Write Up Kediri Cyber Security Competition 2024

Nama Tim - Asal Sekolah

Nama Peserta 1
Nama Peserta 2

Daftar Isi

[Web]

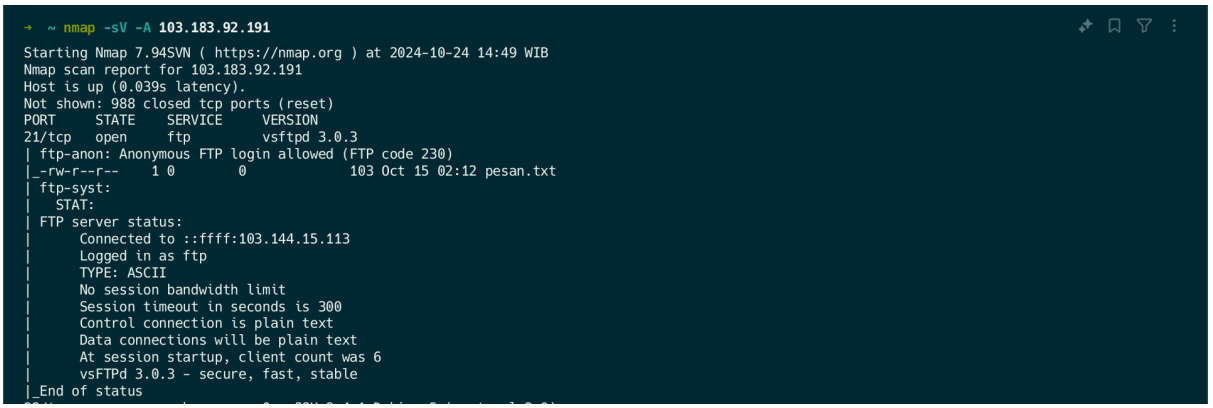
Encode

Screenshoot Soal

Solution

- **Penjelasan proses analisa**
- **Penjelasan proses exploitasi**

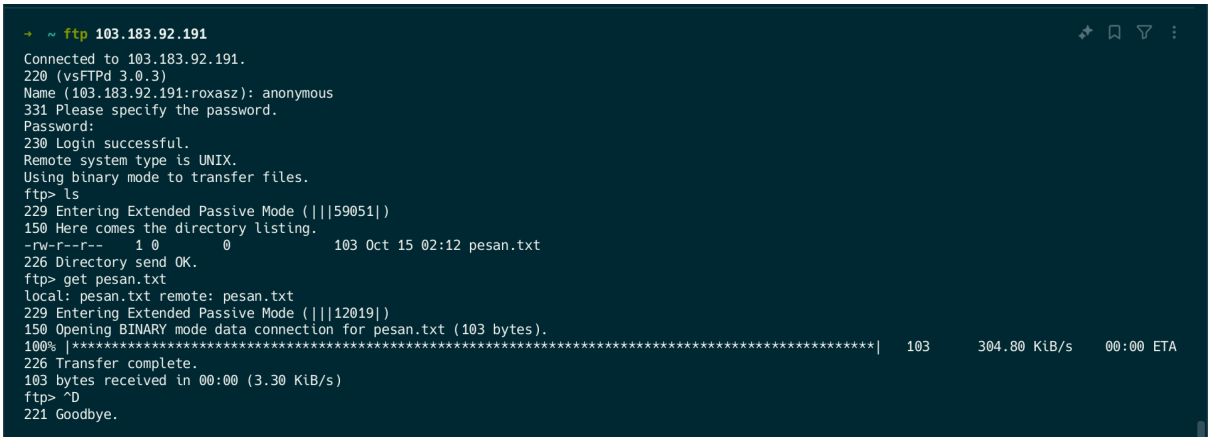
Scan semua port menggunakan nmap



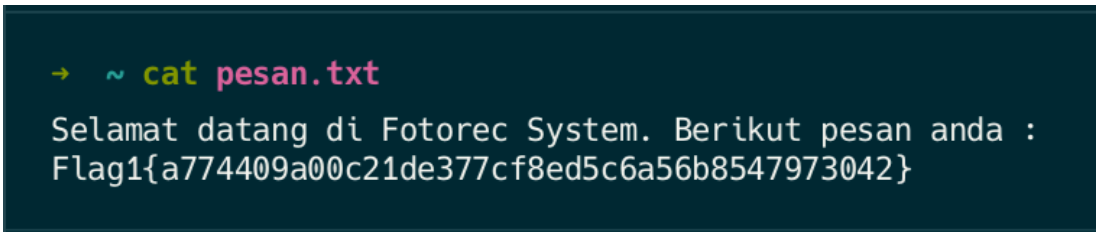
```
→  ~ nmap -sV -A 103.183.92.191
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 14:49 WIB
Nmap scan report for 103.183.92.191
Host is up (0.039s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             103 Oct 15 02:12 pesan.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:103.144.15.113
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 6
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```

ternyata dari hasil scan tersebut, ftp bisa menggunakan user anonymous dan password untuk

anonymous adalah “anonymous”.



setelah itu, ternyata terdapat file bernama pesan.txt, dan ternyata isi file tersebut flagnya, menggunakan command get untuk transfer file dari ftp server ke local.
ref : wikipedia

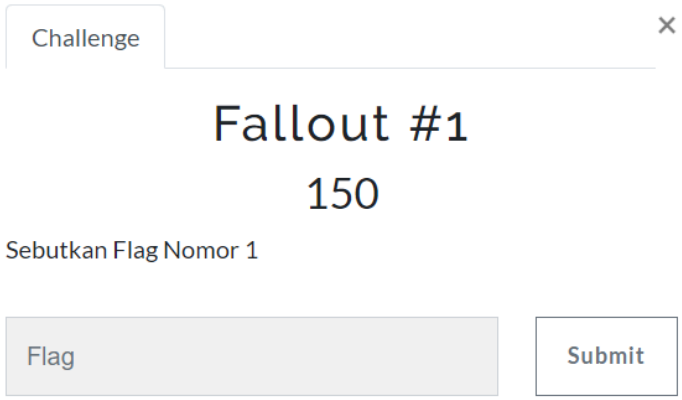


Flag: a774409a00c21de377cf8ed5c6a56b8547973042

[Reverse]

Judul Soal

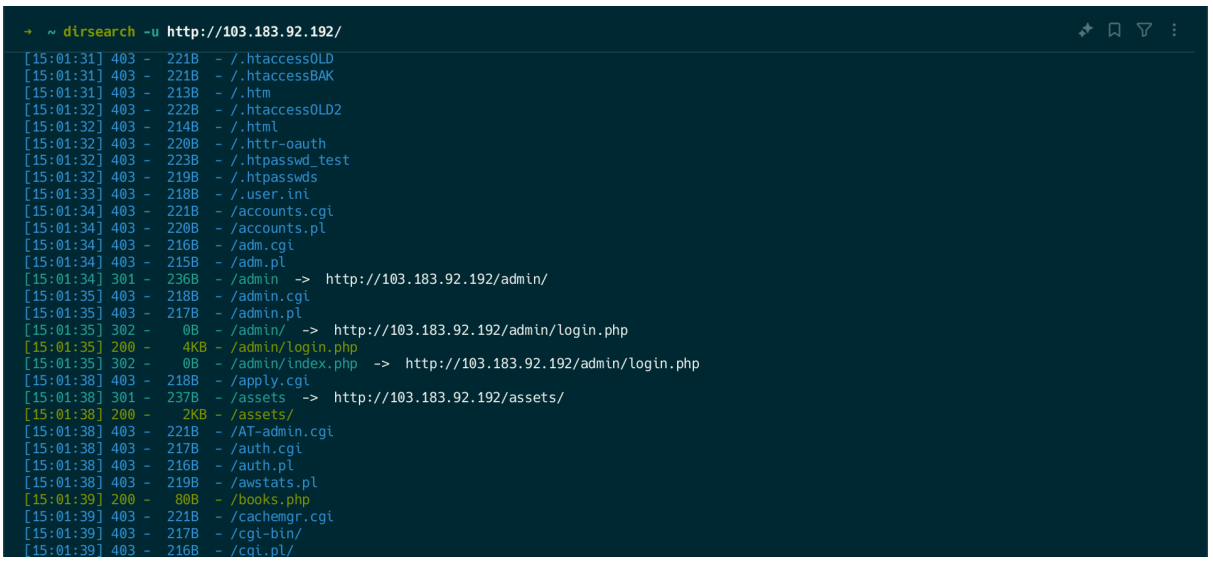
Screenshot



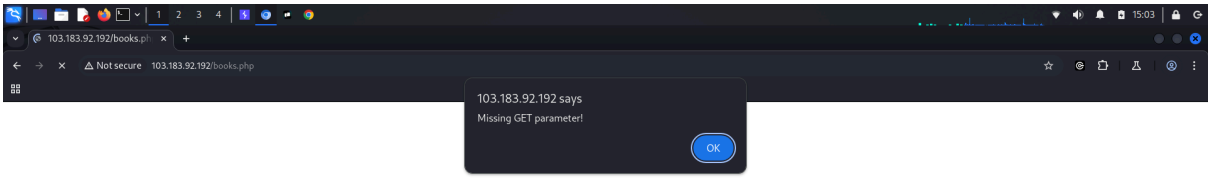
Solution

- **Penjelasan proses analisa**
- **Penjelasan proses exploitas**

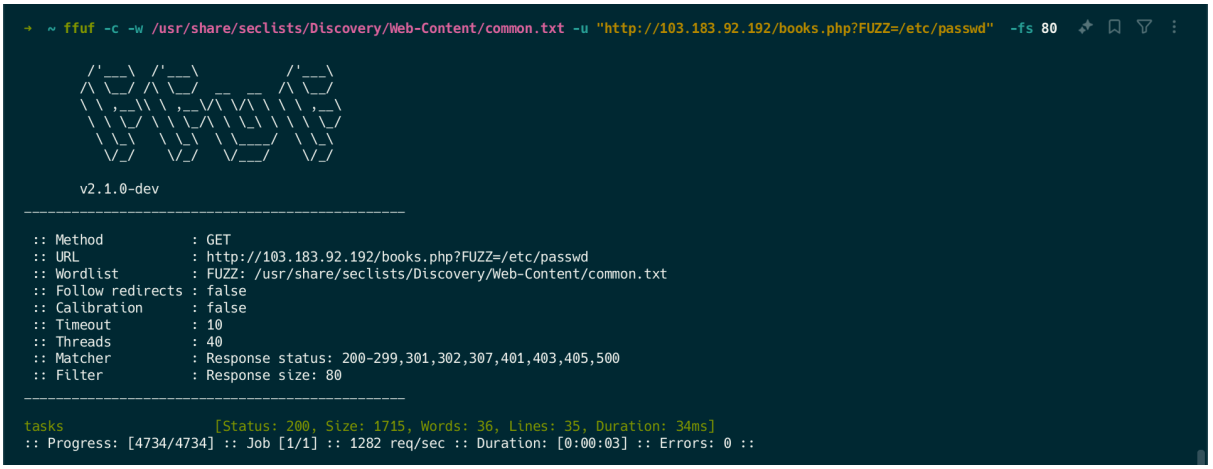
menggunakan dirsearch untuk mendapatkan url yang tidak muncul di halaman page.



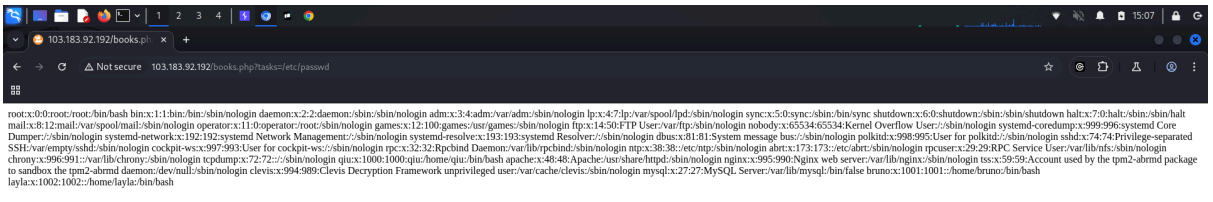
terlihat disana ternyata ada books.php



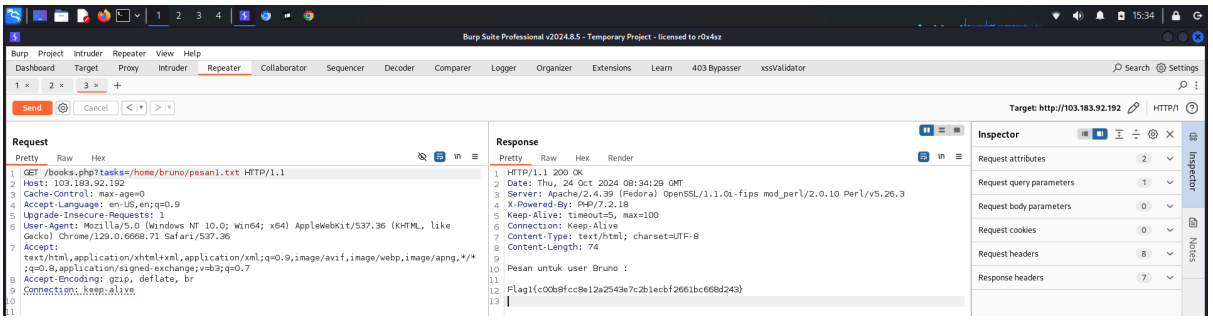
ternyata butuh param, mari kita brute paramnya apa aja yang dipakai menggunakan ffuf

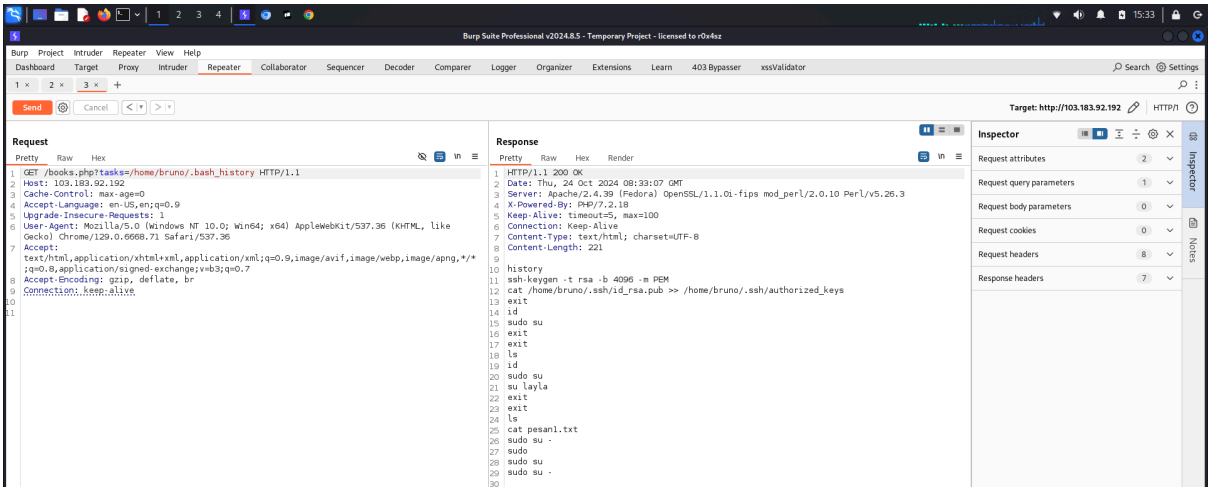


ternyata dari fuzzing tersebut kita dapatkan param tasks langsung saja kita dapatkan /etc/passwdnya.



karena sama seperti vulnhub jadi tinggal ke dir /home/bruno/.bash_history untuk melihat apa aja sih yang user bruno lakukan, lalu ternyata





flag ada di /home/bruno/pesan1.txt

Flag: KCSC{text}

Terimakasih