huntr

Stored XSS viva cshtm file upload in star7th/showdoc

0

Valid Reported on Mar 14th 2022

Description

This is a bypass of the report:https://huntr.dev/bounties/8702e2bf-4af2-4391-b651-c8c89e7d089e/. Here the upload functionality allows the malicious files with the extension .cshtm which leads to Stored XSS.

Proof of Concept

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

```
<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 XSS.cshtm
5.After uploading the file, click on the check button to open that file in a new tab.

PoC URL

https://img.showdoc.cc/622ebe1b26479_622ebe1b2646f.cshtm?e=1647234162&token=-YdeH6WvESHZKz-yUzWjO-uVV6A7oVrCN3UXi48F:u3jx4rpeao3gm0GikHZ_L7tlI3Y=

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-2022-0946

CVE-2022-0946
(Published)

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

Severity
Critical (9)

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

Fixed by

star7th
@star7th
unranked

This report was seen 503 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

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 **e5d575** 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

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us