CSZ CMS Tickets

CSZ CMS is a open source content management system. With Codeigniter.
Brought to you by: cskaza

#2 Cross Site Script Vulnerability on module "Articlle" in CSZ CMS version 1.2.9

Milestone: 1.0	**Status:** open	**Owner:** Champ Cskaza	**Labels:** Bugs (3)
Updated: 2021-07-10	**Created:** 2020-09-04	**Creator:** r0ck3t	**Private:** No

/Describe the bug/
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Article" feature CSZ CMS Backend

/To Reproduce/
Steps to reproduce the behavior:

1. Login into the panel
2. Go to 'CSZCMS/admin/plugin/article/article'
3. Click "New Article"
4. Insert Payload in Pages Content:
   '>< details/open/ontoggle= confirm(1337)>
5. Save & Exit
6. Click Edit >> Alert xss message!

/Expected behavior/
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page

/Impact/
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

/Desktop (please complete the following information):/
OS: Windows
Browser: All

I Hope you fix it ASAP

/Sceemhost/

5 Attachments


1.PNG


2.PNG


3.PNG


4.PNG


5.PNG

Discussion

r0ck3t - *2021-07-10*

CVE-2020-25392

Log in to post a comment.

SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

Team

SourceForge Headquarters

225 Broadway Suite 1600

San Diego, CA 92101

+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status