



**HIGH VULNERABILITY**  
CRAFTCMS – STORED  
XSS & DENIAL OF  
SERVICE

**DATE:** 21/08/2023

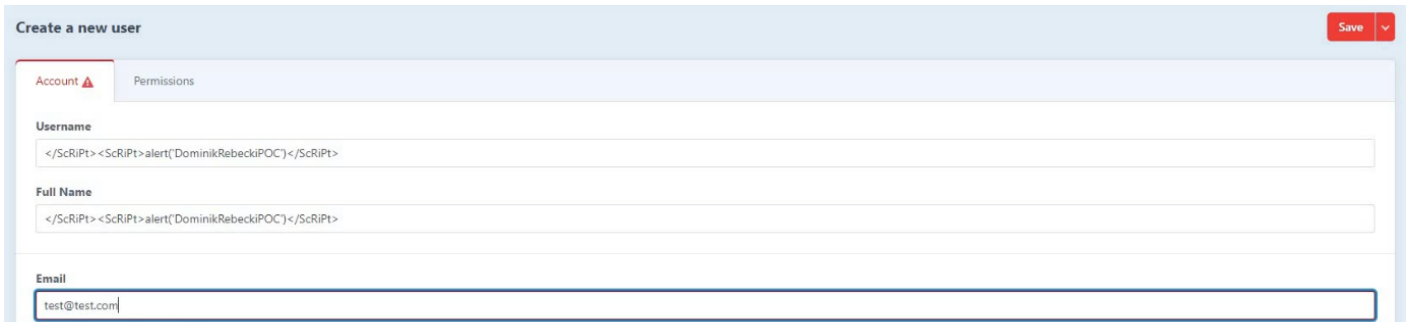
**PREPARED BY:** Dominik Rebecki

# THREAT BRIEFING

## Executive Summary

In the ever-evolving landscape of cybersecurity, recent scrutiny has unveiled two critical vulnerabilities within CraftCMS, identified as CVE-2023-36259 (Stored XSS) and CVE-2023-36260 (DoS).

The first vulnerability, CVE-2023-36259, highlights a Stored Cross-Site Scripting flaw stemming from deficient input validation within CraftCMS's Audit Plugin. Malicious actors are able to exploit this vulnerability by introducing malevolent JavaScript code during the user creation phase. This is shown in the screenshot below.



After accessing the "audit" tab, users inadvertently trigger the execution of the injected code, potentially resulting in unauthorised access and data breaches, as evidenced in the following screenshot..



Notably, CraftCMS promptly addressed this issue in version 3.0.2 of the Audit Plugin, signifying a dedication to enhancing security protocols.

The second vulnerability, CVE-2023-36260, manifests as a Denial of Service (DoS) hazard. This vulnerability capitalises on CraftCMS's susceptibility to injected JavaScript code, particularly

within specific fields (Name and Feed URL), as illustrated in the screenshots below.

</ScRiPt><ScRiPt>alert('DominikRebeckiPOC')</ScRiPt>

**Name** •  
What this feed will be called in the CP.

**Feed URL** •  
Can be a file on the local file system or from a website url (http://...).

**Feed Type** •  
Choose what type of feed you're retrieving.  
ATOM

**Element Type** •  
Choose what element you want to save your feed data to.  
Asset

**Asset Volume** •  
Choose the asset volume you want to save your feed data into.  
None

By adroitly manipulating these fields, cyber attackers can set off a sequence of errors upon accessing the "feed-me" page, as seen in the screenshot below. This effectively renders the targeted website non-responsive, inflicting significant financial losses and reputational harm.



Recognising the gravity of this threat, CraftCMS responded with a patch released in version >4.6.1.1, effectively mitigating the vulnerability and safeguarding against potential service disruptions.

AMR CyberSecurity, the security research entity behind the discovery of these vulnerabilities, strongly recommends a prompt and comprehensive response. Updating to version 3.0.2 of the Audit Plugin and CraftCMS version >4.6.1.1 (for the DoS vulnerability) is essential to mitigating these risks. These instances underscore the paramount importance of proactive security measures, robust input validation, and swift updates in the continuous endeavour to fortify digital systems against the evolving landscape of cybersecurity threats.

## Additional information

More information about the rick above is available from the following sources:

- <https://github.com/sjelfull/craft-audit/commit/b99e4eacbc291473cf8179d0389e49024aaadc2a>
- <https://github.com/sjelfull/craft-audit/pull/73>
- <https://github.com/craftcms/feed-me/commit/b5d6ede51848349bd91bc95fec288b6793f15e28>

## *MITRE ATT&CK Techniques Observed*

<b>ID</b>	<b>Description</b>
T1059	Command-Line Interface
T1496	Resource Hijacking
T1499	End Point Denial of Service
T1500	Hooking