Redmine - Defect #6792

Set cookie secure flag when accessing Redmine over HTTPS

2010-11-02 12:48 - Sen Haerens

Status:	Closed		**Start date:**	2010-11-02
Priority:	Normal		**Due date:**	
Assignee:			**% Done:**	0%
Category:			**Estimated time:**	0.00 hour
Target version:				
Resolution:	Invalid		**Affected version:**	1.0.3

Description

Is it possible to add this to Redmine?
I'm proxying via Nginx with header "X-Forwarded-Proto https".

http://codebutler.com/firesheep-a-day-later

Full HTTPS for everything — Some sites support full encryption everywhere, but don't implement it properly by failing to set the "Secure" flag on authentication cookies, negating most of the benefits and leaving users at risk. What that means is that any time you type the URL (e.g. "manage.slicehost.com") into your web browser (without explicitly typing https:// beforehand, which people rarely do) you will inadvertently leak your cookies with that first request, prior to being redirected to the HTTPS page. Slicehost and Dropbox are good examples of this mistake.

History

#1 - 2010-11-02 13:24 - Holger Just

- Status changed from New to Closed

- Resolution set to Invalid

It is possible. Add :secure => true to the hash in config/initializers/session_store.rb.

In the future, please ask such questions in the forums. The issue tracker is only uses for code issues, not for support questions.