New issue

Jump to bottom

Fix XSS security vulnerability #2072

Merged richard015ar merged 6 commits into dev from pb-404-xss-fix on Jan 13, 2021

Conversation 6 Commits 6 Checks 0 Files changed 4

arzola commented on Jan 12, 2021 • edited — Contributor

Related issues #2066 and #404

This security fix clean and sanitize metadata book info metaboxes to prevent XSS attacks on fields that allows HTML input, this uses Htmlawed to filter and sanitize the input values.

How to test

Requirements:

- Access to the latest Pressbooks admin interface

Steps:

- Enter to the admin interface
- Select any book and go to the book info page
- Try to fill any **wysiwyg** and **textareas** with malicious XSS strings and open the book front page of that book to see the safe sanitized values printed
- TIP you can use the following XSS Filter Evasion Cheat Sheet
- You can try to test any input field metabox in the book info with the previous step, those values are already being properly escaped in the cover front page

Notes

Two tests were added

Functional test

Unit test

`Improved sanitization function` 1cc4704

arzola changed the title ~~Improved sanitization function~~ **Fixed XSS security vulnerability** on Jan 12, 2021

`Fixed lint` a3b1b90

codecov bot commented on Jan 12, 2021 • edited

Codecov Report

> Merging #2072 (d637867) into dev (b266952) will **increase** coverage by 0.01% .
> The diff coverage is 87.50% .

```
@@             Coverage Diff              @@
##                dev    #2072      +/-   ##
============================================
+ Coverage     67.73%   67.75%   +0.01%
  Complexity     4907     4907
============================================
  Files           128      128
  Lines         21190    21198       +8
============================================
+ Hits          14354    14362       +8
  Misses         6836     6836
```

`Test improved coverage` fd7f5e7

SteelWagstaff commented on Jan 12, 2021 — Member

@arzola will you add a reference to the issue addressed by this PR in the PR description as well as any information the reviewer/tester might need to review/test this PR? See pressbooks/pressbooks-lti-provider-1p3#126 or #2070 for two previous examples.

👍 1

SteelWagstaff requested a review from **richard015ar** 2 years ago

SteelWagstaff changed the title ~~Fixed XSS security vulnerability~~ **Fix XSS security vulnerability** on Jan 12, 2021

arzola commented on Jan 13, 2021 — Contributor Author

@SteelWagstaff @richard015ar I added the description I think now it's ready for review, thanks 👍

👍 1

richard015ar reviewed on Jan 13, 2021

View changes

`inc/sanitize/namespace.php` Outdated — Show resolved

arzola added 3 commits 2 years ago

- `Simplify condition` — `3b9bb4b`
- `Added two more assertions to increase coverage` — `94604fc`
- `Fixed test assertions` — ✓ `d637867`

richard015ar self-requested a review 2 years ago

richard015ar approved these changes on Jan 13, 2021

View changes

richard015ar left a comment — Contributor

LGTM! thank you Oscar!

🎉 1

richard015ar merged commit **`941a8c5`** into `dev` on Jan 13, 2021

richard015ar deleted the `pb-404-xss-fix` branch 2 years ago

Reviewers

richard015ar ✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants