Redmine - Patch #16087

Markdown renderer doesn’t clean HTML properly

2014-02-13 03:43 - Charmander -

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Text formatting	**Estimated time:**	0.00 hour
Target version:			

Description

The current renderer strips HTML (contrary to conventional Markdown) and still fails to catch everything:

```
[bad link](javascript:alert(1\))
```

This fixes both behaviours. scrub-classes is a patch to remove unrecognized classes that could potentially be used to annoy; I haven’t completed the list because the existing implementation already allows all classes through syntax highlighting:

```
~~~any-class-here
code block
~~~
```

History

#1 - 2014-02-13 03:45 - Charmander -

- File redmine-markdown-scrub-classes.diff added

This one needs a more comprehensive list of acceptable classes.

#2 - 2014-06-13 01:32 - Charmander -

ahem

#3 - 2014-06-13 02:27 - Toshi MARUYAMA

Please add tests.
source:trunk/test/unit/lib/redmine/wiki_formatting/markdown_formatter.rb

#4 - 2014-06-14 01:09 - Charmander -

Yes, one is already included in that patch.

#5 - 2014-06-14 02:59 - Toshi MARUYAMA

Please add test cases in your patch.

#6 - 2014-06-14 04:27 - Charmander -

Like I said, the patch includes a test case.

#7 - 2014-07-29 18:07 - Charmander -

ahem

#8 - 2015-05-08 04:26 - Charmander -

Okay, I’ve added tests to my patch.

#9 - 2019-02-07 05:26 - Go MAEDA

- Status changed from New to Closed

Current versions of Redmine don't render [bad link](javascript:alert(1\)). And code blocks don't accept unknown language name (r16501 and r16502).

Files

redmine-markdown-loofah.diff	2.42 KB	2014-02-13	Charmander -
redmine-markdown-scrub-classes.diff	1.53 KB	2014-02-13	Charmander -