

Stored XSS viva .properties file upload in star7th/showdoc

0



Valid

Reported on Mar 14th 2022

Description

The application allows .properties 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.properties:

```
<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.properties

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

PoC URL

https://img.showdoc.cc/622f4eac577a2_622f4eac5779c.properties?e=1647271151&token=-YdeH6WvESHZKz-yUzWjO-uVV6A7oVrCN3UXi48F:v4d5wUVXBnlauueh9ouLkifIL1w=

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 L333

Chat with us

CVE

CVE-2022-0960

(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 506 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 **92bc6a** 8 months ago

star7th has been awarded the fix bounty ✓

Chat with us

This vulnerability will not receive a CVE 

AttachmentModel.class.php#L333 has been validated 



Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us