

Redmine - Defect #22967

Special character like quote breaks wiki links

2016-06-02 17:35 - Philippe Le Brouster

Status: Closed	Start date:
Priority: Normal	Due date:
Assignee: Jean-Philippe Lang	% Done: 0%
Category: Wiki	Estimated time: 0.00 hour
Target version: 4.0.0	Affected version: 3.2.2
Resolution: Fixed	

Description

Affected version: 3.1.5, 3.2.2, at least

To reproduce:

- create a new wiki page
- insert a link with a quote inside. For ex. : `[[This is a link'test]]`

Explanation:

I'm trying to upgrade redmine from 2.4.2 to 3.1.5 (or 3.2.2) and I've an issue with the wiki links.

With the version 2.4.2, using quote "" in the wiki links was working (using the `redmine_redcarpet_formatter`).

For example :

```
[[This is a link'test]]
```

With the version 3.1.5 or 3.2.2 the same code break the wiki link during html formatting. The output is something like

```
This is a link&
```

I suspect there is a problem during the text escaping because the function `parse_wiki_links` in `app/helpers/application_helper` consider that there is an anchor. The supposed anchor come from the html escaped form of the quote (which is `'`).

In French language, this is a major problem because the quote character is often used.

Regards,
Philippe Le Brouster.

Related issues:

Duplicated by Redmine - Defect # 10413: Creating wiki pages with special char...	Closed
Duplicated by Redmine - Defect # 11985: Version Wiki page '#' gets escaped	Closed

Associated revisions

Revision 17490 - 2018-09-15 11:11 - Jean-Philippe Lang

Special character like quote breaks wiki links (#22967).

Patch by Marius BALTEANU.

History

#1 - 2016-06-22 16:51 - Toshi MARUYAMA

- File `link.png` added

I cannot reproduce on vanilla Redmine version:3.2.3 ruby 1.9.3p551 (2014-11-13 revision 48407) [x86_64-linux].

link.png

#2 - 2016-06-22 16:52 - Toshi MARUYAMA

- Status changed from New to Needs feedback

#3 - 2016-06-23 14:56 - Philippe Le Brouster

- File *wiki_edit.png* added

- File *wiki_content.png* added

Hi,

The problem exists only with the markdown text format. The textile format is ok.

Did you test with this markdown text format ?

I've just set a vanilla redmine 3.2.3 (tarball from the website). And I can reproduce this bug.

wiki_edit.png

wiki_content.png

Regards,

Philippe Le Brouster

#4 - 2016-07-04 07:51 - Toshi MARUYAMA

- Subject changed from *Special character like ' (quote) breaks wiki links* to *markdown: special character like ' (quote) breaks wiki links*

- Status changed from Needs feedback to New

#5 - 2016-07-17 09:01 - Adrien Crivelli

I am also affected by this bug on Redmine 3.0.0.

I'd say it should be quite high on the priority list, because it will break things for a lot of french users, and possibly other languages too. But it will also break in English, as seen in those examples:

Markdown input:

[[Jack & Coke]]

[[a "quoted" name]]

[[le français, c'est super]]

[[broken < less]]

[[broken > more]]

[[also <broken> link]]

Actual output:

Jack & Coke
a "quoted" name
le français, c&
broken < less
broken > more
also link

Expected output:

Jack & Coke
a "quoted" name
le français, c'est super
broken < less
broken > more
also broken link

#6 - 2018-03-31 15:02 - Marius BALTEANU

- *File tests_for_special_characters_breaks_wiki_links.patch added*

I made some tests based on the first 5 examples added by Adrien Crivelli in his post. The tests fail on both Textile and Markdown formatters.

#7 - 2018-03-31 15:17 - Marius BALTEANU

- *File fix_for_22967.patch added*

I made also a potential patch that fixes these issues. I'm saying just potential because I'm not sure if it is ok from a security point of view. From my tests it is ok, but I need a second opinion.

Regarding the case "[[also <broken> link]]", is harder to make a fix because the tag is completely removed by the markdown formatter.

#8 - 2018-03-31 15:23 - Marius BALTEANU

- *Status changed from New to Confirmed*

#9 - 2018-05-14 23:57 - Marius BALTEANU

- *Duplicated by Defect #10413: Creating wiki pages with special characters may be problematic added*

#10 - 2018-05-15 00:36 - Marius BALTEANU

- *Target version set to Candidate for next minor release*

I'm considering this issue quite annoying and I would like to fix it in a next version. @Go Maeda, which version do you think is more appropriate?

#11 - 2018-05-19 09:36 - Go MAEDA

Marius BALTEANU wrote:

| *I'm considering this issue quite annoying and I would like to fix it in a next version. @Go Maeda, which version do you think is more appropriate?*

I think 4.0.0 is preferable to minor releases because it requires some manual work to backport the tests to 3.4/3.3-stable.

#12 - 2018-05-19 12:09 - Marius BALTEANU

- Target version changed from Candidate for next minor release to 4.1.0

#13 - 2018-05-21 02:03 - Go MAEDA

- Assignee set to Go MAEDA

#14 - 2018-05-22 12:55 - Go MAEDA

- File `fix_for_22967-v2.diff` added

Update the patch for r17346.

#15 - 2018-05-22 23:41 - Go MAEDA

- Assignee changed from Go MAEDA to Marius BALTEANU

The following patch also works. Marius, do you think it is OK? I prefer this code because it is simpler and `CGI.unescapeHTML` is already used in `application_helper.rb`.

Index: `app/helpers/application_helper.rb`

=====

--- `app/helpers/application_helper.rb` (revision 17346)

+++ `app/helpers/application_helper.rb` (working copy)

@@ -740,6 +740,7 @@

link_project = project

esc, all, page, title = \$1, \$2, \$3, \$5

if esc.nil?

+ page = CGI.unescapeHTML(page)

if page =~ /^#\(.+\)\$/

anchor = sanitize_anchor_name(\$1)

url = "#{anchor}"

#16 - 2018-06-10 20:50 - Marius BALTEANU

- Assignee deleted (Marius BALTEANU)

LGTM. I'm not sure why I chose then the `htmlentities` gem instead of `CGI`, I think that I've read somewhere that it is better, but I can't find anymore.

Anyway, the single concern I have is regarding how safe are our both solution against XSS, but from my tests, everything looks good. Maybe we should let Jean-Philippe Lang to fix this one.

#17 - 2018-06-11 01:19 - Go MAEDA

- Assignee set to Jean-Philippe Lang

#18 - 2018-06-17 09:10 - Go MAEDA

- Target version changed from 4.1.0 to 4.0.0

#19 - 2018-09-15 11:11 - Jean-Philippe Lang

- Subject changed from markdown: special character like ' (quote) breaks wiki links to Special character like quote breaks wiki links

- Status changed from Confirmed to Closed

- Resolution set to Fixed

Patch committed, thanks.

#20 - 2018-09-16 13:14 - Marius BALTEANU

- Duplicated by Defect #11985: Version Wiki page '#' gets escaped added

Files

link.png	11 KB	2016-06-22	Toshi MARUYAMA
wiki_edit.png	5.87 KB	2016-06-23	Philippe Le Brouster
wiki_content.png	8.63 KB	2016-06-23	Philippe Le Brouster
tests_for_special_characters_breaks_wiki_links.patch	2.31 KB	2018-03-31	Marius BALTEANU
fix_for_22967.patch	965 Bytes	2018-03-31	Marius BALTEANU
fix_for_22967-v2.diff	868 Bytes	2018-05-22	Go MAEDA