File Upload Restriction Bypass leading to Stored XSS Vulnerability in star7th/showdoc

0

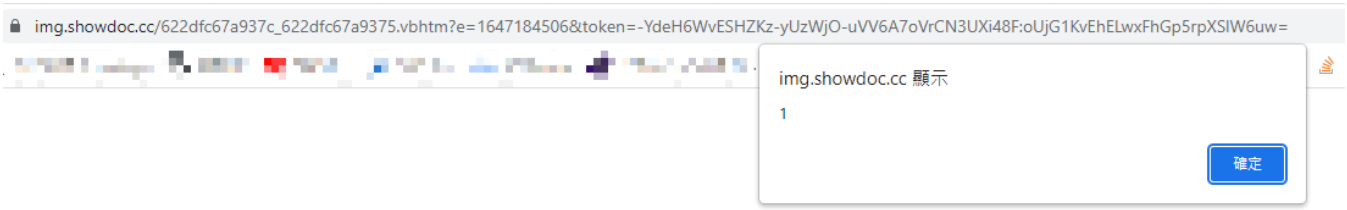
Valid Reported on Mar 13th 2022

Description

File Upload Restriction Bypass leading to Stored XSS Vulnerability, by leveraging file extension **vbhtm, vbhtml, soap, even any extension ends with html (e.g. aahtml, bbhtml)**

Proof of Concept

Step 1) Access https://www.showdoc.com.cn/attachment/index
Step 2) Prepare a file with content below and named as xss.vbhtm to upload
<script>alert(1)</script>
Step 3) Click check
XSS will be triggered



Impact

An attacker could leverage this to perform social engineering and thereby stealing victim's cookie etc.

CVE
CVE-2022-0951
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
High (8.2)

High (8.2)

Visibility
Public

Status
Fixed

Found by

James Yeung
@scriptidiot
unranked

Fixed by

star7th
@star7th
unranked

This report was seen 557 times.

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

James Yeung modified the report 8 months ago

James Yeung modified the report 8 months ago

James Yeung 8 months ago Researcher

@maintainer, please adopt whitelist instead of blacklist, otherwise a lot of file extensions could be abused to cause stored XSS.

James Yeung modified the report 8 months ago

James Yeung modified the report 8 months ago

James Yeung modified the report 8 months ago

James Yeung modified the report 8 months ago

James Yeung modified the report 8 months ago

star7th validated this vulnerability 8 months ago

James Yeung 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