

Business Logic Errors in microweber/microweber

0



Valid

Reported on Feb 23rd 2022

Description

Product (status of product is unpublished) has been deleted by admin (in Trash folder) but user can still add to cart and make purchases

Proof of Concept

Step 1: Admin go to Shop > Products: Unpublish product and Delete product

Step 2: User add product to cart by request

POST /demo/api/update_cart HTTP/1.1

Host: demo.microweber.org

Cookie: laravel_session=RFi1m9FJtrMWKbIiBU1jtkSbS1kptgVMESVsCq3E; csrf-token=

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0

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: 13

Origin: https://demo.microweber.org

Dnt: 1

Referer: https://demo.microweber.org/demo/shop

Sec-Fetch-Dest: empty

Sec-Fetch-Mode: cors

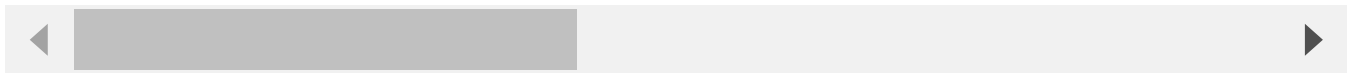
Sec-Fetch-Site: same-origin

Te: trailers

Connection: close

[Chat with us](#)

content_id=15



Demo with product id = 15

<https://drive.google.com/file/d/1XriKKJz3q6TchFMHF9Ec2wM0aSxVEHU/view?usp=>



Impact

User can add deleted product to cart and buy it

CVE

CVE-2022-0762

(Published)

Vulnerability Type

CWE-840: Business Logic Errors

Severity

Medium (5.5)

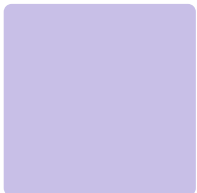
Visibility

Public

Status

Fixed

Found by



Andy

unranked ▾

Fixed by



Bozhidar Slaveykov

maintainer

Chat with us

This report was seen 426 times.

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

9 months ago

Andy 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

Andy has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in 1.3 with commit **763612** 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

hacktivity

leaderboard

FAO

part of 418sec

company

about

team

Chat with us

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)