Creating Visits Part 2

Sergio Revilla
@elreplicante

based on Martin Tschischauskas (@martynasc) slides

Unknown action

The action 'create' could not be found for VisitsController

Implementing the `create` action

`app/controllers/visits_controller.rb`

```ruby
class VisitsController < ApplicationController
 def create
 end
end
```

Template is missing

Missing template visits/create, application/create with {:locale=>[:en], :formats=>[:html], :variants=>[], :handlers=>[:erb, :builder, :raw, :ruby, :jbuilder, :coffee]}. Searched in: * "/vagrant/meet_me/app/views"

The log!

```
Started POST "/locations/3/visits" for 10.0.2.2 at 2014-07-09 15:58:16 +0000
Processing by VisitsController#create as HTML
  Parameters: {"utf8"=>"✓", "authenticity_token"=>"kSGQM+NJDRuMLdk/u/7/
yY8odvj870UgBHOJo0Evm8w=", "visit"=>{"user_name"=>"Martin",
"from_date(1i)"=>"2014", "from_date(2i)"=>"7", "from_date(3i)"=>"10",
"from_date(4i)"=>"15", "from_date(5i)"=>"56", "to_date(1i)"=>"2015",
"to_date(2i)"=>"7", "to_date(3i)"=>"10", "to_date(4i)"=>"15", "to_date(5i)"=>"56"},
"commit"=>"Save", "location_id"=>"3"}
Completed 500 Internal Server Error in 27ms
```

The log!

"visit"=>{"user_name"=>"Martin", "from_date(1i)"=>"2014", "from_date(2i)"=>"7", "from_date(3i)"=>"10", "from_date(4i)"=>"15", "from_date(5i)"=>"56", "to_date(1i)"=>"2015", "to_date(2i)"=>"7", "to_date(3i)"=>"10", "to_date(4i)"=>"15", "to_date(5i)"=>"56"}, "commit"=>"Save", "location_id"=>"3"}

params variable

IRON HACK

The form

```
<form accept-charset="UTF-8" action="/locations/3/visits" class="new_visit"
id="new_visit" method="post">

  <label for="visit_user_name">User name</label>
  <input id="visit_user_name" name="visit[user_name]" type="text" />
  <br/>
  <select id="visit_from_date_1i" name="visit[from_date(1i)]">
<option value="2009">2009</option>
...
</select>

  <br/>
  <input name="commit" type="submit" value="Save" />
</form>
```

Implementing the `create` action

```
def create
  @location = Location.find(params[:location_id])
  @visit = @location.visits.new params[:visit]

    if @visit.save
      redirect_to action: 'index', controller: 'visits',
location_id: @location.id
    else
      render 'new'
    end
  end
```

Implementing the `create` action

1. Load existing location

```
@location = Location.find(params[:location_id])
```

Implementing the `create` action

2. Instantiate a new visit in the loaded location with the data from the form

```
@visit = @location.visits.new params[:visit]
```

Implementing the `create` action

3. Try to save in the database:
  - if success, then perform a redirection
  - if fails, render the “new” form

```
    if @visit.save
      redirect_to action: 'index', controller: 'visits',
location_id: @location.id
    else
      render 'new'
    end
```

ActiveModel::ForbiddenAttributesError in VisitsController#create

ActiveModel::ForbiddenAttributesError

Extracted source (around line **#10**):

```
8   def create
9     @location = Location.find(params[:location_id])
10    @visit = @location.visits.new params[:visit]
11
12    if @visit.save
13      redirect_to action: 'index', controller: 'visits', location_id: @location.id
```

Strong Parameters!

Understanding mass assignments

"visit"=>{"user_name"=>"Martin", "from_date(1i)"=>"2014", "from_date(2i)"=>"7", "from_date(3i)"=>"10", "from_date(4i)"=>"15", "from_date(5i)"=>"56", "to_date(1i)"=>"2015", "to_date(2i)"=>"7", "to_date(3i)"=>"10", "to_date(4i)"=>"15", "to_date(5i)"=>"56"}, "commit"=>"Save", "location_id"=>"3"}

```
@visit = @location.visits.new params[:visit]
```

params assignment

IRON HACK

Understanding mass assignments

- Imagine our application implements a model User
- A location entry belongs to a user
- The attacker could add a hidden text field into the existing form with the name “visit[user_id]”

Understanding mass assignments

“visit”=>{“user_name”=>"Martin",...
“user_id”=> 1
}, "commit"=>"Save", "location_id"=>"3"}

“visit”=>{“user_name”=>"Martin",...
“user_id”=> 666
}, "commit"=>"Save", "location_id"=>"3"}

IRON HACK

Understanding mass assignments

```
def create
  @location = Location.find(params[:location_id])
  @visit = @location.visits.new params[:visit]

    if @visit.save
      redirect_to action: 'index', controller: 'visits',
location_id: @location.id
    else
      render 'new'
    end
  end
```

Understanding mass assignments

```
def create
    @location = Location.find(params[:location_id])
    @visit = @location.visits.new params[:visit]
    @visit.user = User.find(session[:user_id])

    if @visit.save
      redirect_to action: 'index', controller: 'visits',
location_id: @location.id
    else
      render 'new'
    end
  end
```

Back to our app…

Rails Strong Parameters

```ruby
class VisitsController < ApplicationController
  …
  private

  def visit_params
    params.require(:visit).permit(:user_name, :from_date, :to_date)
  end
end
```

Rails Strong Parameters

```
def create
    @location = Location.find(params[:location_id])
    @visit = @location.visits.new visit_params
    if @visit.save
      redirect_to action: 'index', controller: 'visits',
location_id: @location.id
    else
      render 'new'
    end
  end
```

Displaying validation errors

- User name can't be blank

User name

2014 July 10 — 16 : 26

2014 July 10 — 16 : 26

Save

```
> l = Location.new
> l.errors.empty?
=> true
> l.valid?
=> false
```

validations

```
> l.errors.empty?
=> false
> l.errors.size
=> 2
> l.errors.full_messages
=> ["Name can't be blank", "Name is invalid"]
```

```
<% if @visit.errors.any? %>
  <ul>
  <% @visit.errors.full_messages.each do |error_message| %>
    <li><%= error_message %></li>
  <% end %>
  </ul>
<% end %>

<%= form_for [@location, @visit] do |f| %>
  <%= f.label :user_name %>
  <%= f.text_field :user_name %>
  <br/>
  <%= f.datetime_select(:from_date, default: Time.now + 1.days ) %>
  <br/>
  <%= f.datetime_select(:to_date, default: Time.now + 1.days ) %>
  <br/>
  <%= f.submit "Save" %>
<% end %>
```

```
 <div class="field_with_errors"><label for="visit_user_name">User name</label></div>
  <div class="field_with_errors"><input id="visit_user_name" name="visit[user_name]" type="text" value="" /></div>
```