Redmine - Feature #10966

[SECURITY] Project Managers should not be able to choose an URL for a local repository

2012-05-18 17:03 - Alexandre VIAL-BOUKOBZA

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	SCM	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Duplicate		

Description

Hello,

First, thanks to all contributors of redmine as it's a very powerful project management platform !

Now the subjet :)

Here is a list of reasons why repository path (for local repos) should not be choosen at project level:

- People who has access to the repository configuration menu of a project can declare any local repository whatever the path (for exemple outside /var/repos). It means you can access at least with read privilege on any apache served repository.
- Any project manager can declare any repository even one of his own. because security is at Apache level and all repositories are owned by apache user, he should be able to commit on any repository or at least to see his content on redmine.

I think defining a repository base path (for each repository type) from the admin panel for local repos and prevent any repository declaration outside this base path should secure the first point.

For the second one, why not preventing the manager from choosing the repos name which could be the project identifier ? For any extra repository, just concatenate project id with a definable repository id (projectid.repositoryid) as it's already on Redmine.pm for permissions validation.

Of course, no such limitations for remote repos as there is no security by-pass.

What do you think about it ?

Related issues:

Has duplicate Redmine - Defect #18159: Security issue when using local reposi...	**Closed**	
Is duplicate of Redmine - Feature #1415: Let system administrator limit repos...	**Closed**	**2008-06-09**

History

#1 - 2012-06-09 14:08 - Andriy Lesyuk

Agree! At least warnings should be added everywhere where possible!

#2 - 2012-11-01 23:57 - Jean-Baptiste Barth

- Tracker changed from Defect to Feature

- Priority changed from High to Normal

It's actually not a defect : things work as intended in the current version, but it seems your use case doesn't fit what's done, which is a bit different.

I agree there could be warnings somewhere about this side of repo management, but let me ask some questions :

- if you don't trust your project managers, why do you give them the permission to manage repositories ? you can perfectly imagine only global administrators can change repository address (that's what I do personnally at work...)
- isn't there any way to protect your repo ? I thought there was an ability to provide a local password, maybe managed through htaccess or something...

#3 - 2014-10-23 00:22 - Jean-Philippe Lang

- Has duplicate Defect #18159: Security issue when using local repositories added

#4 - 2014-11-08 11:57 - Jean-Philippe Lang

- Status changed from New to Closed

- Resolution set to Duplicate

Closing as a dup of #1415 which is addressed for 3.0 by adding configuration settings to limit valid repository path.

#5 - 2014-11-08 11:57 - Jean-Philippe Lang

- Is duplicate of Feature #1415: Let system administrator limit repositories valid sources added