Redmine - Defect #15735
OpenID login fails due to CSRF verification

2013-12-18 21:18 - Marcel M

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	2.4.2		
Resolution:	Fixed	**Affected version:**	2.4.1

Description

Hi,

after upgrading from 2.3.0 to 2.4.1 I could no longer login via openid.

This is the log snippet:

```
Generated checkid_setup request to https://openid.xxx.com/index.php?user=John.Doe
 with assocication bmshmeqgqqlrpqbu5sjo4g3g84
Started GET "/support/login?_method=post&openid1_claimed_id=...
 for 192.168.x.x at Sun Dec 15 15:24:48 +0100 2013
Processing by AccountController#login as HTML
  Parameters: {"openid1_claimed_id"=>"https://openid.xxx.com/John.Doe", "rp_nonce"=>"2013-12-15T14:24:43ZZ0jbBB"}
WARNING: Can't verify CSRF token authenticity
  Rendered common/error.html.erb within layouts/base (0.8ms)
Filter chain halted as :verify_authenticity_token rendered or redirected
Completed 422 Unprocessable Entity in 28.0ms (Views: 27.3ms | ActiveRecord: 0.0ms)
```

After googling a bit I found a solution based on this https://github.com/xaviershay/enki/issues/91

So I tweaked app/controllers/account_controller.rb a bit:

```
diff redmine/app/controllers/account_controller.rb redmine-2.4.1/app/controllers/account_controller.rb
23,25c23
<   skip_before_filter :check_if_login_required, :check_password_change, :verify_authenticity_token, :only => :login
<   before_filter :verify_authenticity_token_unless_openid, :only => :create
<
---
>   skip_before_filter :check_if_login_required, :check_password_change
345,349d342
<
<   def verify_authenticity_token_unless_openid
<     verify_authenticity_token unless using_open_id?
<   end
<
```

and I can now successfully login.

From my point of view I did not introduce a security issue here but a 2nd opionion would be great before this is added to redmine.

Associated revisions

Revision 12438 - 2013-12-21 13:04 - Jean-Philippe Lang

Fixed that OpenID authentication fails with 422 error due to token verification (#15735).

Revision 12444 - 2013-12-22 15:48 - Jean-Philippe Lang

Merged r12438 (#15735).

History

#1 - 2013-12-19 04:21 - Toshi MARUYAMA

- Target version set to 2.4.2

#2 - 2013-12-21 13:07 - Jean-Philippe Lang

- Subject changed from OpenID login and CSRF failure to OpenID login fails due to CSRF verification

- Status changed from New to Resolved

- Assignee set to Jean-Philippe Lang

- Resolution set to Fixed

This is fixed in r12438, thanks for pointing this out.

#3 - 2013-12-22 15:48 - Jean-Philippe Lang

- Status changed from Resolved to Closed

Merged.

#4 - 2013-12-22 15:57 - Jean-Philippe Lang

- Duplicated by Feature #11907: Custom Field Version (Locked/Open) added

#5 - 2013-12-22 15:58 - Jean-Philippe Lang

- Duplicated by deleted (Feature #11907: Custom Field Version (Locked/Open))