Redmine - Defect #5915

Invalid form authenticity token for some users

2010-07-20 15:55 - Benjamin FRAUD

Status:	Closed	**Start date:**	2010-07-20
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:			
Resolution:	No feedback	**Affected version:**	0.9.3

Description

Some users of my Redmine (0.9.3) encounter this error when they want to perform any action linked to forms. Some users don't seem to have any problem, so I'm guessing it has something to do with the tokens registered in the database and not the server (we're using Apache).
I've seen that this problem has already been raised in previous defects, but I couldn't find any valuable information. Is this going to be fixed in the next release?

Related issues:

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

History

#1 - 2010-07-20 17:54 - Felix Schäfer

- Status changed from New to Closed

- Resolution set to Invalid

Benjamin FRAUD wrote:

> Some users of my Redmine (0.9.3) encounter this error when they want to perform any action linked to forms. Some users don't seem to have any problem, so I'm guessing it has something to do with the tokens registered in the database and not the server (we're using Apache).
> I've seen that this problem has already been raised in previous defects, but I couldn't find any valuable information. Is this going to be fixed in the next release?

That happens if you keep your form open too long (for example: open a new tab with a form, do something else, the token has expired). The authenticity token is a rails feature to thwart XSS attacks.

#2 - 2010-07-21 08:48 - Benjamin FRAUD

- Status changed from Closed to Reopened

Hi Felix, thank you for your answer.

However, the problem doesn't seem to be linked to the waiting time of some users regarding forms, as I tried to submit some form entries just a few seconds after accessing the page.
Obviously, the tokens stored in the session variable and in the forms hidden field don't match, but I don't understand why. And since the problem occurs for just some users, could it has something to do with the registration process? Tests have been made on several computers using different browsers, so I don't think it's related to the way of stocking session variables, but I can't be sure. Can I access the client-side token variable to see what it looks like?

#3 - 2010-07-21 09:15 - Benjamin FRAUD

An important thing : the problem seems to move when I try to connect to the same account on several computers or on multi-browsers. As far as I know, this is not supposed to be a problem on Redmine, but what you need to know is that for security reasons we had to delete the ability for users to log out. The function was not erased in the account controller, but the link in the top menu and the route reaching the log out action are no longer available. We installed the plug in "http authentication" to let Apache deal with user authentication.

#4 - 2010-07-21 10:51 - Felix Schäfer

In the view, the authenticity_token is stored in a hidden field, I'm not sure where it gets stored where it gets stored 'server-side', but I'd wager it's in the session. If you have the stock session store, the sessions are stored in encrypted and signed cookies, which also means sessions aren't/can't be shared across cookie jars/browsers.

My advice would be to try with a stock redmine, or at least without the http-authentication plugin. If there really was such a glaring problem with the tokens, basically every other rails app would have it too and it would certainly be known, so I suspect the http-auth plugin doesn't handle sessions

correctly.

#5 - 2010-07-21 11:49 - Nikolay Kotlyarov

In my case the same problem was due to redmine_time_tracker plugin and was fixed by plugin developer:
http://github.com/delaitre/redmine_time_tracker/commit/822b573601875c618d87964589d655e670a674eb

Try to post an issue on plugin's developer page:
http://github.com/AdamLantos/redmine_http_auth/issues

#6 - 2010-08-03 12:59 - claude g

In case it could help, I have the same situation (0.9.6 with NO plugin but runing with a Bitnami stack):

- if using Firefox : OK
- if using Internet Explorer 8 : OK with IP address in URL but KO with real URL
  => solved under Internet Explorer by changing **Internet Option** / **Privacy**/ **Advanced** :
  + Override automatic cookie handling checked
  + Always allow session cookies

#7 - 2010-08-04 11:19 - Stu Bendelow

Same issue caused by opening Redmine in more than one browser
-open Firefox and log into Redmine (copy A)
-open a second copy of Firefox and log into Redmine (Copy B)
attempt to save a change in copy A and you see the invalid form authenticity token warning
however you do not get the same issue using tabs in Firefox I could log in on two seperate tabs and save changes in both, it has to be a seperate copy of the browser

#8 - 2010-08-04 11:36 - Felix Schäfer

Stu Bendelow wrote:

> Same issue caused by opening Redmine in more than one browser

This is normal as the session information is stored in a cookie in the browser: only the "last" cookie is valid, thus logging in in a second browser will deprecate the session cookie from the first browser, effectively logging you out.

#9 - 2010-09-16 10:45 - jin wang

Hi~ I find this problem caused by opening redmine in more than one browser. If you delete the files in *Temporary Internet Files * and restart your pc you can solve this proble.

清空ie缓存，重新刷新或打开页面；
如果还不行就清空ie临时文件夹下所有文件，然后重启下机器。
IE临时文件夹：C:\Documents and Settings\用户名\Local Settings\Temporary Internet Files（默认为隐藏目录）你也可以通过这个操作查看：打开IE---工具---internet选项---常规---设置。
IE临时文件夹里存放着我们最近浏览过的网页的内容，这样做的目的是提高我们的上网浏览的速度。

呵呵

#10 - 2010-09-16 13:34 - Felix Schäfer

Benjamin, can you confirm this is still a problem for you, or did you find what was going wrong?

#11 - 2010-09-29 17:26 - Felix Schäfer

- Status changed from Reopened to Closed

- Resolution changed from Invalid to No feedback