Redmine - Feature #2579

Configure SSL schema for "private" actions.

2009-01-25 16:25 - Kevin Menard

Status:	Closed	**Start date:**	2009-01-25
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:	Wont fix		

Description

Right now I have my entire Redmine installation hosted on an SSL-enabled vhost in Apache2. I have a mod_rewrite rule for anything on port 80 to redirect to the SSL-enabled vhost. This is largely overkill, but I wanted to protect any page with private information. Enumerating all the possible URLs for this and drafting mod_rewrite rules is a lengthy and error-prone process.

What I would like to see is a project setting for enabling SSL for "private" actions. Private here meaning user privacy and not a language-level construct. All this option would do is enable the creation of SSL links for these actions or internally redirect to the same URL with the HTTPS schema. The SSL portion would still be handled at the web server level.

For whatever it's worth, that's what I thought the "Protocol" setting would do when I first started with Redmine. It wasn't until later that I realized it was for email links.

Related issues:

Related to Redmine - Feature #24763: Force SSL when Setting.protocol is "https"	**New**

History

#1 - 2017-01-16 01:09 - Go MAEDA

- Related to Feature #24763: Force SSL when Setting.protocol is "https" added

#2 - 2024-02-26 22:29 - Holger Just

- Status changed from New to Closed

- Resolution set to Wont fix

All actions are private in the end (or none are) as session information is transmitted along with the data and attackers who can intercept the data could also intercept active sessions.

As such, it is currently best practice to use and enforce https for all of Redmine. Increased resource consumption for TLS is usually not an issue in the current times.

#3 - 2024-02-26 22:52 - Kevin Menard

Holger Just wrote in #note-2:

> All actions are private in the end (or none are) as session information is transmitted along with the data and attackers who can intercept the data could also intercept active sessions.
>
> As such, it is currently best practice to use and enforce https for all of Redmine. Increased resource consumption for TLS is usually not an issue in the current times.

Thanks. It's been a while, but I believe this issue predated Redmine's option for enforcing HTTPS. I agree that everything should be SSL now. It was fashionable at the time to use non-SSL for things like unauthenticated issue displays (IIRC, for search engine indexing). I'm happy we've finally embraced SSL universally.