# Redmine - Defect #10780

## Logout by using POST REST API

2012-04-26 14:29 - Vincent Schänzer

| | | | |
|---|---|---|---|
| **Status:** | Needs feedback | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | REST API | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **Resolution:** | | **Affected version:** | 1.4.1 |

**Description**

I'm currently login in REDMINE, but after making a POST over the REST API, I'm no longer login to REDMINE.

About your application's environment
Ruby version 1.8.7 (x86_64-linux)
RubyGems version 1.3.7
Rack version 1.1.3
Rails version 2.3.14
Active Record version 2.3.14
Active Resource version 2.3.14
Action Mailer version 2.3.14
Active Support version 2.3.14
Database adapter sqlite3

Javascript:

```
RedmineUrl = 'https://projects.modell-aachen.de'
AuthToken = '9611ec7f30316e04967a0aef4ed34e44719405b7'

$.ajax({
    type: 'POST',
    url: RedmineUrl+'/issues.json',
    username: AuthToken,
    dataType: 'json',
    data: {"issue": {"project_id": "test","subject": "Test issue",}},
    async: true,
    success: function(data){console.dir(data)}
})
```

**Related issues:**

| | |
|---|---|
| Related to Redmine - Defect #15424: Filter chain halted as :verify_authentici... | **Closed** |

### History

#### #1 - 2012-04-26 15:09 - Etienne Massip

What's in your production.log?

#### #2 - 2012-04-26 15:17 - Vincent Schänzer

```
Processing AccountController#login (for 77.11.63.231 at 2012-04-26 15:15:40) [POST]
  Parameters: {"password"=>"[FILTERED]", "authenticity_token"=>"zoLBWotuKKmwlcfb1w9Bfo7guuq1nZEN3FeOBBcXwHw=",
 "action"=>"login", "login"=>"Anmelden \302\273", "controller"=>"account", "back_url"=>"https%3A%2F%2Fprojects
.modell-aachen.de%2F", "username"=>"schaenzer"}
Redirected to https://projects.modell-aachen.de/
Completed in 195ms (DB: 3) | 302 Found [https://projects.modell-aachen.de/login]

Processing WelcomeController#index (for 77.11.63.231 at 2012-04-26 15:15:41) [GET]
  Parameters: {"action"=>"index", "controller"=>"welcome"}
Rendering template within layouts/base
Rendering welcome/index
Completed in 188ms (View: 167, DB: 5) | 200 OK [https://projects.modell-aachen.de/]

Processing IssuesController#create to json (for 77.11.63.231 at 2012-04-26 15:15:49) [POST]
  Parameters: {"format"=>"json", "action"=>"create", "issue"=>{"subject"=>"Test issue", "project_id"=>"test"},
```

```
 "controller"=>"issues"}
Filter chain halted as [:check_if_login_required] rendered_or_redirected.
Completed in 12ms (View: 0, DB: 2) | 401 Unauthorized [https://projects.modell-aachen.de/issues.json]

Processing IssuesController#create to json (for 77.11.63.231 at 2012-04-26 15:15:49) [POST]
  Parameters: {"format"=>"json", "action"=>"create", "issue"=>{"subject"=>"Test issue", "project_id"=>"test"},
 "controller"=>"issues"}
Sending email notification to:
Rendering issues/show (created)
Completed in 920ms (View: 48, DB: 29) | 201 Created [https://projects.modell-aachen.de/issues.json]

Processing WelcomeController#index (for 77.11.63.231 at 2012-04-26 15:15:58) [GET]
  Parameters: {"action"=>"index", "controller"=>"welcome"}
Redirected to https://projects.modell-aachen.de/login?back_url=https%3A%2F%2Fprojects.modell-aachen.de%2F
Filter chain halted as [:check_if_login_required] rendered_or_redirected.
Completed in 11ms (DB: 2) | 302 Found [https://projects.modell-aachen.de/]

Processing AccountController#login (for 77.11.63.231 at 2012-04-26 15:15:58) [GET]
  Parameters: {"action"=>"login", "controller"=>"account", "back_url"=>"https://projects.modell-aachen.de/"}
Rendering template within layouts/base
Rendering account/login
Completed in 20ms (View: 10, DB: 2) | 200 OK [https://projects.modell-aachen.de/login?back_url=https%3A%2F%2Fp
rojects.modell-aachen.de%2F]
```

#### #3 - 2012-05-20 10:51 - Patrick Atamaniuk

Affects me, too.

Redmine version: tag 1.4.1
Ruby version 1.8.7 (x86_64-linux)
RubyGems version 1.6.2
Rack version 1.1.3
Rails version 2.3.14
Active Record version 2.3.14
Active Resource version 2.3.14
Action Mailer version 2.3.14
Active Support version 2.3.14
Database adapter postgresql 9.1.3-2
Database schema version 20120301153455

I am logged in: get the welcomepage on the first browsertab.

```
Processing WelcomeController#index (for 192.168.57.1 at 2012-05-20 10:29:28) [GET]
  Parameters: {"action"=>"index", "controller"=>"welcome"}
Rendering template within layouts/base
Rendering welcome/index
Completed in 1886ms (View: 1190, DB: 531) | 200 OK [http://192.168.57.11/redmine/]
```

using api in another browser tab from a plugin

```
Processing XblMasterBacklogController#productbacklog to json (for 192.168.57.1 at 2012-05-20 10:29:45) [POST]
  Parameters: {"project_id"=>"fooproject", "action"=>"update", "subject"=>"asd2", "issue_id"=>"7527", "format"
=>"json", "controller"=>"xbl_master_backlog"}
Completed in 406ms (View: 45, DB: 315) | 200 OK [http://192.168.57.11/redmine/xbl_master_backlog/project/foopr
oject/productbacklog.json/7527?_dc=1337502585894]
```

Request completes successfully. (routes are ok, permissions ok, accept_api_auth ok etc.)

After that on the first tab i am logged out. Trying to get my page:

```
Processing MyController#account (for 192.168.57.1 at 2012-05-20 10:30:07) [GET]
  Parameters: {"action"=>"account", "controller"=>"my"}
Redirected to http://192.168.57.11/redmine/login?back_url=http%3A%2F%2F192.168.57.11%2Fredmine%2Fmy%2Faccount
Filter chain halted as [:check_if_login_required] rendered_or_redirected.
Completed in 165ms (DB: 147) | 302 Found [http://192.168.57.11/redmine/my/account]

Processing AccountController#login (for 192.168.57.1 at 2012-05-20 10:30:08) [GET]
  Parameters: {"action"=>"login", "back_url"=>"http://192.168.57.11/redmine/my/account", "controller"=>"accoun
t"}
Rendering template within layouts/base
Rendering account/login
Completed in 376ms (View: 103, DB: 248) | 200 OK [http://192.168.57.11/redmine/login?back_url=http%3A%2F%2F192
.168.57.11%2Fredmine%2Fmy%2Faccount]
```

#### #4 - 2012-05-20 14:58 - Patrick Atamaniuk

Although the request has a valid session cookie, it looks like the response header of the request sets the _redmine_session new.
This fixes it for me: https://gist.github.com/2758024
It also probably will kill my cat...

Edit: this could introduce csrf issues. This is no valid workaround.

#### #5 - 2012-05-21 11:55 - Etienne Massip

*- Description updated*

#### #6 - 2012-05-21 14:48 - Etienne Massip

Can't reproduce; from what you say you're calling the API from a new tab in the browser so the already authenticated user session will be used instead of the specified API user, won't it??

#### #7 - 2012-05-25 13:24 - Patrick Atamaniuk

So i would have expected, too. But it seems that the authenticated session is not used.
The XmlHttpRequest post header does indeed contain the session cookie, but (1.4.2) app/controllers/application_controller.rb find_current_user falls into the

```
elsif Setting.rest_api_enabled? && accept_api_auth?
```

branch. session[:user_id] seems not to be set at this point.

Redmine then successfully uses the api key, but returns a new session cookie with no user_id, thus logging out the other tab.
I'd construct a minimal test plugin for your convenience. I would need some days to prepare that.

#### #8 - 2012-05-28 18:20 - Patrick Atamaniuk

I have put together a testcase which you can use to reproduce the effect:
https://patrickatamaniuk@github.com/patrickatamaniuk/redmine_REST_test.git

I hope it proves useful.

#### #9 - 2012-05-31 09:42 - Patrick Atamaniuk

Provide a valid X-CSRF-Token in the POST request headers solves the issue.

See redmine public/javascripts/application.js how to do this.

#### #10 - 2012-05-31 10:27 - Etienne Massip

That's related to the use of the new tab in the same browser, this is not a regular use of the Rest API.

#### #11 - 2012-05-31 23:25 - Terence Mill

I think the stufftodo plugin utilizes this the same way, whats why we get logged ou or not logged ou correctly if using two tabs in same browser

https://github.com/GOYELLO/goyello_stuff_to_do/issues/15

I vote to fix that behaviour and allow such usage for future.

#### #12 - 2012-09-26 06:35 - Adam Chasen

This appears to affect several different uses of the REST API including applications such as RedminePro. I am using the latest version of Redmine (2.0.4)

I receive the following in my production log whenever running a POST:

```
Started POST "/projects/8/issues.json" for 127.0.0.1 at Mon Sep 24 22:27:22 +0000 2012
Processing by IssuesController#create as JSON
  Parameters: {"project_id"=>"8", "issue"=>{"custom_field_values"=>{}, "project_id"=>8, "done_ratio"=>"0", "su
bject"=>"Trench", "tracker_id"=>2, "description"=>"Dig trench for foundation"}}
WARNING: Can't verify CSRF token authenticity
Filter chain halted as :authorize rendered or redirected
Completed 401 Unauthorized in 195ms (ActiveRecord: 1.8ms)
```

Should RedminePro be adding the CSRF header? It seems like that would break a simple REST implementation especially considering that the API key for REST use appears to be there explicitly to avoid this mess.

#### #13 - 2012-12-12 09:48 - Terence Mill

I'm using redmine 2.1.4

The same problem occours for Fat Client Redmine Client from Mana-Sys. But only on write (Post) operation not or read access.

```
WARNING: Can't verify CSRF token authenticity
```

#### #14 - 2015-01-22 17:19 - @ go2null

related to Defect #15424

#### #15 - 2015-01-23 06:43 - Mischa The Evil

*- Status changed from New to Needs feedback*

@ go2null wrote:

> related to Defect #15424

That would also mean that the issues reported in this issue were fixed starting from Redmine 2.4.0.
Can anybody acknowledge this?

#### #16 - 2015-01-23 06:43 - Mischa The Evil

*- Related to Defect #15424: Filter chain halted as :verify_authenticity_token rendered or redirected added*