Redmine - Patch #24051

As a non-admin user using API, I want to be able to filter users by their username without getting forbidden exception

2016-10-11 20:36 - Anonymous

Status:	Resolved	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:			

Description

We created an Odoo -> Redmine connector for uploading time spent from Redmine to HR tools in Odoo (https://github.com/savoirfairelinux/connector-redmine/tree/ddufresne_port_to_8_0).

When we call that function from a superuser API key, all works well, but when it is normal user API key, it does return a forbidden exception :

```
redmine_api.user.filter(name="SOMEUSERNAME")
```

I think that to reinforce security by not giving superuser Redmine API key to Odoo would be interesting.

That would be possible by allowing standard Redmine users to use API to filter users by their username instead of throwing an exception.

Related issues:

Related to Redmine - Defect #7773: Only Redmine administrators can get users ...	**New**	**2011-03-04**

History

#1 - 2016-10-11 20:56 - Anonymous

- File 0001-As-a-non-admin-user-using-API-I-want-to-be-able-to-f.patch added

- Status changed from New to Resolved

There is the patch for the development version. Requesting review for implement.

GitHub pull request if its now a thing : https://github.com/redmine/redmine/pull/86

#2 - 2016-10-12 16:57 - Anonymous

- File allowing-nonsuperusers-to-search-users-by-filters-from-api.patch added

#3 - 2016-10-12 17:08 - Anonymous

- File redmine_lte_v3.2_allow-stdusers-filter-users-from-api.patch added

You can use this patch if you have Redmine <= 3.2

#4 - 2016-10-12 17:11 - Anonymous

- File redmine_lt_v3.3_allow-stdusers-filter-users-from-api.patch added

#5 - 2016-10-27 21:54 - Holger Just

When removing the admin requirement on UsersController#index, there need to be the User.visible scope added to the ActiveRecord query in order to only show users which are visible to the current user.

Once this is fixed, I think it is a great idea to have a user listing available. With the now available role-based controls for the user visibility, this should work without negatively affecting privacy.

#6 - 2016-11-02 17:51 - Mitsuhiro Tanino

I think Defect #7773 is trying to solve same problem of this and I posted a patch on that thread.
Could I get a feedback for that patch?

#7 - 2016-11-22 17:49 - Toshi MARUYAMA

- Related to Defect #7773: Only Redmine administrators can get users from REST API added

Files

0001-As-a-non-admin-user-using-API-I-want-to-be-able-to-f.patch	979 Bytes	2016-10-11	Anonymous
allowing-nonsuperusers-to-search-users-by-filters-from-api.patch	371 Bytes	2016-10-12	Anonymous
redmine_lte_v3.2_allow-stdusers-filter-users-from-api.patch	371 Bytes	2016-10-12	Anonymous
redmine_lt_v3.3_allow-stdusers-filter-users-from-api.patch	371 Bytes	2016-10-12	Anonymous