huntr

# Stored XSS viva axd and cshtml file upload in star7th/showdoc in star7th/showdoc

0

✓ Valid Reported on Mar 13th 2022

## Description

This is a bypass of the report: https://huntr.dev/bounties/3eb5a8f9-24e3-4eae-a212-070b2fbc237e/ & https://huntr.dev/bounties/6127739d-f4f2-44cd-ae3d-e3ccb7f0d7b5/. Here the upload functionality allows the malicious files with the extension .cshtml and .axd which leads to Stored XSS.

## Proof of Concept

1.First, open your text file/notepad and paste the below payload and save it as New_XSS.cshtml and XSS.axd:

```
<html>
<script>alert(1337)</script>
<script>alert(document.domain)</script>
<script>alert(document.location)</script>
<script>alert('XSS_by_Samprit Das')</script>
</html>
```

2.Then go to https://www.showdoc.com.cn/ and login with your account.
3.Afther that navigate to file library (https://www.showdoc.com.cn/attachment/index)
4.In the File Library page, click the Upload button and choose the New_XSS.cshtml and XSS.axd
5.After uploading the file, click on the check button to open that file in a new tab.

## PoC URL

https://img.showdoc.cc/622e39769ff8d_622e39769ff86.cshtml?e=1647201129&token=-YdeH6WvESHZKz-yUzWjO-uVV6A7oVrCN3UXi48F:gy0tywgMIYI1yTi7KYfXI1PJtIE=
https://img.showdoc.cc/622e441f9f79c_622e441f9f793.axd?e=1647202922&token=-YdeH6WvESHZKz-yUzWjO-uVV6A7oVrCN3UXi48F:esQLnEOOKHWz0j9QqpI999fchtE=

## Video & Image PoC

https://drive.google.com/drive/folders/1lvidM91pZBkQH3HpafrU-6wmh4Y5MLUD?usp=sharing

## Impact

This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.

CVE
CVE-2022-0945
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
Critical (9)

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

Fixed by

star7th
@star7th
unranked

This report was seen 498 times.

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

Chat with us

star7th validated this vulnerability 8 months ago

SAMPRIT DAS 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 ba45d1 8 months ago

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us