Redmine - Feature #23634

Restrict permissions for anonymous role

2016-08-22 15:48 - JW Fuchs

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Permissions and roles	**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

Even when all permissions for the anonymous role are deactivated, without login in users can still see

- the project list
- public project members
- activity in public projects
- news in public projects

It would be a useful feature to be able to disable all access for anonymous users, i.e. include additional options "view public project list", "view activity" and "view news" in the roles/permissions configuration.

The current setting leads to some display sideeffects. Links to issues and versions in news items aren't displayed properly, but rather their sourcecode:

View for any logged-in user:
news_user.PNG

View for anonymous:
news_anon.PNG

History

#1 - 2016-08-22 16:02 - Toshi MARUYAMA

- Description updated

#2 - 2016-08-30 17:16 - Holger Just

These permissions you ask for are all related currently:

- Public projects are visible to all users. The data inside these projects is visible based on the permissions of the respective roles.
- The members list of projects a user can see is also visible to them. This is because in order to be able to use filters and show issues, the members are visible anyway.
- If a user can see a project (either by being a member or because it is public), they can also see the activity view. The contents of the activity view is restricted to the data a user can see based on their permissions
- "View news" is not a separate permission since the idea is that all user participating in a project also should be able to view the news. The implicit "view news" permission is thus bound to the ability to see a project.

Thus, in the end, it boils down to the question of whether anonymous users should be able to see public projects. This can already be configured in **Administration** -> **Settings** -> **Authentication** -> **Authentication required**. If the setting is enabled, all access of the Anonymous role is effectively disabled which appears to be what you want to achieve.

As for your observation that sometimes the source code is shown, this is an consequence of how these links are handled. The renderer checks the permissions of the current user. Only if the user is allowed to see the linked-to object (a version in this case), the link is rendered. If the permission would not be checked, some additional data might be inadvertently leaked like the subject for issues.

#3 - 2016-08-31 10:45 - JW Fuchs

Thank you for the explanation. We have indeed changed the configuration to require authentication as described. While not ideal, this setting currently works for us. Separate permission settings "view public project list", "view project members", "view activity" and "view news" would still be useful for better role and access definitions.

#4 - 2020-09-25 21:36 - Hashem Nasarat

I would like to use redmine so customers can anonymously submit bugs but don't have access to anything else apart from the project name.

Due to security policies, the fact that redmine shows member names, roles, news, etc means I cannot used the anonymous/public project feature.

Files

news_user.PNG	6.35 KB	2016-08-22	JW Fuchs
news_anon.PNG	6.97 KB	2016-08-22	JW Fuchs