

New issue

[Jump to bottom](#)

Exporting to PDF contains opportunities for XSS attacks #3178

Closed

fungo1024 opened this issue on Jul 28, 2019 · 1 comment

Labels

security issue 🐛

fungo1024 commented on Jul 28, 2019 · edited

Current behavior

Notes Exported to PDF Format Is Existing XSS Attacks.

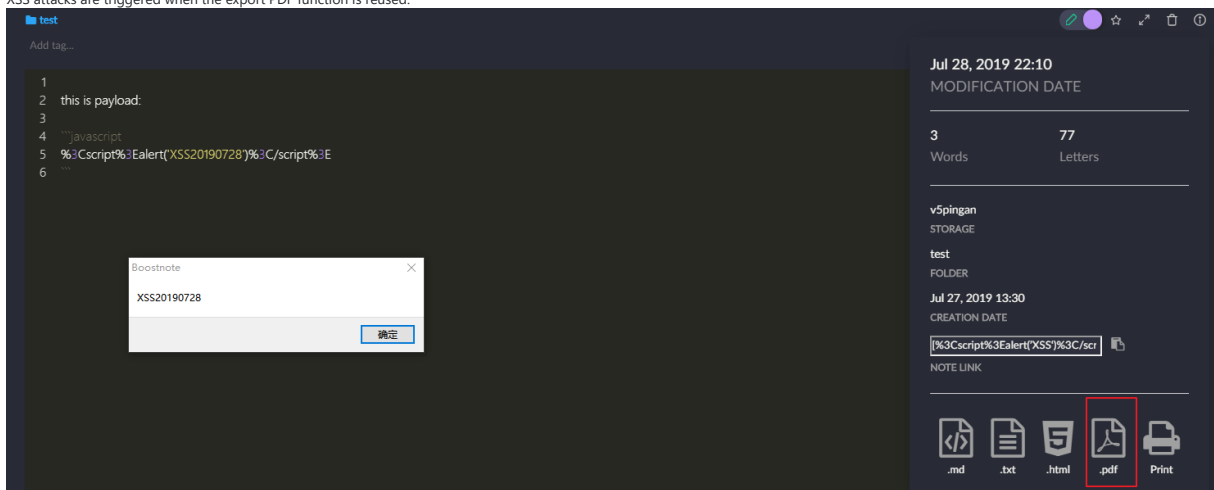
Expected behavior

Notes Exported to PDF Format Is Existing XSS Attacks.

When there is a code in the note:

```
``` JavaScript
% 3Cscript%3Ealert('XSS')%3C/script%3E
```
```

XSS attacks are triggered when the export PDF function is reused.



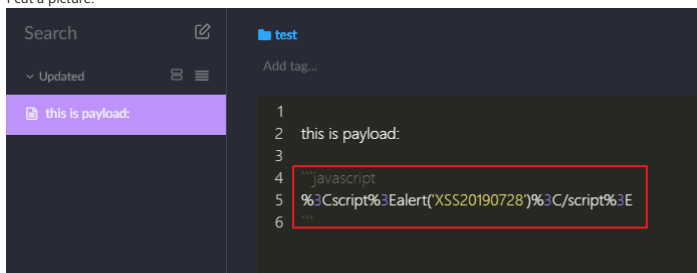
Steps to reproduce

1. Put the payload below into your notes.

- Payload:

```
``` JavaScript
% 3Cscript%3Ealert('XSS')%3C/script%3E
```
```

I cut a picture:



2. Click on the "Info" button in the upper right corner of the note to export the file in PDF format. This will trigger payload to generate a bullet window, that is, there is an XSS attack.

Environment

- Version : 0.12.1
- OS Version and name : Microsoft Windows 10 Home Chinese Version

 Flexo013 added the security issue  label on Jul 28, 2019

  Flexo013 changed the title ~~Notes Exported to PDF Format Is Existing XSS Attacks~~ Exporting to PDF contains opportunities for XSS attacks on Jul 28, 2019

  AWolf81 mentioned this issue on Jul 31, 2019

Fix XSS vulnerability after PDF export (issue #3178) #3192

 Merged

Flexo013 commented on Aug 24, 2019

Contributor


Will be fixed in 0.13.0

 Flexo013 closed this as completed on Aug 24, 2019

Assignees

No one assigned

Labels

security issue 

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

