huntr

Stored XSS via file upload in star7th/showdoc

0

✓ Valid Reported on Mar 13th 2022

Description

Hello Team,

This is a bypass to the report in https://huntr.dev/bounties/6127739d-f4f2-44cd-ae3d-e3ccb7f0d7b5/.
The upload feature allows the files with the extension `.xxhtml` which leads to Stored XSS.

Proof of Concept

```
filename="poc.xxhtml"

<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.xxhtml`
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 URL: `https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=f79c619fb54bf22255af3797e25cfcfc`

Impact

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

Chat with us

CVE

CVE-2022-0938
(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

Ajaysen R

@ajaysenr

unranked

This report was seen 515 times.

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

Ajaysen R modified the report 8 months ago

Ajaysen R modified the report 8 months ago

Ajaysen R submitted a patch 8 months ago

star7th validated this vulnerability 8 months ago

Ajaysen R has been awarded the disclosure bounty ✓

Chat with us

The fix bounty is now up for grabs

star7th marked this as fixed in **v2.10.4** with commit **830c89** 8 months ago

Ajaysen R has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us