

Less-than sign in issue description and comments are not escaped

2022/05/09 15:10 - Admin Redmine

ステータス:	Reopen	開始日:	2010/11/24
優先度:	通常	期日:	
担当者:		進捗率:	0%
カテゴリ:	Text formatting_26	予定工数:	0.00時間
対象バージョン:	Candidate for next major release_32	作業時間:	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/6969	status_id:	8
category_id:	26	tracker_id:	1
version_id:	32	plus1:	0
issue_org_id:	6969	affected_version:	
author_id:	24305	closed_on:	
assigned_to_id:	1	affected_version_id:	25
comments:	6		

説明

When an issue description or comment contains a less-than sign (@<@), this sign is output verbatim in the issue page, instead of being escaped with ampersand-"lt"-semicolon. This causes the issue details page to be invalid XHTML, which is contrary to the page's doctype, and makes it impossible to read the page with an XML parser. I created "an issue on the demo site": <http://demo.redmine.org/issues/38181> to demonstrate the problem.

To reproduce, run @xmllint URL-OF-ISSUE-PAGE@, like this:

```
$ xmllint http://demo.redmine.org/issues/38181
http://demo.redmine.org/issues/38181:166: parser error : StartTag: invalid element name
```

Hm: <

```

      ^
http://demo.redmine.org/issues/38181:241: parser error : StartTag: invalid element name
mg alt="Comment" src="/images/comment.png?1286930539" />
```

And this? <

```
http://demo.redmine.org/issues/38181:330: parser error : Entity 'copy' not defined
PowerRedmine © 2006-2010 Je
```

The third error is a false positive (xmllint doesn't know XHTML entities), but the first two errors are symptoms of this problem.

journals

Thank you for reporting this issue.

Textile formatter in the latest trunk (r14634) is still affected.

Here is a test to catch this issue: attachment:issue6969_test_escaping.diff

Fixed in r14812.

Fix reverted, see #21202.

related_issues

履歴

#1 - 2022/05/10 17:21 - Admin Redmine

- カテゴリを Text formatting_26 にセット

- 対象バージョンを Candidate for next major release_32 にセット