Redmine - Feature #25253

Password reset should count as a password change for User#must_change_passwd

2017-03-03 11:07 - Felix Schäfer

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	3.4.0		
Resolution:	Fixed		

Description

Currently resetting the password through the "forgotten password" feature will not also reset the "must change password" attribute for users. This means users will sometimes reset their password and have to change their password again just after that when logging in.

The following patch would enforce the password change and reset the "must change password" attribute for users. This can not be used for a brute force attack on a user's password as that would require to know a user's password reset token, and if an attacker gets to know a user's password reset token he wouldn't need to brute force the password as he can set it to another password known to him.

```
diff --git a/app/controllers/account_controller.rb b/app/controllers/account_controller.rb
index 54a29fbf4..0aac5c1eb 100644
--- a/app/controllers/account_controller.rb
+++ b/app/controllers/account_controller.rb
@@ -80,7 +80,11 @@ class AccountController < ApplicationController
         return
       end
       if request.post?
+        if @user.must_change_passwd? && @user.check_password?(params[:new_password])
+          flash.now[:error] = l(:notice_new_password_must_be_different)
+        else
         @user.password, @user.password_confirmation = params[:new_password], params[:new_password
_confirmation]
+        @user.must_change_passwd = false
         if @user.save
           @token.destroy
           Mailer.password_updated(@user)
@@ -88,6 +92,7 @@ class AccountController < ApplicationController
           redirect_to signin_path
           return
         end
+        end
       end
       render :template => "account/password_recovery"
       return
```

Another possibility would also be to only reset the "must change password" attribute of the user if the password given during the password reset is not the same as the "previous"/current password, thus requiring the user to change his/her password if the password given during the password reset did not effectively change the password, but I think I like enforcing the password change on password reset better.

Associated revisions

Revision 16374 - 2017-03-05 10:16 - Jean-Philippe Lang

Password reset should count as a password change for User#must_change_passwd (#25253).

Patch by Felix Schäfer.

Revision 16375 - 2017-03-05 10:16 - Jean-Philippe Lang

Adds tests for #25253.

History

#1 - 2017-03-03 21:32 - Jean-Philippe Lang

- Category set to Accounts / authentication

- Target version set to 3.4.0

#2 - 2017-03-05 10:17 - Jean-Philippe Lang

- Status changed from New to Closed

- Assignee set to Jean-Philippe Lang

- Resolution set to Fixed

The first solution sounds good to me. It's committed with tests, thanks.

#3 - 2017-03-05 10:21 - Felix Schäfer

Looks good, thanks!