Defect #33846

Inline issue auto complete doesn't sanitize HTML tags

Added by Fernando Hartmann over 2 years ago. Updated over 1 year ago.

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

Description

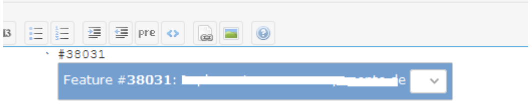
If referring a issue that have a HTML tag in subject, the tag is rendered as an object in the auto complete tip.

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



This can be dangerous,as some one can inject HTML

- tip.png (6.45 KB) Fernando Hartmann, 2020-08-12 19:26
- sanitize_html.patch (868 Bytes) Marius BALTEANU, 2020-10-05 22:51
- autocomplete-by-title.png (56.7 KB) Go MAEDA, 2020-10-15 14:01
- sanitize_html_v2.patch (1.01 KB) Marius BALTEANU, 2020-10-16 07:47
- tribute.png (132 KB) Marius BALTEANU, 2020-10-16 07:49
- sanitize_html_v3.patch (878 Bytes) Marius BALTEANU, 2020-10-16 08:01
- test_for_33846.patch (809 Bytes) Marius BALTEANU, 2020-12-05 18:10
- sanitize_html_v4.patch (2.18 KB) Go MAEDA, 2021-03-15 16:52

Related issues

Related to Redmine - ~~Feature #31989~~: Inline issue auto complete (#) in fields with text-format...	Closed			

History

Updated by Marius BALTEANU over 2 years ago #1

- **Assignee** set to *Marius BALTEANU*

Updated by Marius BALTEANU about 2 years ago #2

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

Updated by Marius BALTEANU about 2 years ago #3

- **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.

Updated by Marius BALTEANU about 2 years ago #4

- **Assignee** deleted (~~*Marius BALTEANU*~~)

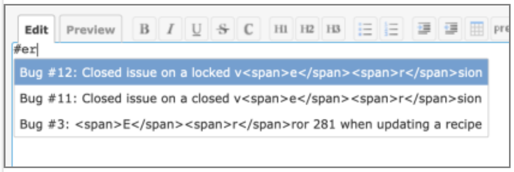
Updated by Go MAEDA about 2 years ago #5

- **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 `<span>` tags when using auto-complete by issue subject.



#er

Bug #12: Closed issue on a locked v<span>e</span><span>r</span>sion

Bug #11: Closed issue on a closed v<span>e</span><span>r</span>sion

Bug #3: <span>E</span><span>r</span>ror 281 when updating a recipe

Updated by Marius BALTEANU about 2 years ago #6

- **Assignee** set to *Marius BALTEANU*

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

Updated by Marius BALTEANU about 2 years ago #7

- **File** sanitize_html_v2.patch added
- **File** tribute.png added
- **Assignee** deleted (~~*Marius BALTEANU*~~)

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

Associated revisions

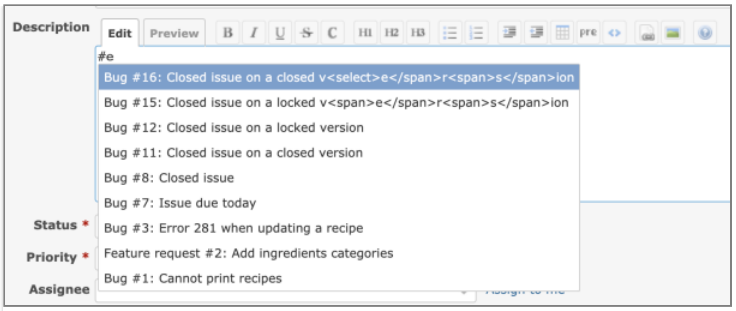
Revision 20827
Added by Go MAEDA over 1 year ago

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

Patch by Marius BALTEANU.

Revision 20828
Added by Go MAEDA over 1 year ago

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



#e

Bug #16: Closed issue on a closed v<select>e</span>r<span>s</span>ion
Bug #15: Closed issue on a locked v<span>e</span>r<span>s</span>ion
Bug #12: Closed issue on a locked version
Bug #11: Closed issue on a closed version
Bug #8: Closed issue
Bug #7: Issue due today
Bug #3: Error 281 when updating a recipe
Feature request #2: Add ingredients categories
Bug #1: Cannot print recipes

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?

Updated by **Marius BALTEANU about 2 years** ago **#8**

- **File** sanitize_html_v3.patch added

This one works on IE 11 as well.

Updated by **Marius BALTEANU about 2 years** ago **#9**

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

Updated by **Marius BALTEANU about 2 years** ago **#10**

- **File** *test_for_26089.patch.zip* added

Updated by **Marius BALTEANU about 2 years** ago **#11**

- **File** deleted (~~*test_for_26089.patch.zip*~~)

Updated by **Marius BALTEANU about 2 years** ago **#12**

- **File** test_for_33846.patch added

Updated by **Marius BALTEANU about 2 years** ago **#13**

- **Assignee** set to *Jean-Philippe Lang*

Updated by **Marius BALTEANU almost 2 years** ago **#14**

- **Assignee** changed from *Jean-Philippe Lang* to *Go MAEDA*

Updated by **Go MAEDA almost 2 years** ago **#15**

- **File** sanitize_html_v4.patch added

Update the patch for the latest trunk (r20791).

Updated by **Go MAEDA over 1 year** ago **#16**

- **Status** changed from *New* to *Closed*
- **Resolution** set to *Fixed*

Committed the fix. Thank you all for your contribution.

Updated by **Go MAEDA over 1 year** ago **#17**

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

Updated by **Holger Just over 1 year** ago **#18**

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.

Updated by **Marius BALTEANU over 1 year** ago **#19**

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.