Foreman - Bug #6858

HTML tags should be escaped when we update any parameter value under settings tab

07/31/2014 05:28 AM - Dominic Cleal

Status:	Closed		
Priority:	Normal		
Assignee:	Amir Fefer		
Category:	Settings		
Target version:	1.11.1		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1125181	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/3264		

Description

Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1125181
Description of problem:
I was trying to update parameter defined under settings tab and I was able to update it with HTML tags and those tags should be escaped properly.

For example, I updated 'administrator' parm value with :foo

And UI shows me a link to 'foo'. Please see the screenshot.

Please note that UI doesn't escaped the HTML tags immediately after updating the value. But once you navigate away from settings page to other and get back then it will be escaped.

Version-Release number of selected component (if applicable):
sat6 GA snap1

How reproducible:
always

Steps to Reproduce:
1. pick any parameter which open a text box to update its value
2. edit the value with html tags like: foo
3. save it

Actual results:
UI doesn't escaped the HTML tags immediately after updating the value. But once you navigate away from settings page to other and get back then it will be escaped.

Expected results:
HTML tags should be escaped as soon as you save the parameter value

Additional info:
similar issue with other parameter "email_reply_address"

Associated revisions

Revision e108822a - 03/06/2016 02:28 AM - Amir Fefer

Fixes #6858 - escape HTML tags when update a parameter value in settings

Revision 42e29a0f - 04/18/2016 01:45 PM - Amir Fefer

Fixes #6858 - escape HTML tags when update a parameter value in settings

(cherry picked from commit e108822a1a3ab567ea17d733754ccc9c9447dc8a)

History

#1 - 07/31/2014 05:38 AM - Dominic Cleal

- Category set to Settings

I don't believe this has a security impact, as it's only shown to the user that updates the value. The value gets escaped when it's rendered - including if it's updated via the API.

#2 - 01/18/2015 08:39 AM - Tom Caspy

+1 on dominic's conclusion - there's no security issue here. I say we close this.

#3 - 01/19/2015 03:50 AM - Dominic Cleal

It's valid, so it can stay open.

#4 - 02/29/2016 10:12 AM - Amir Fefer

- Assignee set to Amir Fefer

#5 - 03/01/2016 02:59 PM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/3264 added

#6 - 03/06/2016 03:01 AM - Amir Fefer

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset e108822a1a3ab567ea17d733754ccc9c9447dc8a.

#7 - 03/07/2016 03:46 AM - Dominic Cleal

- translation missing: en.field_release set to 141