

Unrestricted Upload of File with Dangerous Type in star7th/showdoc



Valid

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`:

```
if (strstr(strip_tags(strtolower($uploadFile['name'])), ".php")
    || strstr(strip_tags(strtolower($uploadFile['name'])), ".htm")
    || strstr(strip_tags(strtolower($uploadFile['name'])), ".svg")

) {
    $this->sendError(10100, '不支持此文件类型');
    return false;
}
```

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`

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8"/>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Test Upload File</title>
</head>
```

[Chat with us](#)

```
<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

CVE-2022-0409

(Published)

Vulnerability Type

CWE-434: Unrestricted Upload of File with Dangerous Type

Severity

High (7.2)

Visibility

Public

Status

Fixed

Found by



KhanhCM

@khanhcmvn

Chat with us



@khanncnauminn

pro

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%0dtml 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

We have sent a follow up to the **star7th/showdoc** team. We will try again in 7 days. 10 months ago

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 star7th/showdoc team. We will try again in 7 days.
10 months ago

We have sent a second fix follow up to the star7th/showdoc team. We will try again in 10 days.
10 months ago

We have sent a third and final fix follow up to the star7th/showdoc 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

2022 © 418sec

huntr

home

hacktivity

part of 418sec

company

about

Chat with us

[leaderboard](#)

[team](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)