File upload filter bypass leading to stored XSS in microweber/microweber

0

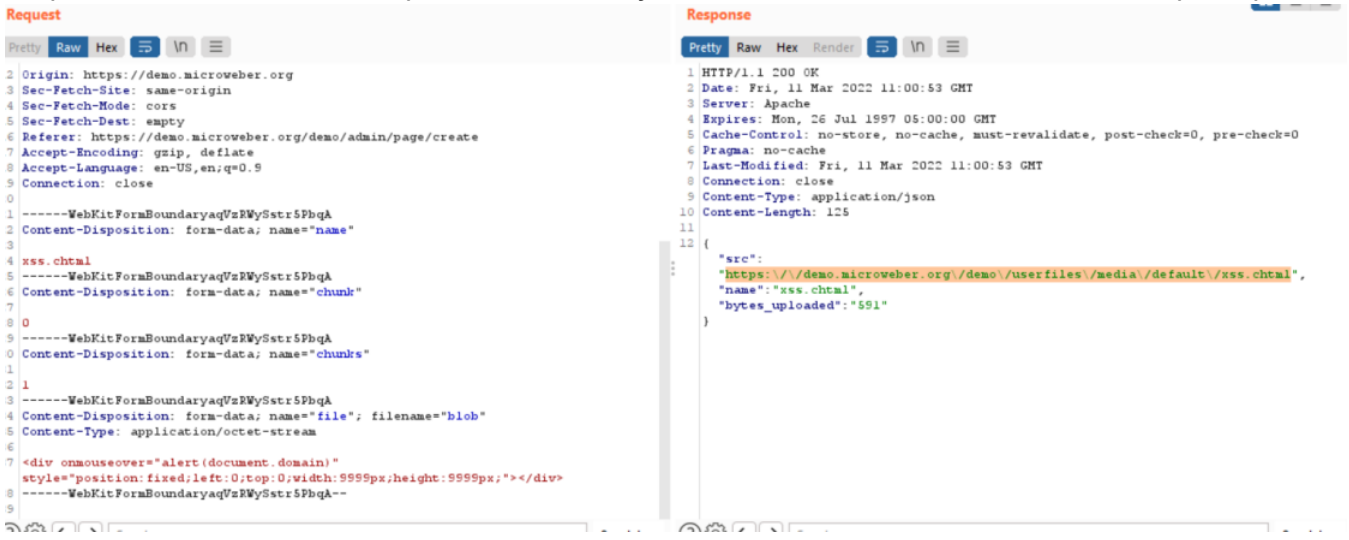
Valid Reported on Mar 11th 2022

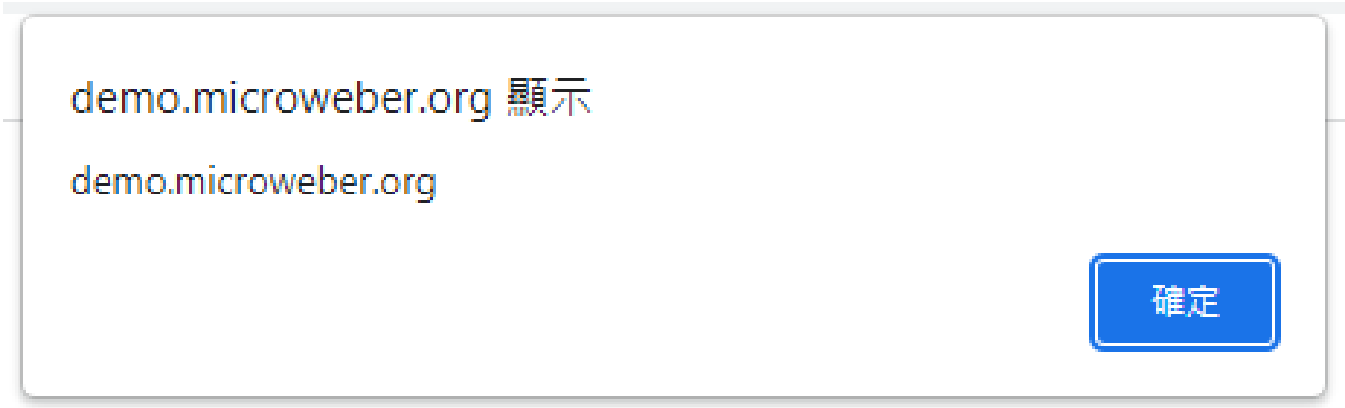
Description

A User can upload .[a-z]html file (e.g. ahtml, bhtml, chtml, ddhtml, AS LONG AS it ends with html) with XSS payload. Upon upload, a URL with malicious html can be accessed and javascript will be executed.

Proof of Concept (taking chtml as example)

Step (1) Login to the demo portal with admin creds at https://demo.microweber.org/demo/admin/
Step (2) Add new > Page > Add file in picture
Step (3) Upload below file with content below and named as xss.chtml
Step(4) Access the link in response and once you move the cursor, alert box will be prompted





Impact

If an attacker can control a script that is executed in the victim's browser, they might compromise that user, in this case, an admin, by stealing its cookies.

CVE
CVE-2022-0930
(Published)

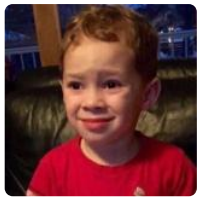
Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
High (8)

Visibility
Public

Status
Fixed

Found by



James Yeung
@scriptidiot
unranked

Fixed by

Bozhidar Slaveykov
@bobimicroweber

maintainer

This report was seen 911 times.

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

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

Bozhidar Slaveykov validated this vulnerability 9 months ago

James Yeung has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in **1.2.12** with commit **33eb4c** 9 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

leaderboard

FAQ

contact us

terms

privacy policy

team

Chat with us