Redmine - Defect #9239
autenticity_token is not checked properly

2011-09-13 14:22 - Karel Pičman

Status:	Closed	**Start date:**	2011-09-13
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Fixed	**Affected version:**	1.2.1

Description

I'm afraid that auhtenticity_token is not checked properly. E.g. While submitting a user change I stop the submitting using Tamper Data Firefox plugin and change authenticity_token or remove the value of authenticity_token completely. To check the Redmine behaviour I change form value admin = 1 in Tamper Data. Althought authenticity_token is not equal to the original value sent from the server, the request is successfully processed. The user got Administrator role and only after that is the user logged out because of wrong authenticity_token.
I'd expect this procedure:

1. Check authenticity_token
2. If it's OK then process the request
3. If not then deny to process the request

I've tried to document the test on attached screen shots:

Step 1: Edit a user
Step 2: Stop execution and alter sent data(admin flag and authenticity_token)
Step 3About your application's environment
Ruby version 1.8.7 (x86_64-linux)
RubyGems version 1.3.7
Rack version 1.1.2
Rails version 2.3.11
Active Record version 2.3.11
Active Resource version 2.3.11
Action Mailer version 2.3.11
Active Support version 2.3.11
Edge Rails revision unknown
Application root /home/picman/tmp/redmine-1.2.1
Environment production
Database adapter mysql
Database schema version 20110511000000: Submit the request
Step 4: We can see, that the user was promoted to administrator.

Clear installation without any changes or additional plugins. The same problem in version 1.2.0.

Related issues:

Related to Redmine - Defect # 4825: Several related bugs relating to registra...	**New**	**2010-02-13**

History

#1 - 2011-10-05 16:13 - Karel Pičman

Is there any chance that somebody will look at this issue? I'm afraid that it has impact on security of each Redmine instance installed on the Internet.

#2 - 2011-10-05 17:02 - Felix Schäfer

So you're logged in as an admin and can change things with a wrong authenticity token, or what seems to be the problem?

#3 - 2011-10-05 17:09 - Karel Pičman

Yes. The user profile is updated first and only after that is the authenticity token checked. The authenticity token must be checked always first otherwise authenticity principle is useless in my opinion.
In case of wrong authenticity token no data can be changed.

#4 - 2011-10-05 17:27 - Felix Schäfer

I think it's been corrected in trunk http://www.redmine.org/projects/redmine/repository/diff?rev=6316&rev_to=6314 , can't find any issue for it though. Could you try it on trunk?

#5 - 2011-10-05 18:42 - Felix Schäfer

(for the record, it's been fixed and released in Chiliproject about 2 months ago in 2.1.0 and 1.5.1 </shameless plug>)

#6 - 2011-10-06 11:20 - Karel Pičman

- Status changed from New to Resolved
- % Done changed from 0 to 100

Works fine in the current trunk. Thank you.

#7 - 2011-10-06 11:28 - Etienne Massip

- Status changed from Resolved to Closed
- Resolution set to Fixed

Thanks for your feedback.

Files

step_1.png	116 KB	2011-09-13	Karel Pičman
step_2.png	67.8 KB	2011-09-13	Karel Pičman
step_3.png	47.6 KB	2011-09-13	Karel Pičman
step_4.png	115 KB	2011-09-13	Karel Pičman