

Forbid to edit/update/delete the anonymous user

2022/05/09 18:14 - Admin Redmine

ステータス:	Closed	開始日:	2022/05/09
優先度:	通常	期日:	
担当者:		進捗率:	0%
カテゴリ:	Accounts / authentication_7	予定工数:	0.00時間
対象バージョン:	3.4.0_119	作業時間:	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/25483	status_id:	5
category_id:	7	tracker_id:	3
version_id:	119	plus1:	0
issue_org_id:	25483	affected_version:	
author_id:	2784	closed_on:	
assigned_to_id:	1	affected_version_id:	
comments:	4		

説明

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 anonymous 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": <https://plan.io/redmine-hosting>.

journals

Confirmed the problem. Setting target version to 3.4.0.

Thank you for sharing the patch.

Patch committed, thanks!

Holger Just wrote:

- When deleting the anonymous 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.

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.

履歴

#1 - 2022/05/10 17:06 - Admin Redmine

- カテゴリを Accounts / authentication_7 にセット

- 対象バージョンを 3.4.0_119 にセット