Foreman - Bug #12698

Insufficient URL validation for smart proxy and medium

12/04/2015 04:39 AM - Daniel Lobato Garcia

Status:	Closed		
Priority:	Normal		
Assignee:	Daniel Lobato Garcia		
Category:	Security		
Target version:	1.11.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/2960		

Description

Problem: The regex that validates smart proxies URLs only matches 'beginning of text'. This allows us to add just \n after a valid URL and put anything after it. For instance, javascript:alert('hacked'). I haven't found any link to the Foreman proxy URL so the script would not trigger, but if we were to put link_to @smart_proxy.url somewhere (or a plugin did this) it would be unsafe.

Solution: Make the regex match the end of the URL with \Z

Related issues:

Related to Foreman - Feature #12787: The url validator accepts bad urls like ...	**New**	**12/11/2015**
Has duplicate Foreman - Bug #12697: Insufficient validation for smart proxy URL	**Duplicate**	**12/04/2015**

Associated revisions

Revision 98f6ca54 - 12/11/2015 09:06 AM - Daniel Lobato Garcia

Fixes #12698 - Insufficient URL validation Smart Proxy and Medium.

Problem: The regex that validates smart proxies URLs only matches 'beginning of text'. This allows us to add just \n after a valid URL and put anything after it. For instance, javascript:alert('hacked'). I haven't found any link to the Foreman proxy URL so the script would not trigger, but if we were to put link_to @smart_proxy.url somewhere (or a plugin did this) it would be unsafe. Same problem occurrs on Medium path.

Solution: Make the regex match the end of the URL with \Z. I substituted the regex by an standard one, URI.regexp so we don't have to maintain it anymore.

Extra: I added one test for this, but other tests have been rearranged to use stubs rather than building actual SmartProxy objects & associations.

History

#1 - 12/04/2015 04:48 AM - Dominic Cleal

- Has duplicate Bug #12697: Insufficient validation for smart proxy URL added

#2 - 12/04/2015 05:52 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/2960 added

#3 - 12/10/2015 07:42 AM - Daniel Lobato Garcia

- Subject changed from Insufficient validation for smart proxy URL to Insufficient URL validation for smart proxy and medium

#4 - 12/11/2015 09:07 AM - Dominic Cleal

- Category set to Security

- translation missing: en.field_release set to 71

#5 - 12/11/2015 10:01 AM - Daniel Lobato Garcia

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 98f6ca54bd689c2df59cedb41d724f6e7c19a83f.

#6 - 12/11/2015 02:56 PM - David Davis

- Related to Feature #12787: The url validator accepts bad urls like "https://" added