Stored XSS due to Unrestricted File Upload in star7th/showdoc

0

Valid Reported on Mar 13th 2022

Description

Stored XSS via uploading files in `.xsl` format.

Proof of Concept

```
filename="poc.xsl"

<a:script xmlns:a="http://www.w3.org/1999/xhtml">alert(1)</a: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.xsl` 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 URL: `https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=73b27c6f38a6d5daed4df8e9d3b86185`

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.

CVE
CVE-2022-0941

(Published)

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

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by

Ajaysen R
@ajaysenr
unranked

Fixed by

Ajaysen R
@ajaysenr
unranked

This report was seen 520 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 submitted a **patch** 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 **v2.10.4** with commit **4b6e66** 8 months ago

Ajaysen R has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation