Exploit Title: Cuppa CMS – Stored Cross-Site-Scripting

Date: 22-01-2021

Exploit Author: Abida Shariff

Vendor Homepage: <https://www.cuppacms.com/>

Software Link: <https://cuppacms.com/files/cuppa_cms.zip>

Tested on: Windows 10

Stored Cross-Site-Scripting(XSS):

Stored XSS, occurs when user supplied input is stored and then rendered within a web page. Typical entry points for stored XSS are: message forums, blog comments, user profiles and username fields. An attacker typically exploits this vulnerability by injecting XSS payloads, tricking them into viewing the page that contains the stored XSS payload. The victim visits the page and the payload is executed client side by the victim’s web browser. Stored XSS is also known as persistent XSS.

Attack Vector:

Stored XSS is particularly dangerous in application areas where users with high privileges have access. When the administrator visits the vulnerable page, the attack is automatically executed by their browser. This might expose sensitive information such as session authorization tokens and it can be used in combination with other web vulnerabilities to exploit a higher severity security vulnerability.

Vulnerable Parameters: First Name, Last Name

Steps To Reproduce:

1. Login into Cuppa cms.
2. In the Users section, go to Users Accounts and click on Add New User.
3. Put the below payload in the Name and Lastname of the field

bawse"><img src=x onerror=confirm(1)>

1. Click on Save
2. Now open the User which was saved. The below output will be showed.

URL:

<https://localhost/cuppacms/#/component/table_manager/view/cu_users/bawse>

1. The XSS will be triggered.

