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

0

Valid Reported on Jan 2nd 2022

Description

Stored XSS is a vulnerability in which the attacker can execute arbitrary javascript code in the victim's browser. The XSS payload is stored in a webpage and it gets executed whenever someone visits that webpage.

Proof of Concept

1 Visit "Contact Us" page and put `<img src=asdasd onerror=alert(document.domain)>` in `Message` field. Click on `Send Message` button.
2 Now, the admin opens the `Contact Us` module in admin panel and attacker's xss payload will be executed.

Impact

The attacker can execute any arbitrary javascript code and acheive the following:
Steal CSRF token of the **admins** and do any unintended actions on their behalf like enable/disable a module, change website etc.
Execute malicious javascript e.g. crypto miners
and many more...

Occurrences

FormsManager.php L137-L794

Not cleaning xss payloads

CVE-2022-0278
(Published)

Vulnerability Type

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

Severity
High (7.2)

Visibility
Public

Status
Fixed

Found by

Rohan Sharma
@r0hansh
unranked

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 349 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

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

its fixed

Bozhidar 10 months ago Maintainer

https://github.com/microweber/microweber/commit/b64ef574b82dbf89a908e1569d790c7012d1ccd7

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 b64ef5 10 months ago

Peter Ivanov has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

FormsManager.php#L137-L794 has been validated ✅

Sign in to join this conversation

terms

privacy policy

Chat with us