Stored XSS on Categories in microweber/microweber

0

Valid Reported on Aug 7th 2022

Description

Title parameter in the body of POST request when creating/editing a category is vulnerable to stored XSS.

Proof of Concept

1 - Go to https://demo.microweber.org/demo/admin/view:content/action:categories
2 - Create a category or edit an existing one.
3 - Modify the title to an XSS Payload: "><iframe onload=prompt(1)>
4 - Save it, And upon visiting categories or shop / when users visit the website an XSS popup will appear.

Screenshots and Video POC

```
https://drive.google.com/drive/folders/155GUYDLkFpgezR8LiaI3rl4Ej57aDoKq?us
```

Post Request Body

```
POST /demo/api/category/1 HTTP/1.1
Host: demo.microweber.org
Cookie: XSRF-TOKEN=eyJpdiI6IlJ1SDdTaU1pTENXbnFHRStHL3NQMlE9PSIsInZhbHVlIjoi
Content-Length: 348
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: application/json, text/javascript, */*; q=0.01
X-Xsrf-Token: eyJpdiI6IlJ1SDdTaU1pTENXbnFHRStHL3NQMlE9PSIsInZhbHVlIjoiT2Q3b
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
```

```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://demo.microweber.org
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.microweber.org/demo/admin/category/1/edit
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

id=1&rel_type=content&rel_id=8&data_type=category&parent_id=0&_method=PATCH
```

Impact

Attackers can steal admin/users cookies

CVE
CVE-2022-2777
(Published)

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

Severity
Medium (6.6)

Registry
Other

Affected Version
1.3.0

Visibility
Public

Status
Fixed

Found by

Amine
@ahkecha
legend

Fixed by

Peter Ivanov

@peter-mw

maintainer

This report was seen 639 times.

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

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

Peter Ivanov validated this vulnerability 4 months ago

Amine has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Peter Ivanov marked this as fixed in **1.3.1** with commit **60eef7** 4 months ago

Peter Ivanov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation