

XSS in /demo/module/?module=HERE in microweber/microweber

0



Valid

Reported on Apr 22nd 2022

Description

Reflected XSS in /demo/module/?module= bypass of fix for CVE-2022-1439

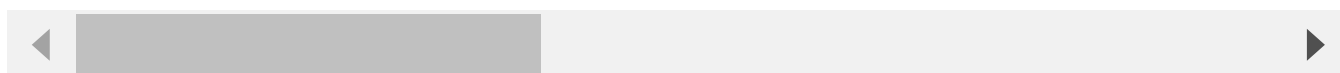
Proof of Concept

In [this report](#) I showed an XSS and while one of the filter evasion mechanisms was fixed, the root cause persists to allow other payloads.

As I mentioned there are event handlers which are unblocked, so even without the <x> trick from last report, you can get XSS.

Here I use ontransitionrun, there are more and there will always come more event handlers, so a blacklist approach will fail here.

[https://demo.microweber.org/demo/module/?module=%27ontransitionrun=alert\(1\)](https://demo.microweber.org/demo/module/?module=%27ontransitionrun=alert(1))



Hitting "tab" will fire the payload.

How to fix this

The html looks like this:

```
<div class='x module module-'ontransitionrun=alert(1) ' tabindex="1" st
```



You can not allow breaking out of the "class" attribute, so remove or encode the 's in the input. That's the main thing here.

Chat with us

Impact

Typical impact of XSS attacks.

References

- [old report](#)

CVE

CVE-2022-1504

(Published)

Vulnerability Type

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

Severity

Medium (6.3)

Registry

Other

Affected Version

?

Visibility

Public

Status

Fixed

Found by



Finn Westendorf

@wfinn

legend

Fixed by



Peter Ivanov

@peter-mw

maintainer

This report was seen 531 times.

Chat with us

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

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

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

Peter Ivanov validated this vulnerability 7 months ago

Finn Westendorf 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 **1.2.15** with commit **1f6a4d** 7 months ago

Peter Ivanov 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

FAQ

part of 418sec

company

about

team

Chat with us

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)