Reflected XSS on demo.microweber.org/demo/module/ in microweber/microweber

0

✓ Valid Reported on Apr 21st 2022

Description

Reflected XSS with filter bypass on /demo/module/ using module= & style= parameters.

Proof of Concept

```
https://demo.microweber.org/demo/module/?module='ont<a>ransitionend=alert(1
```

Press tab for the alert() to show up.
Okay 3 things to unpack here:

" and ' at various places allow breaking out of the html (root cause of the XSS)
ont<x>ransitionend gets sanitized to ontransitionend and bypasses the xss filter
style="transition:outline 1s" tabindex=1 is the setup you need to trigger a transition without a <style> tag

Took me some time to finally find a XSS payload that runs here :)
I'd suggest you do not allow breaking out of the html here, so filter ' & ". ont<x>ansitionend should be examined, this trick doesn't work in every parameter. Additionally, some js eventhandlers are allowed e.g. onunhandledrejection, you could think about a on.*= regex.

Impact

Execute Arbitrary JavaScript as the attacked user.
It's the only payload I found working, you might need to press "tab" but there is probably a paylaod that runs without user interaction.

References

- New Xss Vectors

CVE
CVE-2022-1439

(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 935 times.

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

Finn Westendorf modified the report 7 months ago

Finn Westendorf modified the report 7 months ago

Finn Westendorf modified the report 7 months ago

Finn Westendorf 7 months ago

Researcher

```
https://demo.microweber.org/demo/module/?module=%27onm%3Ca%3Eouseover=alert(1)%27%22ta
```

So the trick actually was the onev<x>nthandler in the module parameter, the transition is not needed, e.g. above I use onmouseover. The html is very different from when a valid value of the module parameter is used.

```
<div class='x module module-'onmouseover=alert(1) '   tabindex="1"   style="width:100%
```

We have contacted a member of the **microweber** team and are waiting to hear back 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 **ad3928** 7 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

Chat with us