Reflected XSS on /api/module in microweber/microweber

1

Valid Reported on Jun 21st 2022

Description

Reflected XSS via filter bypass on /api/module using type= parameter.

Proof of Concept

```
https://demo.microweber.org/demo/api/module?type=</script><script>alert("xs
```

The value of the "type" parameter is injected into the source code of the page at line 63. Since the value of the "type" parameter is not sanitized, it is possible to close the div tag with ' </script> ' and then put javascript code.

Impact

Execute arbitrary JavaScript code with the privileges of the victim's user. This can be used for cookie stealing (account takeover), for example.

CVE
CVE-2022-2174
(Published)

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

Severity
Medium (6.5)

Registry
Other

Affected Version
<=1.2.17

Visibility
Public

Status
Fixed

Found by

jhond0e
@jhond0e
legend

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 580 times.

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

jhond0e 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 **1.2.18** with commit **c51285** 5 months ago

Peter Ivanov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation