Stored XSS viva .webmv file upload in star7th/showdoc

0

✓ Valid   Reported on Mar 14th 2022

Description

The application allows .webmv files to upload which lead to stored XSS

Proof of Concept

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

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

PoC URL

https://img.showdoc.cc/622f4ea2e82e9_622f4ea2e82e2.webmv?e=1647272721&token=-YdeH6WvESHZKz-yUzWjO-uVV6A7oVrCN3UXi48F:WZQWcl9TWatpZGaHXf2Mnf6pEI8=

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.

Occurrences

AttachmentModel.class.php L328

CVE

CVE-2022-0964

(Published)

Vulnerability Type

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

Severity

High (8)

Visibility

Public

Status

Fixed

Found by

SAMPRIT DAS

@sampritdas8

pro

Fixed by

star7th

@star7th

unranked

This report was seen 499 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 **2.10.4** with commit **3caa32** 8 months ago

Chat with us

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

AttachmentModel.class.php#L328 has been validated ✓

Sign in to join this conversation