## huntr

# Unrestricted Upload of File with Dangerous Type in star7th/showdoc

0



Reported on Jan 24th 2022

## Description

There is a filter to prevent upload php, HTML, svg filetype in the code snippet from line 115 to line 122 in AttachmentController.class.php:





However, I found a way to bypass this filter via uploading arbitrary files with those filetypes by using %0d character in the filename.

## **Proof of Concept**

Create an malicious HTML file and named it phish.h%0dtml

```
<body>
    <h1>Test upload</h1>
    <script>alert(1)</script>
</body>
</html>
```

Now after login, click the arrow on the top right corner -> go to File Library.

( https://www.showdoc.com.cn/attachment/index )

In the File Library page, click **Upload** button and choose the phish.h%0dtml After uploading successfully, click on the check button to open it in a new tab. You will see that the HTML file is executed, this will happen the same with other filetypes.

## **Impact**

This vulnerability has the potential to deface websites, result in compromised user accounts, and can run malicious code on web pages, which can lead to a compromise of the user's device.

### Occurrences



AttachmentController.class.php L97-L129

#### CVE

#### Vulnerability Type

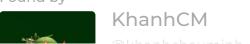
CWE-434: Unrestricted Upload of File with Dangerous Type

#### Severity

#### Visibility

#### Status

#### Found by



Chat with us







#### Fixed by



star7th
@star7th
unranked •

This report was seen 448 times.

We are processing your report and will contact the **star7th/showdoc** team within 24 hours. 10 months ago

KhanhCM modified the report 10 months ago

We have contacted a member of the **star7th/showdoc** team and are waiting to hear back 10 months ago

star7th 10 months ago Maintainer

I tried to upload the file Phish I h%Odtml did succeed. But JS didn't execute when I downloaded it. It directly pops up the file download box and does not execute HTML or JS. Did I reproduce it wrong? https://www.showdoc.com.cn/server/api/attachment/visitFile? sign=d4cdb8d37e715c9940329fbc17bbff0c

KhanhCM 10 months ago

Researcher

I've just retested on both Firefox and Chrome browsers and am still able to reproduce the vulnerability. When I go to the file's link, the JS is executed and the HTML is rendered.

You can view my link at https://www.showdoc.com.cn/server/api/attachment/visitFile?sign=5f0f670e39c18ea5b49a392c86b17a9f

star7th 10 months ago

Maintainer

I have fixed the problem. You can verify it

Chat with us

star7th validated this vulnerability 10 months ago
KhanhCM has been awarded the disclosure bounty ✓
The fix bounty is now up for grabs
We have sent a fix follow up to the <b>star7th/showdoc</b> team. We will try again in 7 days. 10 months ago
We have sent a second fix follow up to the <b>star7th/showdoc</b> team. We will try again in 10 days 10 months ago
We have sent a third and final fix follow up to the <b>star7th/showdoc</b> team. This report is now considered stale. 9 months ago
star7th marked this as fixed in 2.10.2 with commit 7383d7 9 months ago
star7th has been awarded the fix bounty ✓
This vulnerability will not receive a CVE 🗶
AttachmentController.class.php#L97-L129 has been validated ✓
Sign in to join this conversation
22 © 418sec

huntr	part of 418sec
home	company
hacktivity	about

Chat with us

FAO

contact us

terms

privacy policy