Redmine - Defect #6969
Less-than sign in issue description and comments are not escaped
2010-11-24 18:51 - Magnus Henoch

<table>
<thead>
<tr>
<th>Status:</th>
<th>Reopened</th>
<th>Start date:</th>
<th>2010-11-24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>Jean-Philippe Lang</td>
<td>% Done:</td>
<td>0%</td>
</tr>
<tr>
<td>Category:</td>
<td>Text formatting</td>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Target version:</td>
<td>Candidate for next major release</td>
<td>Affected version:</td>
<td>1.0.3</td>
</tr>
</tbody>
</table>

Description
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 to demonstrate the problem.

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

```bash
$ xmllint http://demo.redmine.org/issues/38181
```

http://demo.redmine.org/issues/38181:166: parser error : StartTag: invalid element name
<Hp: Hmm: <<=p>
  ^

mg alt="Comment" src="/images/comment.png?1286930539" /></a></p>And this? <
  ^

http://demo.redmine.org/issues/38181:330: parser error : Entity 'copy' not defined
Powered by a href="http://www.redmine.org/">Redmine</a> &copy; 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.

Related issues:
Related to Redmine - Defect #21202: Left aligned sign in tabular is not worke... Closed

Associated revisions
Revision 14812 - 2015-11-07 11:20 - Jean-Philippe Lang
Fixed that less-than sign is not escaped by textile formatter (#6969).

Revision 14834 - 2015-11-08 09:50 - Jean-Philippe Lang
Merged r14812 (#6969).

Revision 14835 - 2015-11-08 09:50 - Jean-Philippe Lang
Merged r14812 (#6969).

Revision 14836 - 2015-11-08 09:50 - Jean-Philippe Lang
Merged r14812 (#6969).

Revision 14863 - 2015-11-11 08:34 - Jean-Philippe Lang
Reverts r14812 (#6969).

Revision 14864 - 2015-11-11 08:35 - Jean-Philippe Lang
Merged r14863 (#6969).

Revision 14865 - 2015-11-11 08:35 - Jean-Philippe Lang
Merged r14863 (#6969).
Revision 14866 - 2015-11-11 08:35 - Jean-Philippe Lang
Merged r14863 (#6969).

Revision 14867 - 2015-11-11 08:39 - Jean-Philippe Lang
Adds a test for #21202 (#6969).

History
#1 - 2015-10-01 10:34 - Go MAEDA
- File issue6969_test_escaping.diff added
- Category changed from Issues to Security
- Status changed from New to Confirmed
- Private changed from No to Yes

Thank you for reporting this issue.

Textile formatter in the latest trunk (r14634) is still affected.
Here is a test to catch this issue: issue6969_test_escaping.diff

#2 - 2015-10-22 09:11 - Toshi MARUYAMA
- Target version set to 2.6.8

#3 - 2015-11-07 11:21 - Jean-Philippe Lang
- Category changed from Security to Text formatting
- Status changed from Confirmed to Resolved
- Assignee set to Jean-Philippe Lang
- Private changed from Yes to No
- Resolution set to Fixed

Fixed in r14812.

#4 - 2015-11-08 09:51 - Jean-Philippe Lang
- Status changed from Resolved to Closed

#5 - 2015-11-11 08:33 - Jean-Philippe Lang
- Related to Defect #21202: Left aligned sign in tabular is not worked since applying #6969 added

#6 - 2015-11-11 08:39 - Jean-Philippe Lang
- Status changed from Closed to Reopened
- Target version changed from 2.6.8 to Candidate for next major release

Fix reverted, see #21202.

Files
issue6969_test_escaping.diff 576 Bytes 2015-10-01 Go MAEDA