Redmine - Feature #38853

do not disclose login account names (public projects disclose some user info)

2023-07-17 14:56 - Thomas Meyer

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	6.0.0		
Resolution:			

Description

As public project without public access to user info - do no... did not get any reaction, I think it is worth submitting a ticket:

Following the How to prohibit public access to user info discussion:

We recently observed the fact that Redmine (at least until Remdmine 4.2) has the somewhat doubtable default setting that role 2 (anonymous) has the right to see all users and not only members of visible projects. I would say the latter would be a better default.

Furthermore, when there are public projects, all members of these projects are still visible to the public, together with their (login) account name, which is, in case of directory integration, their user name.

This clearly is an information that should not go to the public.

So I would suggest to

- not disclose redmine login account names to the public, even in public projects (this could probably be reached by adding a nick for public display)
- provide an option to add noindex directives to search bots for user and group information

Kind regards, Tom

```
Environment:
Redmine version 5.0.5.stable
Ruby version 2.7.5-p203 (2021-11-24) [x86_64-linux-gnu]
Rails version 6.1.7.2
Environment production
Database adapter PostgreSQL
Mailer queue ActiveJob::QueueAdapters::AsyncAdapter
Mailer delivery smtp
Redmine settings:
Redmine theme Default
SCM:
Subversion 1.13.0
Mercurial 5.3.1
Cvs 1.12.13
Bazaar 3.0.2
Git 2.39.2
Filesystem
Redmine plugins:
no plugin installed
```

History

#1 - 2024-01-23 12:50 - Holger Just

- File 0001-Migration-Set-builtin-and-new-roles-user-visibility-.patch added

The attached patch adds a new migration which sets the database default for new roles from users_visibility: all to users_visibility: members_of_visible_projects which is likely a safer general default. This change only affects newly created roles. As Rails takes the default column value of the database into account when creating a new role, this is enough to set the default value

The migration then also updates the builtin roles (Anonymous and Non-Member) to the new value, regardless of their existing value. Unfortunately, we can not distinguish if the migration is run during the initial setup (i.e. on an initially empty database) or later on an existing Redmine. As such, this may change deliberate role settings (to be more restrictive / secure). I think, this could be safe here as the current default of showing all users is likely unwanted for most installations.

If this is unwanted, we may also alternatively update the existing 20141109112308_add_roles_users_visibility.rb migration to set the builtin role's user visibility to members_of_visible_projects while keeping the database default unchanged (and still change the default in a new migration which is applied to new and updated Redmine installations).

As for hiding the data of visible users: I'm not sure about this. Could you explain what hiding the login name would provide in additional security? This information is not really private and can be used in various locations anyways, e.g. the @-mention autocomplete.

Adding the user's pages to the robots.txt exclusion list may be warranted, but I don't have a strong opinion about that. This appears to be security-by-obscurity rather than an actual security improvement.

#2 - 2024-02-27 21:56 - Marius BĂLTEANU

- Target version set to 6.0.0

Files

0001-Migration-Set-builtin-and-new-roles-user-visibility-.patch	1.3 KB	2024-01-23	Holger Just