Redmine - Defect #11797

Using the API logs out my browser session

2012-09-07 13:46 - Gavin Davies

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	80%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Fixed	**Affected version:**	1.3.3

Description

I am building a bookmarklet that displays issues on a Kanban board. Everything works, but as soon as I, for example, post:

```
{"issue":{"status_id":3}}
```

to https://localhost/issues/3.json, my browser session gets logged out.

My redmine session ID remains the same, so it seems that something in Redmine is saying "this guy is posting to the API via his API key, therefore log him out of his browser session". Is this correct? Have I misunderstood?

Any advice would be appreciated!

Related issues:

Related to Redmine - Defect #15427: REST API POST and PUT broken	**Closed**

History

#1 - 2012-09-07 13:50 - Gavin Davies

If I use another user's API key, I get the same result, so it must be the jQuery call I'm using, which looks like:

```
jQuery.ajax(redmineRoot + 'issues/' + issueId + '.json', {
        headers: {
            'X-Redmine-API-Key': API_KEY,
            'Content-Type': 'application/json'
        },
        processData: false,
        dataType: 'json',
        data: JSON.stringify({issue:{status_id: newStatusId}}),
        type: 'PUT'
    });
```

#2 - 2012-09-07 14:05 - Gavin Davies

correction; it does change my session ID, it just has a prefix which made me think it was the same

#3 - 2012-09-07 16:33 - Gavin Davies

This occurs with PUT and POST, but not with GET - GET requests work as expected - I can browse through the issues using GET and it doesn't hose my session

#4 - 2012-09-08 09:14 - Jean-Philippe Lang

- Category set to REST API

#5 - 2012-09-10 13:28 - Gavin Davies

- % Done changed from 0 to 50

It seems to be to do with the handle_unverified_request method - if I make the following change, it no longer logs me out:

```
  def handle_unverified_request
    return # This is the change that stops it from logging me out
    super
    cookies.delete(:autologin)
  end
```

So there must be some kind of verification going on beyond simply supplying an API key... With that, it sets the autologin cookie, effectively logging my browser session out.

#6 - 2012-09-10 17:10 - Gavin Davies

- % Done changed from 50 to 80

This patch eliminates the issue:

```
From 9db6f1503c9b63a604254a46b37c8ca35f8f5e81 Mon Sep 17 00:00:00 2001
From: Gavin Davies <gavin.davies@boxuk.com>
Date: Mon, 10 Sep 2012 15:36:10 +0100
Subject: [PATCH] Allowing the API to do PUT and POST access without logging
 the user out, provided a valid API key is supplied. Allows
 bookmarklets to work without hosing user's session.

Making changes that Gareth recommended
---
 app/controllers/application_controller.rb |    7 +++++++
 1 files changed, 7 insertions(+), 0 deletions(-)

diff --git a/app/controllers/application_controller.rb b/app/controllers/application_controller.rb
index 483dcf0..d1ba117 100644
--- a/app/controllers/application_controller.rb
+++ b/app/controllers/application_controller.rb
@@ -28,6 +28,13 @@ class ApplicationController < ActionController::Base

   protect_from_forgery
   def handle_unverified_request
+    if request.post? || request.put?
+      if User.find_by_api_key(api_key_from_request)
+        # this is an API request, don't log the user out
+        return
+      end
+    end
+
     super
     cookies.delete(:autologin)
   end
--
1.7.5.4
```

Please update this ticket if you find a better way of doing this. Thanks!

#7 - 2018-05-12 09:42 - Martin Cizek

Seems to be fixed by #15427.

#8 - 2018-05-13 06:55 - Go MAEDA

- Status changed from New to Closed

- Resolution set to Fixed

Martin Cizek wrote:

> Seems to be fixed by #15427.

Thank you for pointing it out. I agree with Martin Cizek because the problem was caused by unnecessary deletion of autologin cookies and it will never happen for API requests after r12311, the change made by #15427.

#9 - 2018-05-13 06:55 - Go MAEDA

- Related to Defect #15427: REST API POST and PUT broken added