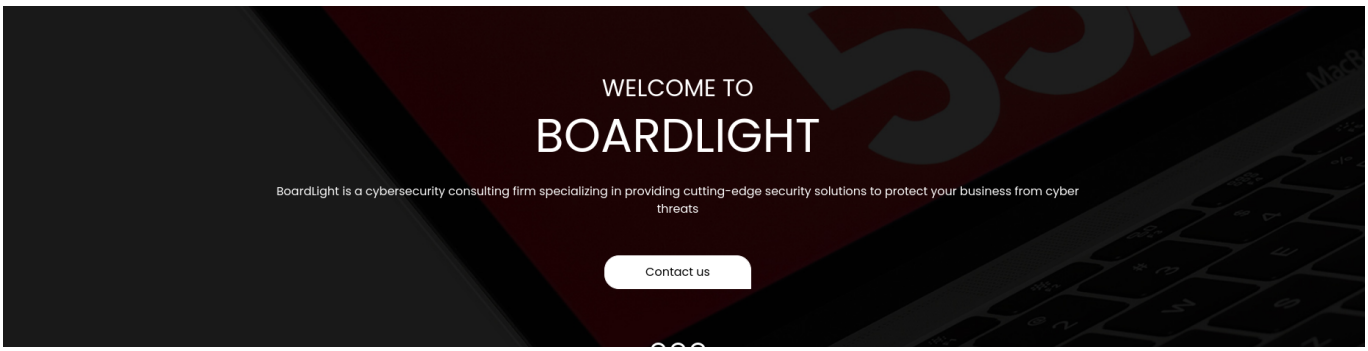
target = 10.10.11.11

nmap scan

```
# Nmap 7.94SVN scan initiated Sun Sep 22 15:52:03 2024 as: nmap -sC -A -v -
oN scan.txt 10.10.11.11
Nmap scan report for 10.10.11.11
Host is up (0.15s 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 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=9/22%OT=22%CT=1%CU=41240%PV=Y%DS=2%DC=T%G=Y%TM=66F0
OS:1311%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(SP=107%GCD=2%ISR=108%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CS
OS:T11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=
OS:FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=
OS:M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)
OS:T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S
OS:+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 10.290 days (since Thu Sep 12 08:55:17 2024)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   195.78 ms 10.10.14.1
2   196.05 ms 10.10.11.11

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun Sep 22 15:52:33 2024 -- 1 IP address (1 host up) scanned
in 30.03 seconds
```

Port 80

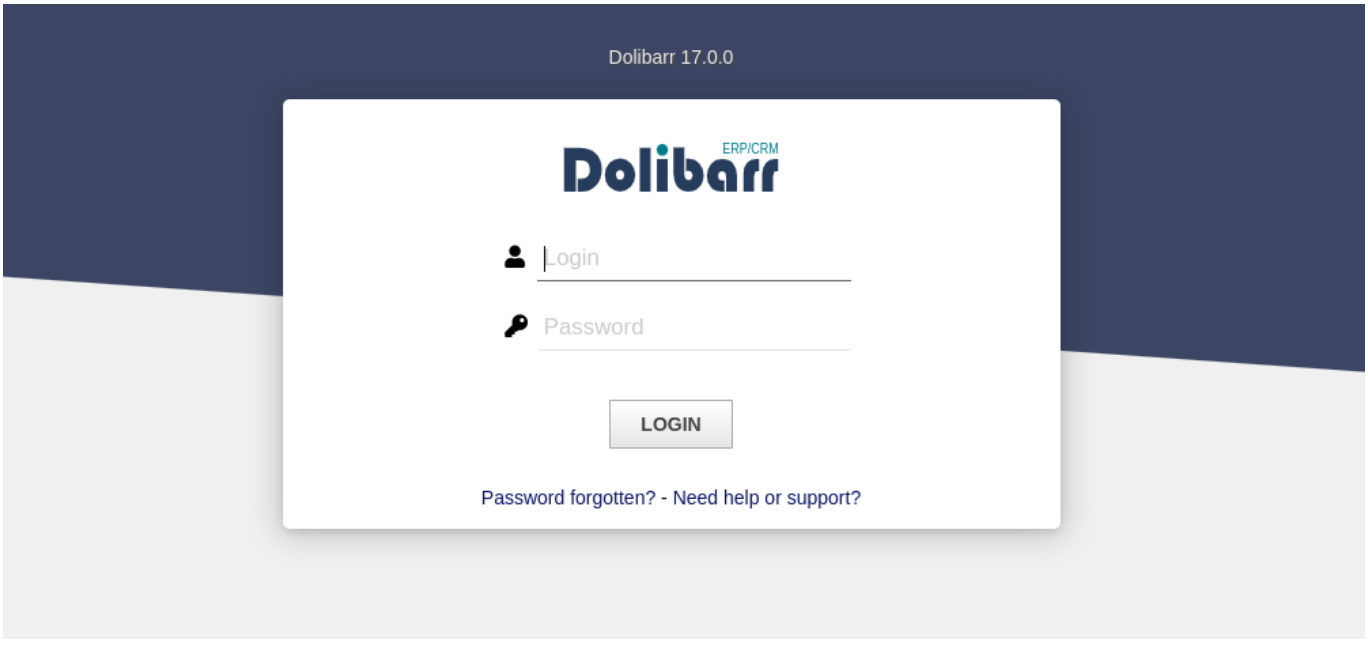
http://board.htb



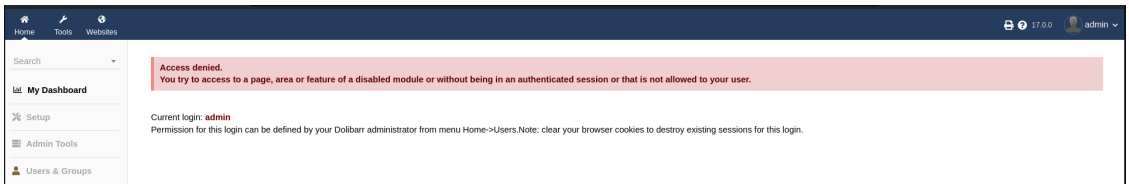
I did directory enumeration but that was a rabbit hole.

Onto subdomain enumeration using ffuf

crm.board.htb

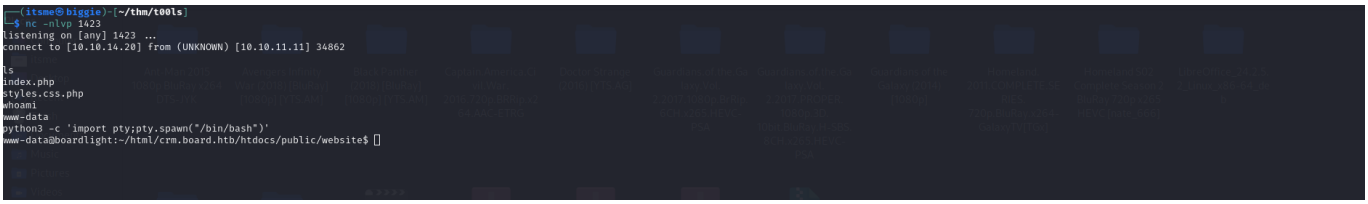


- @1st Thought Process
    - I googled default credentials and I found

    - username=admin;password:admin
    - I logged on but it was of no use
    - 

- @2nd Thought Process
    - I looked for CVE this Dolibarr 17.0.0
        - I found CVE-2023-30253 with an exploit in Github
            - link

With the exploit and a running listener I AM INNN!!!

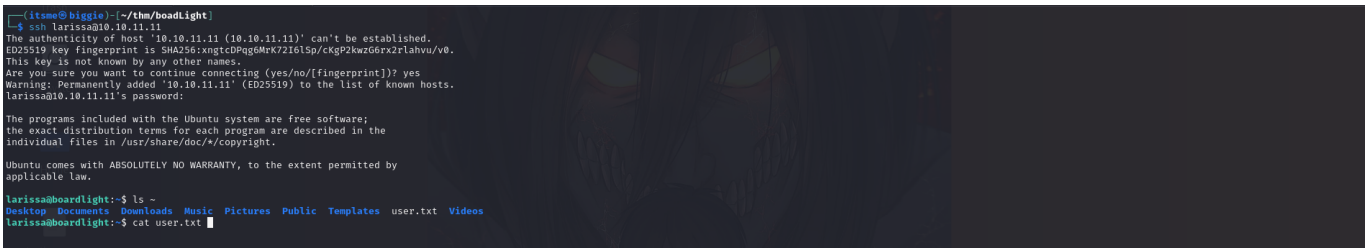


I started looking around then thought hit me, it needs a configuration file. Which I hope will have some database credentials.


```
select login, pass_crypted from llx_user;
+----------+--------------------------------------------------------------+
| login    | pass_crypted                                                 |
+----------+--------------------------------------------------------------+
| dolibarr | $2y$10$VevoimSke5Cd1/nX1Ql9Su6RstkTRe7UX1Or.cm8bZo56NjCMJzCm |
| admin    | $2y$10$gIEKOl7VZnr5KLbBDzGbL.YuJxwz5Sdl5ji3SEuiUSlULgAhhjH96 |
+----------+--------------------------------------------------------------+
```

I tried cracking admin password but I had no luck.

I tried the db password on user larissa and I call me larissa.



Priv Escalation

I approched by running linpeas.

Enlightenment Utilities in suid binaries: These files are part of the Enlightenment window manager system and control various system settings (like backlight and CPU frequency). They require elevated permissions to adjust hardware settings.

```
/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/cpufreq/linux-gnu-x86_64-0.23.1/freqset
```

I did a research in this version and its vulnerable local priv escalation link

I AM ROOT!!!!