Unrestricted Upload of File with Dangerous Type in star7th/showdoc

0

Valid Reported on Mar 13th 2022

Description

This is a bypass of report https://huntr.dev/bounties/3eb5a8f9-24e3-4eae-a212-070b2fbc237e/.
The upload feature allows the files with the extension .*html which leads to Stored XSS.

Proof of Concept

Step 1: Login into showdoc.com.cn.
Step 2: Go to https://www.showdoc.com.cn/attachment/index
Step 3: In the File Library page, click the Upload button and choose file below. You can use any file extension with regex ".([a-zA-Z0-9])*html"

```
<script>alert(origin)</script>
```

Step 4: Click on the check button to open that file in a new tab.
POC URL:
https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=4422094937428007ab74c30faea73ef3
https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=d40db01d06885a0ff0e2b48818d5ad31
https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=08059f8a61fa5838255f9c3b848ad347

Impact

Stored XSS.

CVE
CVE-2022-0950

CVE-2022-0930
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type
Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

nhiephon
@nhiephon
master

Fixed by

star7th
@star7th
unranked

This report was seen 504 times.

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

star7th 8 months ago Maintainer

I just found the problem you fed back. A similar question was fed back this morning. So I simply disabled the entire "htm" string. The problem you fed back should no longer exist

nhiephon 8 months ago Researcher

Hi maintainer,

I think you don't understand my report.
My report includes many extenstion of passing your checks like .2html, .chtm
Apparently the string .html does not exist in the file format I uploaded.
Please see the report clearly

Please see the report clearly.

Regards.

star7th 8 months ago Maintainer

I'm filtering 'htm' strings without dot

nhiephon 8 months ago Researcher

In lasted report, I can't see it. You filtered using $isDangerStr($filename , ".htm")

star7th 8 months ago Maintainer

https://github.com/star7th/showdoc/commit/e5d575928b1371a7e07b09b6592822298335062a

nhiephon 8 months ago Researcher

Hi,

I find a way bypass in this report :))
You can upload file with extension like ".00000ht"
(https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=471a131951d1754299d9ce99e327fc4e).

There are many formats that can lead to XSS execution, so using a blacklist is impossible. I recommend using whitelist to only render some extension like txt, csv, pdf. For the rest of files will return a downloadable file to user.

Regards.

star7th 8 months ago Maintainer

Well, the blacklist is too hard to enumerate. I'm going to enable the whitelist feature

star7th validated this vulnerability 8 months ago

nhiephon 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 237ac6 8 months ago

star7th has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation