Cross-site Scripting (XSS) - Stored in monicahq/monica

0

Valid Reported on Aug 31st 2020

Description

HTML codes can be entered and successfully run in the journal session of Monica, which allows an attacker to trigger XSS query's like `<svg/onload=alert("StoredXSS")>` causing a persistant stored XSS in the journal session. files at monica/2. <3

POC

setup monica using docker or other means like their online test platform.
source : LINK
go to the journal part.
try payload `<svg/onload=alert("blah!!,blah!!!,blah!!!!")>`

Fix Suggestion

Sanitize the input / escape the xss charecters or else escape the user inputs from html tags, i think it works.

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Low (3.8)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Ajmal Aboobacker
@b3ef
pro

Fixed by

Michele Romano
@mik317
unranked

This report was seen 273 times.

Sign in to join this conversation