Redmine - Defect #15567

cookiestore / session management

2013-11-28 17:49 - Jan Niggemann (redmine.org team member)

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jan Niggemann (redmine.org team member)	**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	

Description

I don't know if this is a true threat or not, but redmine is explicitly mentioned here:
http://maverickblogging.com/list-of-websites-using-ruby-on-rails-cookiestore-for-session-management/

http://projects.webappsec.org/w/page/13246944/Insufficient%20Session%20Expiration

Reply: No, Rails' CookieStore isn't broken

Do we need to to something about this?

History

#1 - 2013-11-29 00:23 - Jean-Philippe Lang

Redmine adds a (configurable) maximum lifetime and an idle timeout to sessions so that cookies don't persist "for life". Anyone who runs Redmine is free to switch to ActiveRecordStore or MemCacheStore where sessions are invalidated when the user logs out.

#2 - 2013-11-29 09:00 - Jan Niggemann (redmine.org team member)

- Status changed from New to Confirmed

- Assignee set to Jan Niggemann (redmine.org team member)

It would be a good idea to add information to the RedmineSettings, I'll take care of that.

#3 - 2013-11-29 21:43 - Jan Niggemann (redmine.org team member)

- Status changed from Confirmed to Resolved

- Private changed from Yes to No

Added some information to RedmineSettings

#4 - 2013-11-29 22:46 - Jan Niggemann (redmine.org team member)

- Status changed from Resolved to Closed