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

0

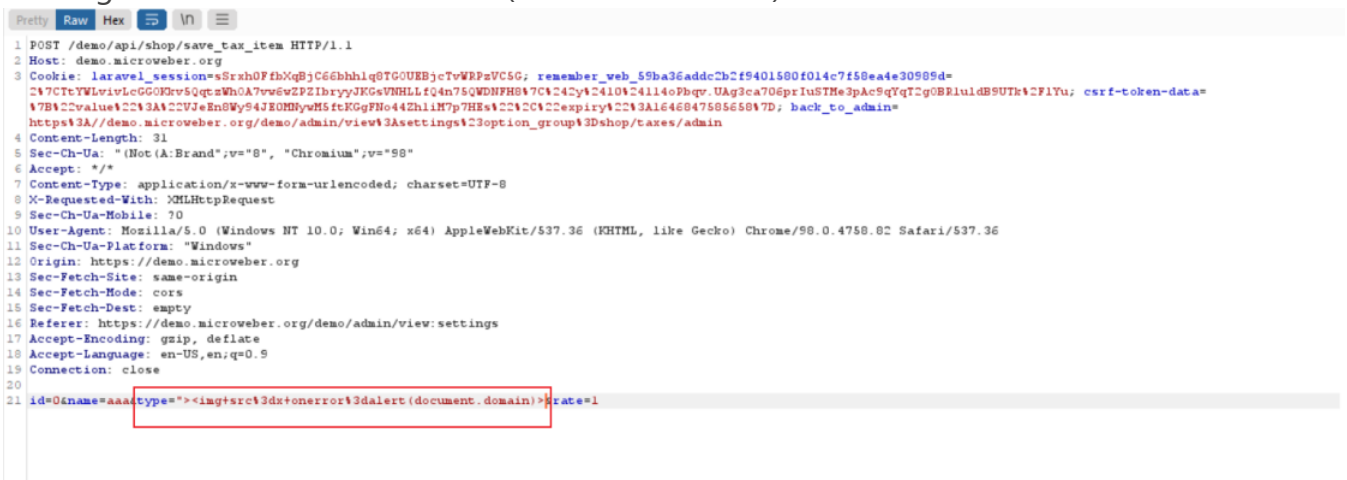
Valid Reported on Mar 9th 2022

Description

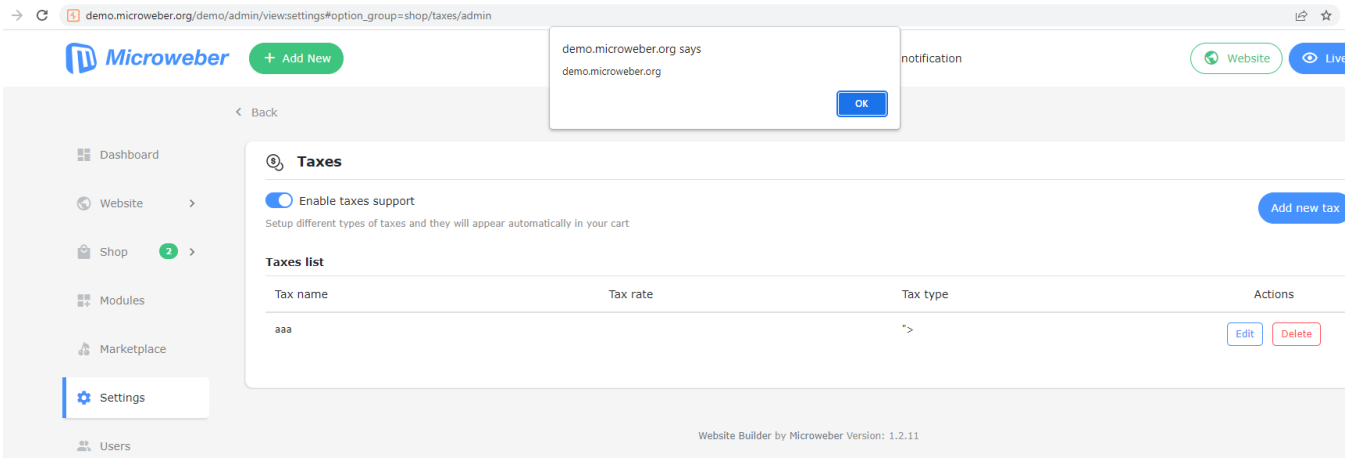
Type parameter in the body of POST request triggered by add/edit tax in microweb are vulnerable to stored XSS.
(1) Settings > Taxes > Tax type

Proof of Concept

Step (1): Access https://demo.microweber.org/?template=dream
Step (2): Browse to Settings > Taxes > Tax type
Step (3): Add or Edit current tax and input legitimate value so as to capture legitimate request
Step (4): Modify the value of type parameter in the POST request body with below example, which is URL encoded:
"><img+src%3dx+onerror%3dalert(document.domain)>



Step (5): Forward the request after modification
An attack controlled alert box will be prompted whenever a user access this page, i.e. (Settings > Taxes > Tax type)



Impact

If an attacker can control a script that is executed in the victim's browser, they might compromise that user, in this case, an admin, by stealing its cookies.

CVE
CVE-2022-0928
(Published)

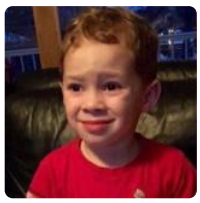
Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by



James Yeung
@scriptidiot
unranked

Fixed by

Bozhidar Slaveykov
@bobimicroweber

Chat with us

maintainer

This report was seen 611 times.

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

James Yeung modified the report 9 months ago

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

Bozhidar Slaveykov validated this vulnerability 9 months ago

James Yeung has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in **1.2.12** with commit **fc9137** 9 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation