Redmine - Feature #12296

Add HSTS enforcement support to Redmine

2012-11-03 00:32 - Bernd May

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Project settings	**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

During initial HTTPS session setup an attacker is able to run a MitM SSLStrip attack agains a client connecting to the webserver replacing any https:// links with http:// ones. This problem has been demonstrated by Moxie Marlinspike on BlackHat in 2009 and there exists an IETF draft for an appropriate HTTPS Header that can alleviate this problem. Basically if you have ever visited a site via https before from a 'secure' environment, the site can tell you to always use https in the future for a given amount of time. Except for IE, browsers already implement the required functionality and it would be really nice to have it also in Redmine. AFAIK all it takes is add some small lines to the part that handles connections - wikipedia provides the general layout for a RoR Application.

Though I think that one could also enforce this on a more global level, e.g. configuring the webserver running the application, it would be nice to make this a (configurable?) feature inside the application to further secure the use of ssl.

History

#1 - 2012-11-03 19:15 - Eduardo Zambrano

- Assignee set to Maxim Krušina

- % Done changed from 0 to 20

#2 - 2012-11-03 21:24 - Maxim Krušina

- Assignee deleted (Maxim Krušina)

- % Done changed from 20 to 0