Redmine - Patch #18980

Parameter back_url not set on redirect to login page when session has expired

2015-01-30 12:53 - Maarten Hoogveld

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:			

Description

When a user requests a page (like "/projects/project_name/issues") and the session has expired, the user is redirected to "/login" without setting the "back_url" parameter.
This results in the user being redirected to "/my/page" after a successful login.
Expected behavior would be to redirect the user back to the originally requested url.
To test this more easily I have manually set the session_timeout to 1 (minute) in the database table (sql: update settings set value = 1 where name = 'session_timeout')

I have written a patch which sends along the proper "back_url" parameter. I have borrowed the code for creating of the "back_url" parameter from the function "require_login" from the same controller. Ruby is not my native language, so please check if this patch is correct (although I'm sure this is done anyway.)
Also logs are included which show the original behavior and the behavior when this patch is applied.

Patch

```
Index: app/controllers/application_controller.rb
===================================================================
--- app/controllers/application_controller.rb    (revision 13953)
+++ app/controllers/application_controller.rb    (working copy)
@@ -62,10 +62,16 @@
   def session_expiration
     if session[:user_id]
       if session_expired? && !try_to_autologin
+        # Extract only the basic url parameters on non-GET requests
+        if request.get?
+          url = url_for(params)
+        else
+          url = url_for(:controller => params[:controller], :action => params[:action], :id => pa
rams[:id], :project_id => params[:project_id])
+        end
         set_localization(User.active.find_by_id(session[:user_id]))
         reset_session
         flash[:error] = l(:error_session_expired)
-        redirect_to signin_url
+        redirect_to signin_url(:back_url => url)
       else
         session[:atime] = Time.now.utc.to_i
       end
```

Log of original version - Page request after session expiration:

```
Started GET "/projects/my_project_name/issues" for 1.2.3.4 at 2015-01-30 11:51:34 +0100
Processing by IssuesController#index as HTML
  Parameters: {"project_id"=>"my_project_name"}
Redirected to https://www.redmine.org/login
Filter chain halted as :session_expiration rendered or redirected
Completed 302 Found in 5.3ms (ActiveRecord: 0.3ms)
Started GET "/login" for 1.2.3.4 at 2015-01-30 11:51:34 +0100
Processing by AccountController#login as HTML
  Current user: anonymous
  Rendered account/login.html.erb within layouts/base (2.1ms)
```

```
Completed 200 OK in 18.3ms (Views: 12.5ms | ActiveRecord: 1.8ms)

Started POST "/login" for 1.2.3.4 at 2015-01-30 11:51:44 +0100
Processing by AccountController#login as HTML
  Parameters: {"utf8"=>"✓", "authenticity_token"=>"3H5asd234aslkjdhakh382y4=", "username"=>"my_use
rname", "password"=>"[FILTERED]", "login"=>"Log in »"}
  Current user: anonymous
Successful authentication for 'my_username' from 1.2.3.4 at 2015-01-30 10:51:44 UTC
Redirected to https://www.redmine.org/my/page
Completed 302 Found in 8.2ms (ActiveRecord: 2.6ms)
Started GET "/my/page" for 1.2.3.4 at 2015-01-30 11:51:44 +0100
Processing by MyController#page as HTML
  Current user: my_username (id=3)
  Rendered my/blocks/_timelog.html.erb (4.9ms)
  Rendered issues/_list_simple.html.erb (14.3ms)
  Rendered my/blocks/_issuesassignedtome.html.erb (33.7ms)
  Rendered issues/_list_simple.html.erb (23.3ms)
  Rendered my/blocks/_issuesreportedbyme.html.erb (34.1ms)
  Rendered my/page.html.erb within layouts/base (75.5ms)
Completed 200 OK in 184.8ms (Views: 175.2ms | ActiveRecord: 4.7ms)
```

Log of patched version - Page request after session expiration:

```
Started GET "/projects/my_project_name/issues" for 1.2.3.4 at 2015-01-30 12:01:49 +0100
Processing by IssuesController#index as HTML
  Parameters: {"project_id"=>"my_project_name"}
Redirected to https://www.redmine.org/login?back_url=https%3A%2F%2Fwww.redmine.org%2Fprojects%2Fmy
_project_name%2Fissues
Filter chain halted as :session_expiration rendered or redirected
Completed 302 Found in 5.9ms (ActiveRecord: 0.5ms)
Started GET "/login?back_url=https%3A%2F%2Fwww.redmine.org%2Fprojects%2Fmy_project_name%2Fissues"
for 1.2.3.4 at 2015-01-30 12:01:49 +0100
Processing by AccountController#login as HTML
  Parameters: {"back_url"=>"https://www.redmine.org/projects/my_project_name/issues"}
  Current user: anonymous
  Rendered account/login.html.erb within layouts/base (2.2ms)
Completed 200 OK in 19.1ms (Views: 13.2ms | ActiveRecord: 1.8ms)

Started POST "/login" for 1.2.3.4 at 2015-01-30 12:02:13 +0100
Processing by AccountController#login as HTML
  Parameters: {"utf8"=>"✓", "authenticity_token"=>"3H5asd234aslkjdhakh382y5=", "back_url"=>"https:
//www.redmine.org/projects/my_project_name/issues", "username"=>"my_username", "password"=>"[FILTE
RED]", "login"=>"Log in »"}
  Current user: anonymous
Successful authentication for 'my_username' from 1.2.3.4 at 2015-01-30 11:02:13 UTC
Redirected to https://www.redmine.org/projects/my_project_name/issues
Completed 302 Found in 12.1ms (ActiveRecord: 4.4ms)
Started GET "/projects/my_project_name/issues" for 1.2.3.4 at 2015-01-30 12:02:13 +0100
Processing by IssuesController#index as HTML
  Parameters: {"project_id"=>"my_project_name"}
  Current user: my_username (id=3)
  Rendered queries/_filters.html.erb (14.7ms)
  Rendered queries/_columns.html.erb (2.5ms)
  Rendered issues/_list.html.erb (248.6ms)
  Rendered plugins/redmine_contacts/app/views/contacts_issues/_contacts.html.erb (1.2ms)
  Rendered issues/_sidebar.html.erb (7.4ms)
  Rendered issues/index.html.erb within layouts/base (287.3ms)
Completed 200 OK in 436.8ms (Views: 318.8ms | ActiveRecord: 13.4ms)
```

Related issues:

Related to Redmine - Patch #19655: Set a back_url when forcing new login afte...	**Closed**

History

#1 - 2015-01-30 12:55 - Maarten Hoogveld

After fighting with spam detection I finally submitted without setting correct issue properties

Category: Accounts / authentication
Affected version: 2.6.1 (and below)

#2 - 2015-02-01 23:41 - Jan Niggemann (redmine.org team member)

- Category set to Accounts / authentication

#3 - 2015-04-07 16:59 - Go MAEDA

- Target version set to Candidate for next minor release

#4 - 2015-04-21 02:55 - Go MAEDA

- Related to Patch #19655: Set a back_url when forcing new login after session expiration added

#5 - 2015-05-09 12:44 - Jean-Philippe Lang

- Status changed from New to Closed

- Target version deleted (Candidate for next minor release)

Superseded by #19655.