Foreman - Bug #7483
CVE-2014-3653 - Provisioning Templates Preview mode strips out text like <<FOO

| Status:     | Closed              |
| Priority:   | Normal              |
| Assignee:   | Aaron Stone         |
| Category:   | Security            |
| Target version: | 1.6.1         |
| Difficulty: |                     |
| Pull request: | https://github.com/theforeman/foreman/pull/1778 |
| Triaged:    |                     |
| Bugzilla link: | Found in Releases: 1.6.0 |

Description
I have Foreman 1.5.1. I will try to test this against 1.5.2 and 1.6.0, but if someone else can test it first that would be grand.

Steps to reproduce:

In Provisioning Templates, click New Template.
Put this into the code box:

```shell
test <<FOO > bar
Hello World
FOO
```
click Preview
click Code

Now the contents are:
```shell
test < bar
Hello World
FOO
```

That's a pretty big problem for templates that want to use shell redirection!

Related issues:
Related to Foreman - Bug #8133: template diffs don't get displayed anymore

```plaintext
Revision cafa9477 - 09/24/2014 06:08 AM - Aaron Stone
Fixes #7483 - Use hidden input value to hold raw template contents (CVE-2014-3653)
```

```plaintext
Revision 159499bd - 10/07/2014 08:15 AM - Aaron Stone
Fixes #7483 - Use hidden input value to hold raw template contents (CVE-2014-3653)
(cherry picked from commit cafa94774b18d54304f031bbf4f7d1a15fc87b3d)
```

History
#1 - 09/16/2014 08:03 PM - Aaron Stone

Tested, this does affect Foreman 1.5.2 and 1.6.0.
I posted screenshots of this bug in action here: https://github.com/sodabrew/foreman/issues/1
Thanks for the report. This has a security impact as it seems to be rendered as HTML, we're getting a CVE assigned. Please go ahead and submit your fix, we'll get it into 1.6.1.

#3 - 09/18/2014 07:15 AM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/1777 added
- Pull request deleted ()

#4 - 09/18/2014 08:09 AM - Dominic Cleal
- Pull request https://github.com/theforeman/foreman/pull/1778 added
- Pull request deleted (https://github.com/theforeman/foreman/pull/1777)

#5 - 09/22/2014 03:06 AM - Dominic Cleal
- Subject changed from Provisioning Templates Preview mode strips out text like <<FOO to CVE-2014-3653 - Provisioning Templates Preview mode strips out text like <<FOO

#6 - 09/24/2014 07:01 AM - Aaron Stone
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset cafaf7774b18d54304031bbf4f7d1a15fc87b3d.

#7 - 10/28/2014 10:20 AM - Michael Moll
- Related to Bug #8133: template diffs don't get displayed anymore added