Redmine - Defect #33846

Inline issue auto complete doesn't sanitize HTML tags

2020-08-12 19:29 - Fernando Hartmann

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	4.1.2		
Resolution:	Fixed	**Affected version:**	4.1.1

Description

If referring a issue that have a HTML tag in subject, the tag is rendered as an object in the auto complete tip.

To reproduce

1. Create one issue with a subject like Test <select> tag
2. Start a new issue, go to description field and type issue number created above

Result

- We should display something like Feature #xxxx Test <select> tag
- We display a select object rendered in the tip, like image bellow

tip.png
This can be dangerous,as some one can inject HTML

Related issues:

Related to Redmine - Feature #31989: Inline issue auto complete (#) in fields...	**Closed**

Associated revisions

Revision 20827 - 2021-03-19 05:24 - Go MAEDA

Fix that inline issue auto complete does not sanitize HTML tags (#33846).

Patch by Marius BALTEANU.

Revision 20828 - 2021-03-19 05:37 - Go MAEDA

Merged r20827 from trunk to 4.1-stable (#33846).

History

#1 - 2020-08-14 08:50 - Marius BĂLTEANU

- Assignee set to Marius BĂLTEANU

#2 - 2020-10-05 00:49 - Marius BĂLTEANU

- Related to Feature #31989: Inline issue auto complete (#) in fields with text-formatting enabled added

#3 - 2020-10-05 22:52 - Marius BĂLTEANU

- File sanitize_html.patch added

- Target version set to 4.1.2

Fernando, thanks for catching this.

I've attached a patch to fix this issue.

#4 - 2020-10-05 22:52 - Marius BĂLTEANU

- Assignee deleted (Marius BĂLTEANU)

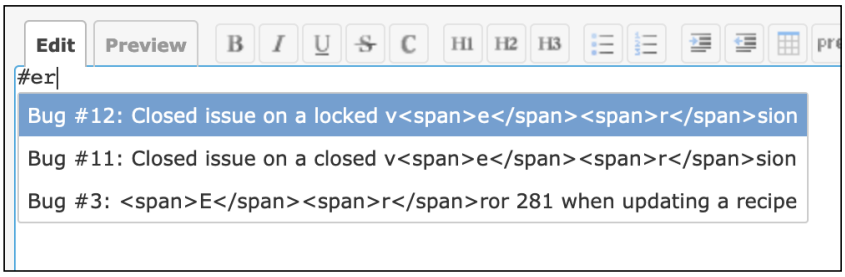
#5 - 2020-10-15 14:02 - Go MAEDA

- File autocomplete-by-title.png added

Marius BALTEANU wrote:

> I've attached a patch to fix this issue.

Thank you for fixing the issue but I see tags when using auto-complete by issue subject.



#6 - 2020-10-16 00:24 - Marius BĂLTEANU

- Assignee set to Marius BĂLTEANU

Thanks for pointing this out, I was able to reproduce the problem. I will post soon a fix.

#7 - 2020-10-16 07:54 - Marius BĂLTEANU

- File sanitize_html_v2.patch added

- File tribute.png added

- Assignee deleted (Marius BĂLTEANU)

Please try this new version, it should work as expected with one mention: the letters that match the search are no longer highlighted.

tribute.png
Also, instead of the sanitzeHTML function, I think it's better to use a library like https://lodash.com/docs/4.17.15#escape, but I'm not sure how to add it without copying the code or by using a module bundler like webpack. @Jean-Philippe, any recommendations on this?

#8 - 2020-10-16 08:01 - Marius BĂLTEANU

- File sanitize_html_v3.patch added

This one works on IE 11 as well.

#9 - 2020-12-05 18:03 - Marius BĂLTEANU

Attached is a test for this issue that can be applied only after #34123 is committed.

#10 - 2020-12-05 18:05 - Marius BĂLTEANU

- File test_for_26089.patch.zip added

#11 - 2020-12-05 18:07 - Marius BĂLTEANU

- File deleted (test_for_26089.patch.zip)

#12 - 2020-12-05 18:10 - Marius BĂLTEANU

- File test_for_33846.patch added

#13 - 2020-12-16 08:20 - Marius BĂLTEANU

- Assignee set to Jean-Philippe Lang

#14 - 2021-03-15 08:34 - Marius BĂLTEANU

- Assignee changed from Jean-Philippe Lang to Go MAEDA

#15 - 2021-03-15 16:53 - Go MAEDA

- File sanitize_html_v4.patch added

Update the patch for the latest trunk (r20791).

#16 - 2021-03-19 05:43 - Go MAEDA

- Status changed from New to Closed

- Resolution set to Fixed

Committed the fix. Thank you all for your contribution.

#17 - 2021-03-19 05:46 - Go MAEDA

- Subject changed from Inline issue auto complete (#) doesn't sanityze HTML tags to Inline issue auto complete doesn't sanitize HTML tags

#18 - 2021-03-26 01:13 - Holger Just

By the way: this a full-blown XSS vulnerability. With an issue subject such as

```
<span onmouseover="alert('pwned');">This is some exciting text</span>
```

arbitrary Javascript can be executed (as well as arbitrary HTML code shown). In my opinion, the assessment of the issue in Security_Advisories should therefore be increased to High.

#19 - 2021-03-26 08:59 - Marius BĂLTEANU

Holger Just wrote:

> By the way: this a full-blown XSS vulnerability. With an issue subject such as
>
> [...]
>
> arbitrary Javascript can be executed (as well as arbitrary HTML code shown). In my opinion, the assessment of the issue in Security_Advisories should therefore be increased to High.

Thanks Holger, I've changed to High.

Files

tip.png	6.45 KB	2020-08-12	Fernando Hartmann
sanitize_html.patch	868 Bytes	2020-10-05	Marius BĂLTEANU
autocomplete-by-title.png	56.7 KB	2020-10-15	Go MAEDA
sanitize_html_v2.patch	1.01 KB	2020-10-16	Marius BĂLTEANU
tribute.png	132 KB	2020-10-16	Marius BĂLTEANU
sanitize_html_v3.patch	878 Bytes	2020-10-16	Marius BĂLTEANU
test_for_33846.patch	809 Bytes	2020-12-05	Marius BĂLTEANU
sanitize_html_v4.patch	2.18 KB	2021-03-15	Go MAEDA