Redmine - Defect #26063

Users can assign a user/group which is not a member of current project, or even a user that doesn't exist

2017-05-29 14:55 - Vincent C.

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Issues	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Fixed	**Affected version:**	3.2.0

Description

Hello !

`Tested on Redmine 3.2.0`

(I consider it as a bug, but it may be standard behaviour, which would be a really strange design decision)

I discovered this after receiving a report that the group which was assigned on an issue couldn't see it. This was normal, because the group was not a member of the related project. But I don't know how the issue could have been assigned to this group since only project members are assignable (even after investigating, I still don't know how it could have happened).

So I uninstalled all plugins on my integration environment, to avoid any plugin-related strange behaviour which could cause that. Then tried to replace the currently assigned user/group ID directly in HTML page (with Chrome "Inspect Element"), just to see if it was a client or server side problem. This led me to this bug report :

- When replacing with the ID of **another user/group from same project**, the issue is saved normally, and the issue is assigned to given group *(this is standard behaviour)*
- When replacing by the ID of **a user/group which is NOT a member of the project**, it also works *(**this should not work**. Even though assigned user/group can't see the issue, it shouln't even be assignable in the first place)*
- When replacing by the ID of **a group which is un-assignable globally** *(= has only an un-assignable role)*, it also works
- When replacing by the ID of **a non-existing user/group**, it also works *(when the issue is saved, the current assignee is just set to "" in web page, and the given ID is set in database)*

18421

This doesn't seem to be the proper way it should be working.
It also allows user/group listing across the entire Redmine instance, which could be considered as a security threat.

PS : I can't test on a more recent version than 3.2.0 ATM, sorry for that. *(it takes 10 sec to reproduce, just inspect element with Chrome, set ID to "9999999" for currently selected option, and save issue)*

Related issues:

Related to Redmine - Defect #23921: REST API Issue PUT responds 200 OK even w...	**Closed**	

History

#1 - 2017-05-29 15:38 - Go MAEDA

- Related to Defect #23921: REST API Issue PUT responds 200 OK even when it can't set assigned_to_id added

#2 - 2017-05-29 15:42 - Go MAEDA

- Status changed from New to Closed

- Resolution set to Fixed

I cannot reproduce the problem on the current trunk (r16580). It seems to be fixed by #23921 for upcoming 3.4.0. Please see source:trunk/app/models/issue.rb@16055#L710 for details.

Thank you for reporting.

Files

redmine_issue_assignee_bug.png	37.4 KB	2017-05-29	Vincent C.