ChiliProject - Feature # 1123: Introduce PBKDF2 password hashes

Status:	Open	**Priority:**	Normal
Author:	Holger Just	**Category:**	User accounts
Created:	2012-08-21	**Assignee:**	
Updated:	2012-08-21	**Due date:**	
Remote issue URL:			
Affected version:			

Description:

Currently, ChiliProject stores passwords hashed as @SHA1(salt + SHA1(password))@. This schema is not very safe towards brute force attacks, even more so when the whole database gets missing in action.

By introducing PBKDF2, we are able to store the passwords much more securely and are even able to later adjust the complexity factor when computers get faster again.

Gregor Schmidt started a plugin implementing this at "Github":https://github.com/schmidt/chiliproject_safe_password_hashes. I'd like to pull this into the core when the following additional functionality is provided:

* a way to migrate existing hashes to the new format "on-thy-fly", i.e. during user login when we have the clear-text password
* a way to expire passwords to enforce renewal of the password or alternatively a way to migrate the password hashes without requiring the clear-text password.

Associated revisions

2008-04-28 10:52 am - Jean-Philippe Lang

Translation updates (closes #1123, #1124):

* Spanish (Gumer Coronel)

* Norvegian (Kai Olav Fredriksen)

git-svn-id: http://redmine.rubyforge.org/svn/trunk@1367 e93f8b46-1217-0410-a6f0-8f06a7374b81

History