

RhodeCode CE/EE - Bug #2264

New user password change doesn't actually require a password change.

27.07.2015 17:22 - Greg Gauthier

Status:	Resolved	Start date:	27.07.2015
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:	v4.4	Spent time:	0.00 hour
Sorting:		Affected Version:	
Commit Number:			

Description

When creating a new user, if you select "password change" checkbox to force a password change on the first login, the user will be prompted appropriately, but he doesn't actually have to supply a different password. It can be the exact same password he first logged on with.

In fact, if you go to @_admin/my_account/password@ after logging in, and execute a change of password, you can put the same password in all three fields, and it will be successful. Its as though we're not doing any checking at all.

Some thoughts I have:

1. If we're going to include a "force change" for new users, it should actually *force* a change, and not allow me to simply use the same password over again.
2. For password changes on a logged in user:
 - a. If we don't care that it's the same password, then we should simply offer a field for the new password, because the old one doesn't really matter.
 - b. If we DO care that it's the same, then we should be checking, just like on new user logins.

What do you guys think?

History

#1 - 25.08.2015 21:55 - Johannes Bornhold

I would narrow down the scope of this problem to only address the "force password change" part.

#2 - 16.03.2016 15:49 - Marcin Kuzminski [CTO]

- Private changed from No to Yes

#3 - 21.06.2016 17:27 - Marcin Kuzminski [CTO]

- Target version set to v4.3

#4 - 26.07.2016 13:29 - Marcin Kuzminski [CTO]

- Target version changed from v4.3 to v4.4

#5 - 05.08.2016 00:49 - Marcin Kuzminski [CTO]

- Private changed from Yes to No

#6 - 05.08.2016 03:31 - Daniel D

Should never allow password changes without entering a current password for the case when a bad party finds a logged in user and can change the password. In fact this should also probably be done to email as well since it can be used to reset the password via 'forgot password' functionality.

#7 - 05.08.2016 05:58 - Redmine Integration

pullrequest created, <https://internal-code.rhodecode.com/rhodecode-enterprise-ce/pull-request/2532>, (status: under_review)

#8 - 08.08.2016 11:35 - Daniel D

- Status changed from New to In Progress

#9 - 12.08.2016 16:01 - Redmine Integration

- Status changed from In Progress to Resolved

Commit <https://internal-code.rhodecode.com/rhodecode-enterprise-ce/changeset/a92da8f244901a192e22530d3a8190a09dd4fef8> changed this issue

#10 - 12.08.2016 16:01 - Redmine Integration

pullrequest merged, <https://internal-code.rhodecode.com/rhodecode-enterprise-ce/pull-request/2532>, (status: approved)