Redmine - Feature #11755
Impersonate user through REST API auth

2012-09-01 15:33 - Vincent Caron

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:	2.2.0		
Resolution:	Fixed		

Description

The following patch implement a 'switch user' feature which lets an admin-level user impersonate any other user in the context of the REST API.

For any API authentication method, it is allowed to either pass a 'su' parameter or a 'X-Redmine-Switch-User' header, which is only considered if the primary auth led to an admin-level user. The expected value is a user 'login' (no ID or API key).

This is currently very useful when linking different applications with Redmine which share the same authentication reference (LDAP in my case), but don't have access to user's credentials (their Redmine API keys or their plain password). I use an admin-level account for every app which wants to talk with Redmine, but this app should ideally lower its privileges to its current user. This feature does just that, without diving into complex SSO problems.

Related issues:

Duplicated by Redmine - Feature # 11551: REST-API: Admine can create time ent...	**Closed**

Associated revisions

Revision 10608 - 2012-10-11 19:07 - Jean-Philippe Lang

Adds an optional X-Redmine-Switch-User header to let admin users swicth user in API calls (#11755).

History

#1 - 2012-09-25 15:08 - Vincent Caron

- Assignee set to Jean-Philippe Lang

#2 - 2012-10-09 21:33 - Jean-Philippe Lang

- Target version set to 2.2.0

Is the parameter option really needed? I'd like to keep the X-Redmine-Switch-User header option only to avoid any clash with other parameters.

#3 - 2012-10-09 21:39 - Jean-Philippe Lang

I think we should handle the case of an invalid username with a specific error response (eg. 412 Precondition Failed seems appropriate).

#4 - 2012-10-09 23:41 - Vincent Caron

- File api-auth-switch-user-v2.patch added

> *Is the parameter option really needed?*

I don't think so, I simply mimicked the api_key implementation which proposed both a param and a header for authentication. I personnaly only use the header way.

> *I think we should handle the case of an invalid username with a specific error response (eg. 412 Precondition Failed seems appropriate).*

Indeed. Right now it will continue as 'admin' which is unsafe.

Find attached a new patch which takes into account those two remarks.

#5 - 2012-10-11 19:10 - Jean-Philippe Lang

- Status changed from New to Closed
- Resolution set to Fixed

Feature added in r10608, thanks.

Patch was slightly refactored and tests were added. A small change was introduced: a 412 response will be returned if the given username exists but is not active (eg. locked).

#6 - 2012-10-11 20:23 - Vincent Caron

Thanks !

I remembered wondering if fetching a user with User.find_by_login() was handling the locked account case and forgot to check.

#7 - 2012-11-05 13:25 - Hannes Meier

this enhancement solves my older ticket #11551 or?
So this can be closed as well i guess
thank you.

#8 - 2012-11-05 13:39 - Jean-Philippe Lang

Hannes Meier wrote:

> *this enhancement solves my older ticket #11551 or?*

Indeed.

Files

api-auth-switch-user.patch	1.74 KB	2012-09-01	Vincent Caron
api-auth-switch-user-v2.patch	1.81 KB	2012-10-09	Vincent Caron