New issue

Jump to bottom

fix: escape invalid lang characters (XSS) #14

Merged **valeriangalliat** merged 1 commit into `valeriangalliat:master` from `ooooooo-q:fix/escape` on Nov 15, 2020

Conversation 3 Commits 1 Checks 0 Files changed 2

ooooooo-q commented on Nov 14, 2020 Contributor

I found XSS in inline code highlighting.

Example

```
`console.log(42)`{.">&lt;img onerror=alert(1) src=.>js}
```

Results

```
<p><code class="language-"><img onerror=alert(1) src=.>js"></code></p>
```

Similar problem: jGleitz/markdown-it-prism#137

`fix: escape invalid lang characters` 4f7b1c7

valeriangalliat commented on Nov 15, 2020 Owner

Good find, thank you!

I'm thinking of tweaking it to escape everything inbetween the `{}` instead, like it was done for the markdown-it-prism issue you linked, something like this (on line 52):

```
const cls = lang ? ` class="${options.langPrefix}${md.utils.escapeHtml(lang)}"` : ''
```

Do you think that would make sense as well?

valeriangalliat merged commit `1f2429c` into `valeriangalliat:master` on Nov 15, 2020

ooooooo-q commented on Nov 15, 2020 Contributor Author

Certainly. If can use `escapeHtml`, it seems better.

ooooooo-q deleted the `fix/escape` branch 2 years ago

valeriangalliat commented on Nov 15, 2020 Owner

👍 the patch is live on 3.3.1, thanks again!

👍 1

minusworld mentioned this pull request on Jan 5, 2021

Fix made in November now absent from code #18

Closed

dependabot bot mentioned this pull request on Mar 13, 2021

Bump markdown-it-highlightjs from 3.3.0 to 3.4.0 hokulea/hokulea#23

Merged

Reviewers

No reviews

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

2 participants