ChiliProject - Bug # 735: any user can edit time entries via context menu

Status:	Closed	**Priority:**	Normal
Author:	Holger Just	**Category:**	
Created:	2011-11-26	**Assignee:**	Holger Just
Updated:	2011-11-30	**Due date:**	
Remote issue URL:	http://www.redmine.org/issues/9405		
Affected version:			

Description:	Any user can update all time entries via the context menu. see related issue for more info.
	
	Mail by Jan Schulz-Hofen on 2011-11-25 09:12 UTC:
	<pre>
	Hi guys,
	
	not sure if CP is affected and/or if you have seen this: http://www.redmine.org/issues/9405
	
	JPL has commited a fix for this tonight and I thought I'd let you know.
	</pre>		

Associated revisions

2011-11-30 08:27 pm - Holger Just

[#735] Don't allow time entry edits with only log_time permission

Based on a patch by Jean-Philippe Lang.

2011-11-30 08:27 pm - Holger Just

[#735] Don't allow time entry creation with only edit permission

Based on a patch by Jean-Philippe Lang.

2011-11-30 08:28 pm - Holger Just

[#735] Log time form on issue update should only be displayed with log_time permission

Based on a patch by Jean-Philippe Lang.

History

2011-11-28 07:58 pm - Holger Just

- Assignee set to Holger Just

It turns put that we are not affected by the bug as is, as we don't allow bulk update of time entries currently.

Nevertheless, the permissions should be reduced down which I did and am going to commit later. Only question that remains is if we still handle this as a security issue or not. Any ideas?

<pre>
diff --git a/app/views/issues/_edit.rhtml b/app/views/issues/_edit.rhtml
index d376b36..c73b298 100644
--- a/app/views/issues/_edit.rhtml
+++ b/app/views/issues/_edit.rhtml
@@ -15,7 +15,7 @@
    <%= render :partial => (@edit_allowed ? 'form' : 'form_update'), :locals => {:f => f} %>

```
        </fieldset>
    <% end %>
-   <% if authorize_for('timelog', 'edit') %>
+    <% if User.current.allowed_to?(:log_time, @project) %>
        <fieldset class="tabular"><legend><%= l(:button_log_time) %></legend>
        <% fields_for :time_entry, @time_entry, { :builder => TabularFormBuilder, :lang => current_language} do |time_entry| %>
        <div class="splitcontentleft">
@@ -26,7 +26,7 @@
        </div>
        <p><%= time_entry.text_field :comments, :size => 60 %></p>
        <% @time_entry.custom_field_values.each do |value| %>
-            <p><%= custom_field_tag_with_label :time_entry, value %></p>
+          <p><%= custom_field_tag_with_label :time_entry, value %></p>
        <% end %>
diff --git a/app/views/issues/_edit.rhtml b/app/views/issues/_edit.rhtml
index d376b36..c73b298 100644
--- a/app/views/issues/_edit.rhtml
+++ b/app/views/issues/_edit.rhtml
@@ -15,7 +15,7 @@
        <%= render :partial => (@edit_allowed ? 'form' : 'form_update'), :locals => {:f => f} %>
        </fieldset>
    <% end %>
-   <% if authorize_for('timelog', 'edit') %>
+    <% if User.current.allowed_to?(:log_time, @project) %>
        <fieldset class="tabular"><legend><%= l(:button_log_time) %></legend>
        <% fields_for :time_entry, @time_entry, { :builder => TabularFormBuilder, :lang => current_language} do |time_entry| %>
        <div class="splitcontentleft">
@@ -26,7 +26,7 @@
        </div>
        <p><%= time_entry.text_field :comments, :size => 60 %></p>
        <% @time_entry.custom_field_values.each do |value| %>
-            <p><%= custom_field_tag_with_label :time_entry, value %></p>
+          <p><%= custom_field_tag_with_label :time_entry, value %></p>
        <% end %>
        <% end %>
    </fieldset>
diff --git a/lib/redmine.rb b/lib/redmine.rb
index 16f5922..716fb4a 100644
--- a/lib/redmine.rb
+++ b/lib/redmine.rb
@@ -100,10 +100,10 @@ Redmine::AccessControl.map do |map|
  end

  map.project_module :time_tracking do |map|
-   map.permission :log_time, {:timelog => [:new, :create, :edit, :update]}, :require => :loggedin
+   map.permission :log_time, {:timelog => [:new, :create]}, :require => :loggedin
    map.permission :view_time_entries, :timelog => [:index, :show], :time_entry_reports => [:report]
-   map.permission :edit_time_entries, {:timelog => [:new, :create, :edit, :update, :destroy]}, :require => :member
-   map.permission :edit_own_time_entries, {:timelog => [:new, :create, :edit, :update, :destroy]}, :require => :loggedin
+   map.permission :edit_time_entries, {:timelog => [:edit, :update, :destroy]}, :require => :member
+   map.permission :edit_own_time_entries, {:timelog => [:edit, :update, :destroy]}, :require => :loggedin
    map.permission :manage_project_activities, {:project_enumerations => [:update, :destroy]}, :require => :member
  end
```

```
diff --git a/test/functional/issues_controller_test.rb b/test/functional/issues_controller_test.rb
index c5b2270..27930f6 100644
--- a/test/functional/issues_controller_test.rb
+++ b/test/functional/issues_controller_test.rb
@@ -781,6 +781,22 @@ class IssuesControllerTest < ActionController::TestCase
     assert_tag :input, :attributes => { :name => 'time_entry[comments]', :value => 'test_get_edit_with_params' }
   end

+  def test_get_edit_should_display_the_time_entry_form_with_log_time_permission
+    @request.session[:user_id] = 2
+    Role.find_by_name('Manager').update_attribute :permissions, [:view_issues, :edit_issues, :log_time]
+
+    get :edit, :id => 1
+    assert_tag 'input', :attributes => {:name => 'time_entry[hours]'}
+  end
+
+  def test_get_edit_should_not_display_the_time_entry_form_without_log_time_permission
+    @request.session[:user_id] = 2
+    Role.find_by_name('Manager').remove_permission! :log_time
+
+    get :edit, :id => 1
+    assert_no_tag 'input', :attributes => {:name => 'time_entry[hours]'}
+  end
+
   def test_update_edit_form
     @request.session[:user_id] = 2
     xhr :post, :new, :project_id => 1,
diff --git a/test/functional/timelog_controller_test.rb b/test/functional/timelog_controller_test.rb
index a869e66..103c1ca 100644
--- a/test/functional/timelog_controller_test.rb
+++ b/test/functional/timelog_controller_test.rb
@@ -111,6 +111,18 @@ class TimelogControllerTest < ActionController::TestCase
     assert_equal 3, t.user_id
   end

+  def test_create_without_log_time_permission_should_be_denied
+    @request.session[:user_id] = 2
+    Role.find_by_name('Manager').remove_permission! :log_time
+    post :create, :project_id => 1,
+                :time_entry => {:activity_id => '11',
+                                :issue_id => '',
+                                :spent_on => '2008-03-14',
+                                :hours => '7.3'}
+
+    assert_response 403
+  end
+
   def test_update
     entry = TimeEntry.find(1)
     assert_equal 1, entry.issue_id
</pre>
```

2011-11-30 07:33 pm - Holger Just

- Status changed from Open to Closed

This is part of 2.5.0.

2011-11-30 07:35 pm - Holger Just

- Project changed from Security to ChiliProject

As this issue is confirmed to not affect the security of an out-of-the-box ChiliProject I'm making it public.