Redmine - Defect #22115

Text in the "removed" part of a wiki diff is double-escaped

2016-02-25 21:00 - Felix Schäfer

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	UI	**Estimated time:**	0.00 hour
Target version:	3.3.0		
Resolution:	Fixed	**Affected version:**	

Description

In a wiki diff (and from the looks of the code the diffs of issue description) html special characters in the deleted parts are double-escaped.

Associated revisions

Revision 15287 - 2016-03-26 11:20 - Jean-Philippe Lang

Text in the "removed" part of a diff is double-escaped (#22115).

Patch by Felix Schäfer.

History

#1 - 2016-02-25 21:08 - Felix Schäfer

- File 22115-dont_double_escape_deleted_diff_parts.diff added

The attached diff adds a test and a diff for this behaviour.

The problem is in source:/trunk/lib/redmine/helpers/diff.rb@15153: the string deleted is concatenated from unsafe strings (lines 46 and 55) and an html escaped string (line 56) and thus html unsafe. It then is added + to an html_safe string in line 65, which causes deleted to be html escaped a second time before being concatenated to the string on the left hand of the +.

The patch moves the explicit html escape to line 65 and keeps the explicit html escape to avoid problems with the implicit html escaping performed by the addition + to a html_safe string.

#2 - 2016-02-25 21:10 - Felix Schäfer

Felix Schäfer wrote:

> The patch moves the explicit html escape to line 65 and keeps the explicit html escape to avoid problems with the implicit html escaping performed by the addition + to a html_safe string.

Ah, and the .join(' ').html_safe at the end is replaced with the safer safe_join which ensures any non-html_safe string in the array is html escaped before concatenation.

#3 - 2016-02-25 21:32 - Felix Schäfer

- File 22115-dont_double_escape_deleted_diff_parts.diff added

safe_join comes from an ActionView::Helper that wasn't included yet in Redmine::Helpers::Diff, this patch corrects this omission.

#4 - 2016-03-26 04:26 - Toshi MARUYAMA

- Target version set to 3.3.0

#5 - 2016-03-26 11:20 - Jean-Philippe Lang

- Subject changed from Text in the "removed" part of a diff is double-escaped to Text in the "removed" part of a wiki diff is double-escaped

- Status changed from New to Closed

- Assignee set to Jean-Philippe Lang

- Resolution set to Fixed

Committed, thanks.

Files

22115-dont_double_escape_deleted_diff_parts.diff	2.07 KB	2016-02-25	Felix Schäfer
22115-dont_double_escape_deleted_diff_parts.diff	2.35 KB	2016-02-25	Felix Schäfer