Redmine - Defect #1
permissions if not admin

2006-12-30 11:35 - Todd McGrath

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

Description

You probably already know this, but just in case....

If a user is not an administrator and they attempt to click on a project where they are a member (in any role, manager, developer, reporter, etc.), there is an unexpected result:

Filter chain halted as [authorize] returned false
Completed in 0.00010 (10000 reqs/sec) | Rendering: 0.00000 (0%) | DB: 0.00000 (0%) | 403 [http://localhost/projects/show/1]

I believe this is the relevant code in the application.rb:

1. admin is always authorized
   return true if self.logged_in_user.admin?
2. if not admin, check membership permission
   @user_membership ||= Member.find(:first, :conditions => ["user_id=? and project_id=?", self.logged_in_user.id, @project.id])
   if @user_membership and Permission.allowed_to_role("%s/%s" % [ctrl, action], @user_membership.role_id)
     return true
   end
   render :nothing => true, :status => 403

-/-

Put another way- create a non-admin user, add this user to a project in any role (manager, developer, etc.) and then login as this new user. when you click on the project, you receive a blank page

-/-

Thoughts? Let me know if you want any help on this or if I'm doing something strange?

Todd

Associated revisions

Revision 473 - 2007-04-24 15:57 - Jean-Philippe Lang

Commit messages are now scanned for referenced or fixed issue IDs.
Keywords and the status to apply to fixed issues can be defined in Admin -> Settings.

Default keywords:

- for referencing issues: refs, references, IssueID
- for fixing issues: fixes,closes
There's no default status defined for fixed issue. You'll have to specify it if you want to enable auto closure of issues.

Example of a working commit message: "This commit references #1, #2 and fixes #3"

History

#1 - 2007-01-01 05:21 - Jean-Philippe Lang

Fixed in Revision 128

#2 - 2006-12-31 11:53 - Jean-Philippe Lang

Hi, You're right. There is a big problem for members of non public
projects. Public actions (projects/show, ...) should be implicitly
authorized to any role. For the moment, i'll fix it this way
(0.4.0 should be released soon).
In 0.5.0, many changes should be done on permissions management,
I'll do my best to answer your needs.

Thanks for your submission.

Best regards,

Jean-Philippe

#3 - 2006-12-30 17:32 - Todd McGrath

I have solution working for me and it also solves feature
request id: 6535. Maybe it will be helpful for you?

On the roles page (new or edit), we could include all
permissions including public. This way, we can control
things like projects/show, projects/list_issues, etc.

In addition, we can control whether or not certain modules
will even appear for certain groups (see feature request id:
6535). For example, if a group does not have "List"
permission for Documents module, the Documents link will not
appear.

I will upload three patch files to this ticket for your review:
roles_controller.rb_PATCH.txt
base.rhtml-PATCH.txt
application_helper.rb-PATCH.txt

#4 - 2006-12-30 15:55 - Todd McGrath

So, on further review, there are going to be many of things

related to this-

projects/list_issues
projects/list_news

etc.

#5 - 2006-12-30 15:28 - Todd McGrath

I think the problem is two parts

1) default data load should include 100 in default
permissions (I'll attach patch file to this ticket)

2) When creating a new Role, we need to add a permission id
of 1. What is the best way to do this? hidden form field?
update the "method" in roles_controller to include
it?

#6 - 2006-12-30 15:16 - Todd McGrath

Pardon me! The code above is perfect.

The problem can be resolved by inserting into the
permission_roles table. The projects/show permission is not
included from default roles and also if you add a new Role.

I'll research more.

#7 - 2009-08-13 11:33 - efgh efgh

- Status changed from Closed to Reopened

#8 - 2009-08-13 11:34 - efgh efgh

—

#9 - 2009-08-13 18:00 - Mischa The Evil

- Status changed from Reopened to Closed

#10 - 2012-10-03 18:01 - Fahmi Setiawan

- Assignee set to Azamat Hackimov
- % Done changed from 0 to 100

#11 - 2012-10-03 18:16 - Etienne Massip

- Assignee deleted (Azamat Hackimov)
- % Done changed from 100 to 0

Files

default-permissions-PATCH.txt	1.11 KB	2008-02-03	Todd McGrath

base.rhtml-PATCH.txt	7.45 KB	2008-02-03	Todd McGrath
roles_controller.rb_PATCH.txt	894 Bytes	2008-02-03	Todd McGrath
application_helper.rb-PATCH.txt	970 Bytes	2008-02-03	Todd McGrath