Redmine - Defect #22897
Leaving HTML tags in collapse macro instead of showing html_safe formatted text

2016-05-25 13:07 - Aleksandar Pavic

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Wiki	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Invalid	**Affected version:**	

Description

If a HTML content like <h1> for example is added to collapse macro, tags are displayed instead of html formatting it:

```
{{collapse
<h1>This is a block of text that is collapsed by default.</h1>
It can be expanded by clicking a link.
}}
```

And the output looks like:{{collapse
<h1>This is a block of text that is collapsed by default.</h1>
It can be expanded by clicking a link.
}}

While it should be:
Screenshot_12.png

Attached is also diff file to make it work as I suggested in this ticket.

History

#1 - 2016-05-25 13:29 - Gregor Schmidt

I have just tested your patch. Unfortunately this change, makes Redmine subject to XSS attacks. Consider the following Textile code:

```
{{collapse
<script>alert(1)</script>
It can be expanded by clicking a link.
}}
```

With your patch applied, the content of the script block is executed. An attacker, with permissions limited to writing comments or wiki pages, could create a malicious page containing this macro and wait for an admin to visit it. They could then hijack the admin session and do whatever they want without any restrictions.

To prevent such an attack, the HTML code is escaped.

#2 - 2016-05-25 13:55 - Aleksandar Pavic

I see html_safe actually does not do stripping of unsafe HTML tags...

So then probably it should be a feature with some ruby lib for filtering,
actuall html filter like: https://github.com/rails/rails-html-sanitizer

#3 - 2016-05-25 14:12 - Gregor Schmidt

Since the content of the collapse block is passed through textile filters, you could achieve the same result using textile syntax. This will be safe against XSS attacks and should already be familiar to Redmine users.

Code:

```
{{collapse
h1. This is a block of text that is collapsed by default.

It can be expanded by clicking a link.
}}
```

Result:

{{collapse
h1. This is a block of text that is collapsed by default.

It can be expanded by clicking a link.
}}

#4 - 2016-05-31 10:57 - Jan from Planio www.plan.io

- Status changed from New to Closed
- Resolution set to Invalid
- Affected version deleted (3.2.0)

Agree with Gregor.

Files

Screenshot_12.png	9.81 KB	2016-05-25	Aleksandar Pavic
macross.diff	800 Bytes	2016-05-25	Aleksandar Pavic