

Stored XSS via File Upload in star7th/showdoc

0

✓ Valid

Reported on Mar 14th 2022

Description

Stored XSS via uploading file in `.md` format.

Proof of Concept

```
filename="poc.md"
```

```
<script>alert(1)</script>
```

Steps to Reproduce

1. Login into showdoc.com.cn.
2. Navigate to file library (<https://www.showdoc.com.cn/attachment/index>)
3. In the File Library page, click the Upload button and choose the `poc.md` file.
4. After uploading the file, click on the check button to open that file in a new tab.

XSS will trigger when the attachment is opened in a new tab.

POC URLs: <https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=5508861cc308714a5e2bd926da5b9678>

Impact

An attacker can perform social engineering on users by redirecting them from a real website to a fake one. a hacker can steal their cookies etc.

(Published)

Vulnerability Type

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

Severity

High (7.1)

Visibility

Public

Status

Fixed

Found by



Ajaysen R

@ajaysenr

unranked ▼

Fixed by



star7th

@star7th

unranked ▼

This report was seen 463 times.

We are processing your report and will contact the **star7th/showdoc** team within 24 hours.
8 months ago

star7th validated this vulnerability 8 months ago

Ajaysen R has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

star7th marked this as fixed in **v.2.10.4** with commit **56e450** 8 months ago

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us



Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us