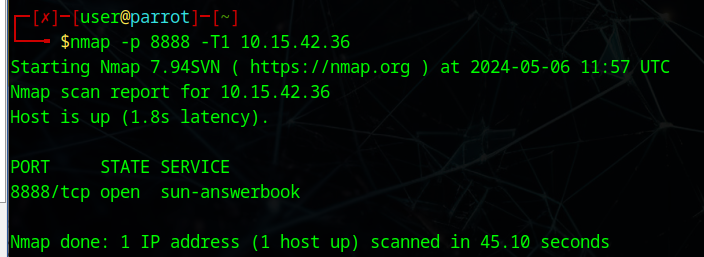
Bagian ip 10.15.42.36

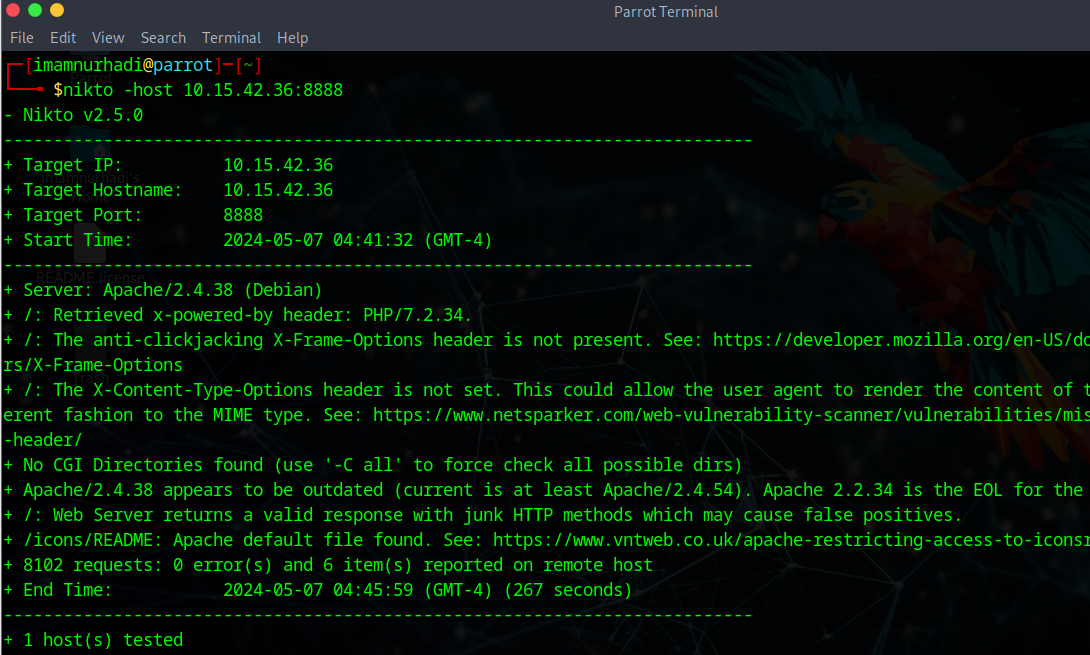
1. Menjalankan nmap -sV -sC -oN nmap1.log -Pn 10.15.42.36 untuk mendapatkan informasi 

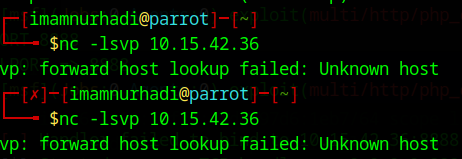
Dari sini kita mendapatkan :

* 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.

Dapat bahwa service dari port 8888 adalah sun-answerbook. Ini dapat dilihat pada **CVE:**

[2002-2425](https://nvd.nist.gov/vuln/detail/CVE-2002-2425) terkait Sun AnswerBook2 1.x - Unauthorized Administrative Script Access

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Mencoba mencari informasi terkait server dan dipatkankan http servernya merupakan apache 2.4.38 yang termask versi yang outdated dan ini 



Mencoba mencari kerentanan web server apache yang outdated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 Dengan didapatkan kerentanan **CVE-2019-0211** dikarenakan versi web server apache yang outdated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](https://www.tenable.com/cve/CVE-2020-7069), [CVE-2020-7070](https://www.tenable.com/cve/CVE-2020-7070)

**https://www.tenable.com/plugins/was/112604**

1. 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

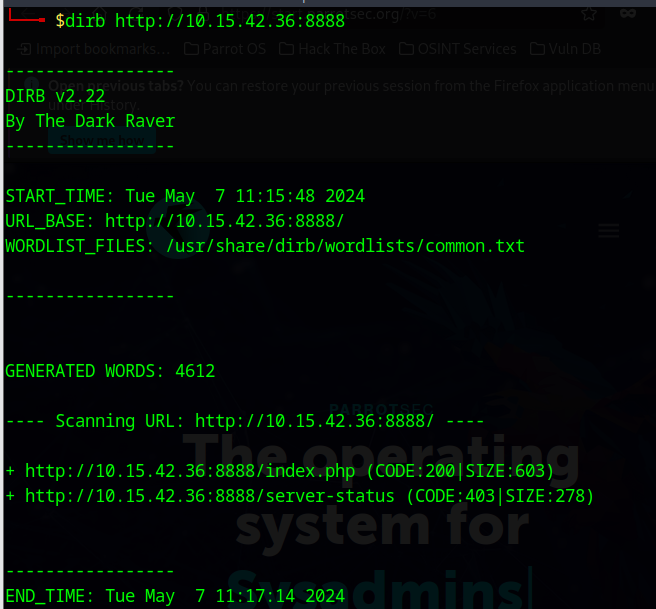
---- Scanning URL: http://10.15.42.36:8888/ ----

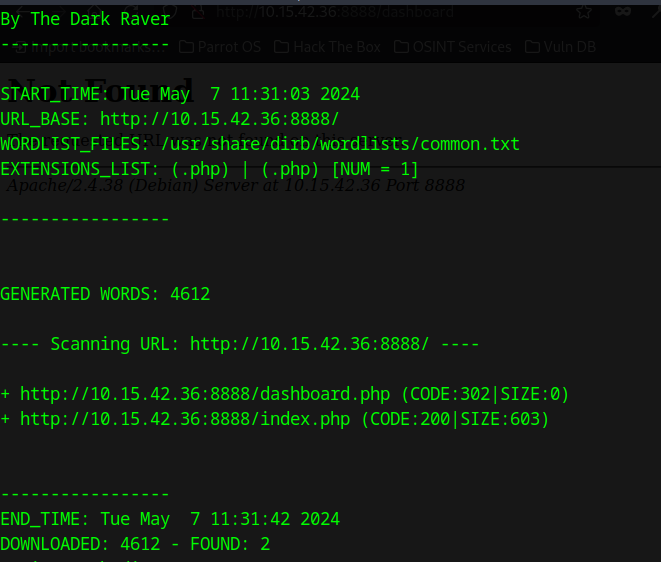
+ http://10.15.42.36:8888/dashboard.php (CODE:302|SIZE:0)

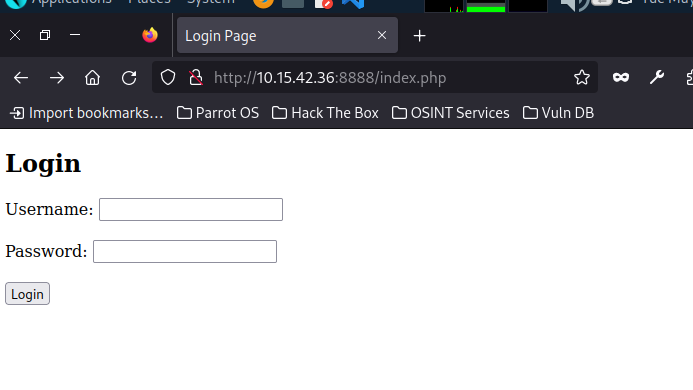
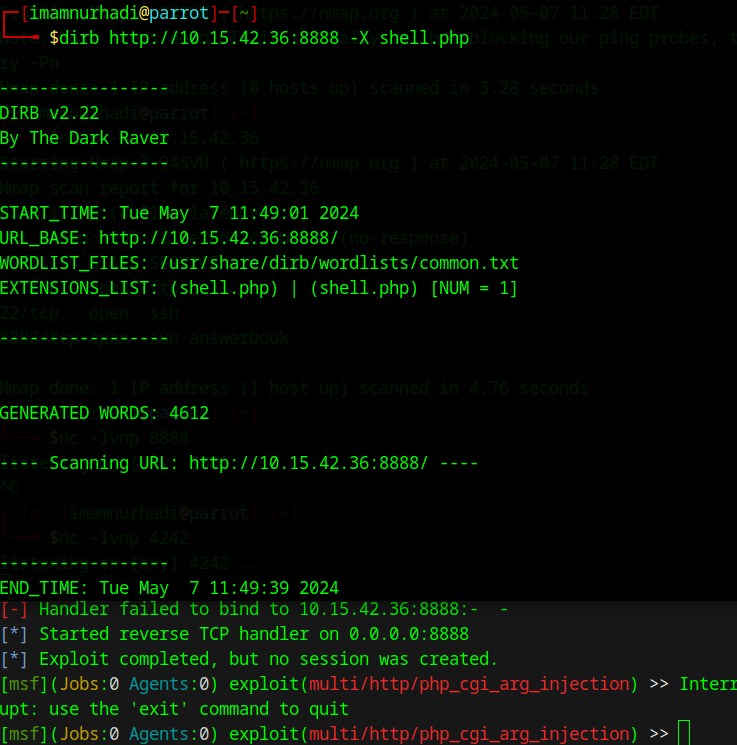
+ http://10.15.42.36:8888/index.php (CODE:200|SIZE:603)

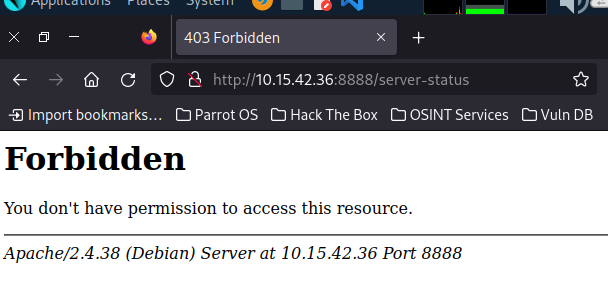
-----------------

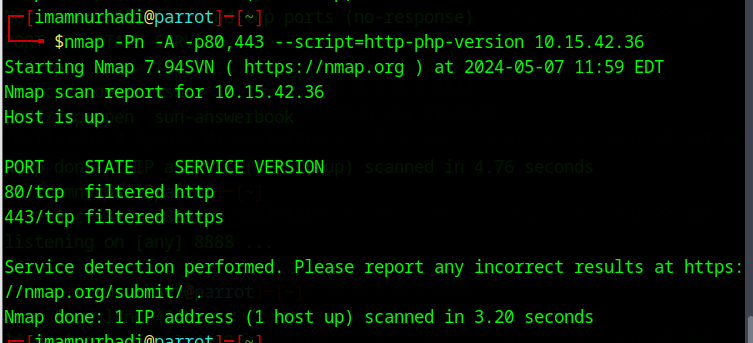
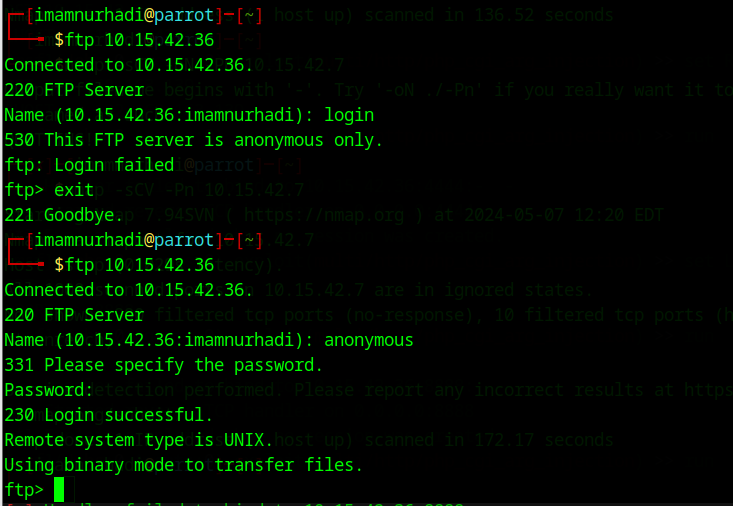
END\_TIME: Tue May 7 11:31:42 2024

DOWNLOADED: 4612 - FOUND: 2

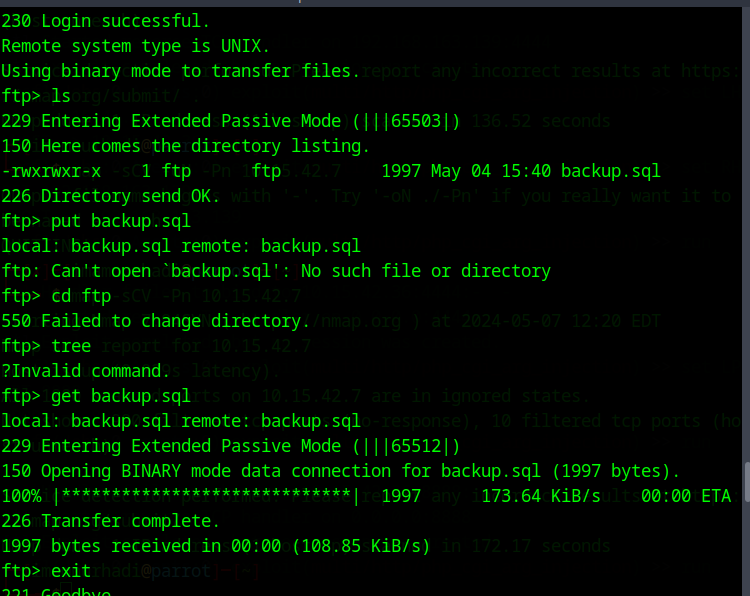


Dan hasil saat dibuka dan tidak ditemukan shell.php sehingga tidak bisa dilakukan reverse shell exploit

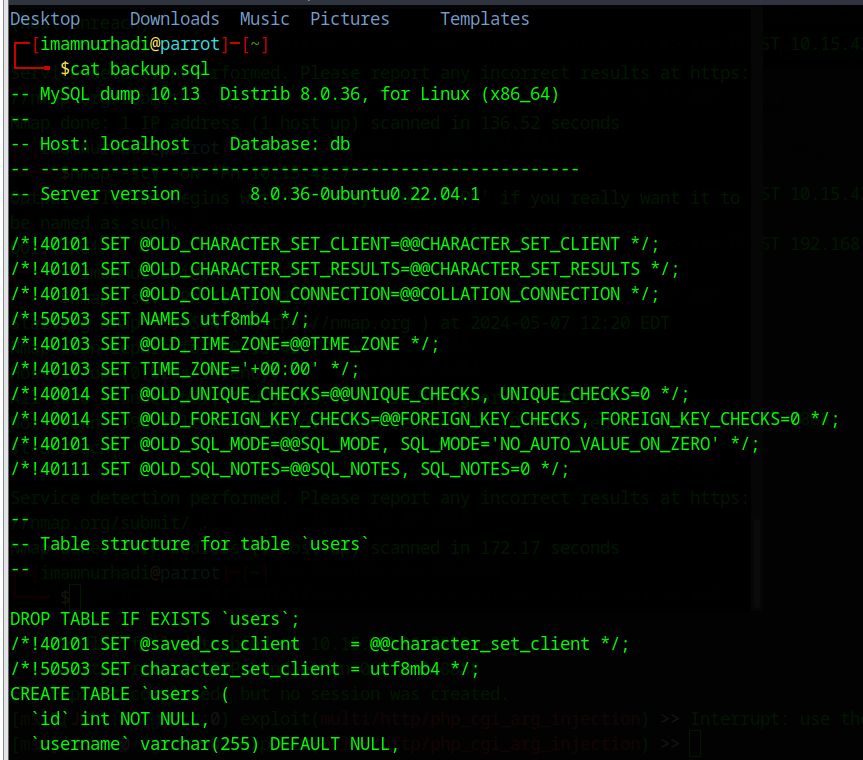


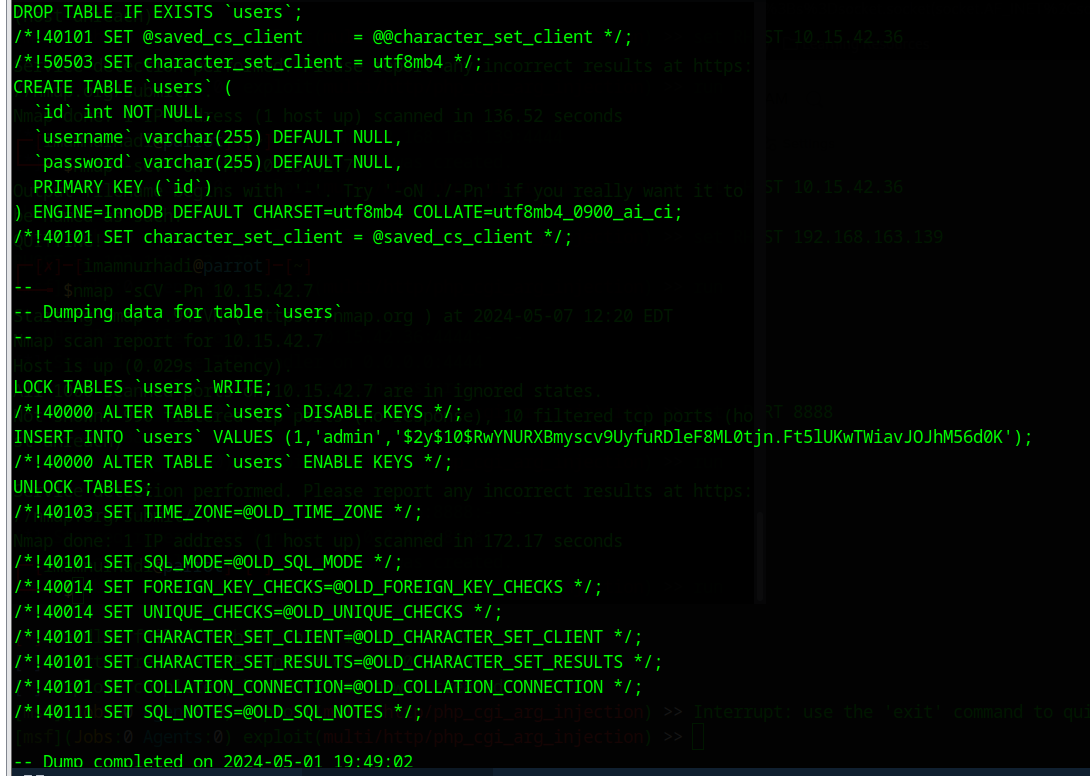
1. Mengetahui versi php yang digunakan pada webserver ip p10.15.42.36 dengan versi 10.1
2. Mencoba masuk ke ftp port 21 

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



Dan melakukan untuk menunjukkan isi dari backup.sql





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

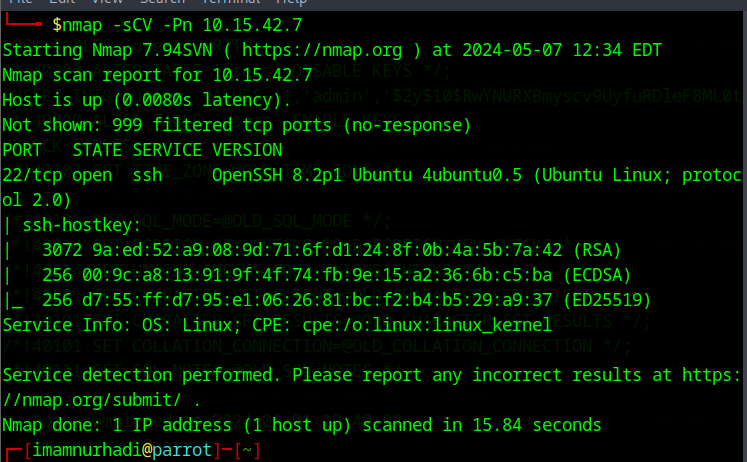
|\_/wp-admin/

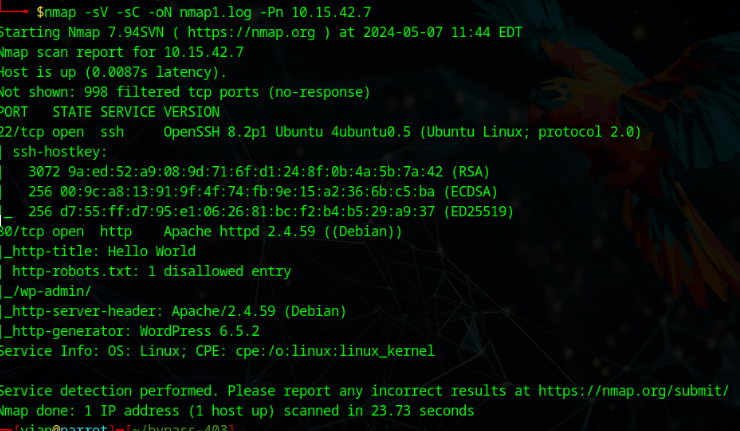
|\_http-title: Hello World

|\_http-generator: WordPress 6.5.2

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

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel





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://www.cve.org/CVERecord?id=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.cve.org/CVERecord?id=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