

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

0



Valid

Reported on Feb 18th 2022

Description

Can escape the `meta` tag because the user doesn't escape the double-quote in the `$redirectUrl` parameter when logging out.

Proof of Concept

```
https://<server>/demo/api/logout?redirect_to="/asdf"><iframe onload=alert(dc
```



Impact

Through this vulnerability, an attacker is capable to execute malicious scripts.

CVE

CVE-2022-0678

(Published)

Vulnerability Type

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

Severity

Medium (6.5)

Visibility

Public

Status

Fixed

Found by



Ducas

Chat with us



Pocas

@p0cas

amateur ✓

Fixed by



Peter Ivanov

@peter-mw

maintainer

This report was seen 420 times.

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

9 months ago

Bozhidar 9 months ago

Maintainer

fixed

Peter Ivanov validated this vulnerability 9 months ago

Pocas has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Peter Ivanov marked this as fixed in 1.2.11 with commit 2b8fa5 9 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

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us