Stored XSS due to Unrestricted File Upload in star7th/showdoc

0

Valid Reported on Mar 13th 2022

Description

Stored XSS via uploading files in `.xsd`, `.asa` and `.aspx` (already mentioned in previous report) formats.

Proof of Concept

For .xsd

```
filename="poc.xsd"

<a:script xmlns:a="http://www.w3.org/1999/xhtml">alert(1)</a:script>
```

For .asa and .aspx

```
filename="poc.asa"

<script>alert(1)</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.xsd` 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 URLs:

.xsd - https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=2f29dd262be2e974572a4387fdb10317

.asa - https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=2a9ce4675debdcfb6b324f52c33c3a72

.aspx - https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=72e7ab226e5df530e3c7d13165f25273

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-2022-0942
(Published)

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

Severity
Critical (9.4)

Visibility
Public

Status
Fixed

Found by

Ajaysen R
@ajaysenr
unranked

Fixed by

Ajaysen R
@ajaysenr
unranked

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 8 months ago — Maintainer

I won't set this problem as "fixed" for the time being. If you find similar problems, you can give feedback again

Ajaysen R 8 months ago — Researcher

Ok, Fine.

star7th 8 months ago — Maintainer

I have updated the whitelist mechanism. And tested it again. There should be no more omissions. So let me fix this problem. At the same time, I'll write you the repairer, so you get an extra $20.

https://github.com/star7th/showdoc/blob/master/server/Application/Api/Model/AttachmentModel.class.php#L325

star7th marked this as fixed in **2.10.4** with commit **3caa32** 8 months ago

Ajaysen R has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation