Redmine - Patch #25483
Forbid to edit/update/delete the anonymous user

2017-03-30 15:20 - Holger Just

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	3.4.0		

Description

Right now, an admin can (in principal) edit and even delete the Anonymous user via the UserController since it doesn't restrict its query to logged users. This should not be possible and doesn't seem to be intended from the surrounding code:

- When showing the edit form for the anonymous user, a template error occurs in app/views/users/_general.html.erb.
- When deleting the anonynmous user, all its objects will be assigned to itself and the user gets deleted. While it will be automatically recreated on next access, all its issues, journals, ... will have dangling user_ids pointing to the old anonymous user.

The attached patch restricts edit/update/delete of users to logged users. Displaying the user page of Anonymous is still supported. The Patch was extracted from Planio.

Associated revisions

Revision 16464 - 2017-04-03 14:59 - Jean-Philippe Lang

Deny edit/update/delete for anonymous user (#25483).

Patch by Holger Just.

History

#1 - 2017-03-31 05:43 - Go MAEDA

- Target version set to 3.4.0

Confirmed the problem. Setting target version to 3.4.0.
Thank you for sharing the patch.

#2 - 2017-04-03 15:06 - Jean-Philippe Lang

- Status changed from New to Closed

- Assignee set to Jean-Philippe Lang

Patch committed, thanks!

#3 - 2017-04-03 15:12 - Jean-Philippe Lang

Holger Just wrote:

> *- When deleting the anonynmous user, all its objects will be assigned to itself and the user gets deleted. While it will be automatically recreated on next access, all its issues, journals, ... will have dangling user_ids pointing to the old anonymous user.*

FTR, I was not able to reproduce this behaviour as AnonymousUser#destroy does nothing and returns false.

#4 - 2017-04-03 17:44 - Holger Just

Ah, because AnonymousUser#destroy is indeed overwritten to do nothing (i.e. just return false). All the hooks would still run which might have unwanted consequences, thus stis patch is still absolutely warranted.

Files

0001-Deny-edit-update-delete-for-anonymous-user.patch	3.35 KB	2017-03-30	Holger Just