

Rails 第三课: Rails 101 (/courses/3/syllabus)

🔍 搜索本课程教材

📄 概览 (/courses/3)

📖 作业 (/courses/3/assignments)

🗨️ FAQ (/courses/3/faqs)

🌟 积分榜 (/courses/3/leaderboard)

👤 1位同学正在浏览当前页面

📑 教材 (/courses/3/syllabus)

📅 动态 (/courses/3/activities)

🔖 (/favorites?post\_id=74)

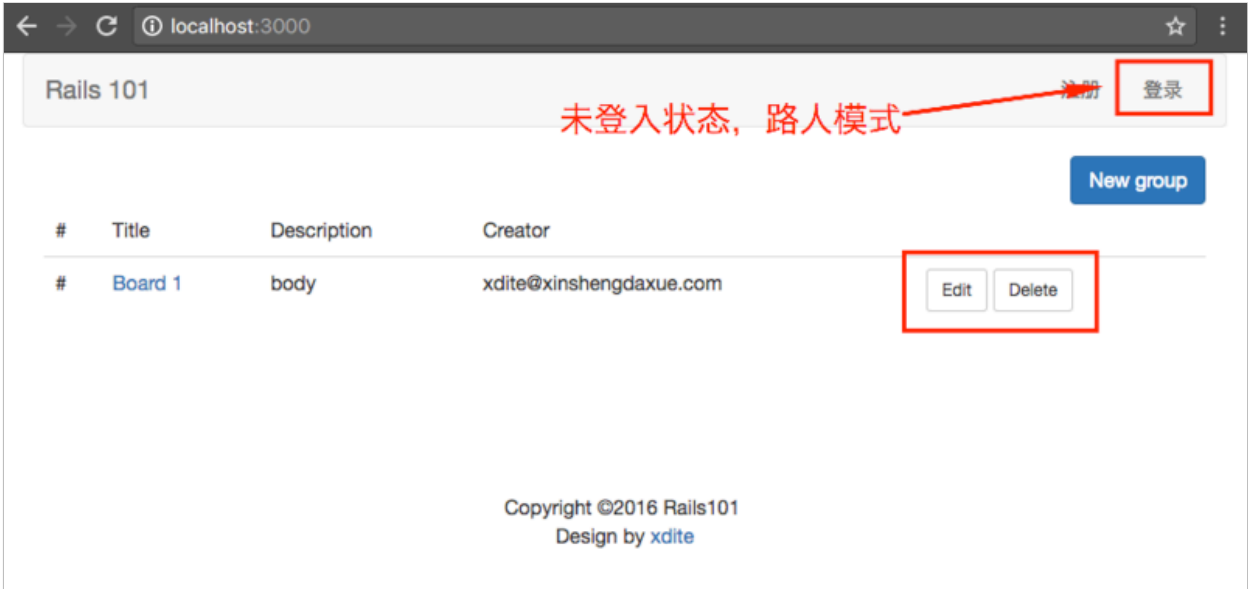
## 目标

- 路人不应该可以看到“编辑”“删除”按钮
- 只有群组的“创始者”可以实际执行“编辑”“删除”群组资讯

## 步骤

### Step 1: 路人不应该可以看到“编辑”“删除”按钮

让我们登出系统，在这里我们察觉一个严重的问题：明明是路人，怎么能看到“编辑”“删除”按钮的资讯呢？



(https://s3-ap-northeast-1.amazonaws.com/ontrackapp-production/Cs72Y8u2Sf6iuS6b7Gqg\_Screenshot%20at%20Feb%2024%2017-55-57.png)

所以在这里我们要把“编辑”“删除”这两个按钮藏起来，限定

- 只有登入模式下

- 而且还必须是群组“创始者”

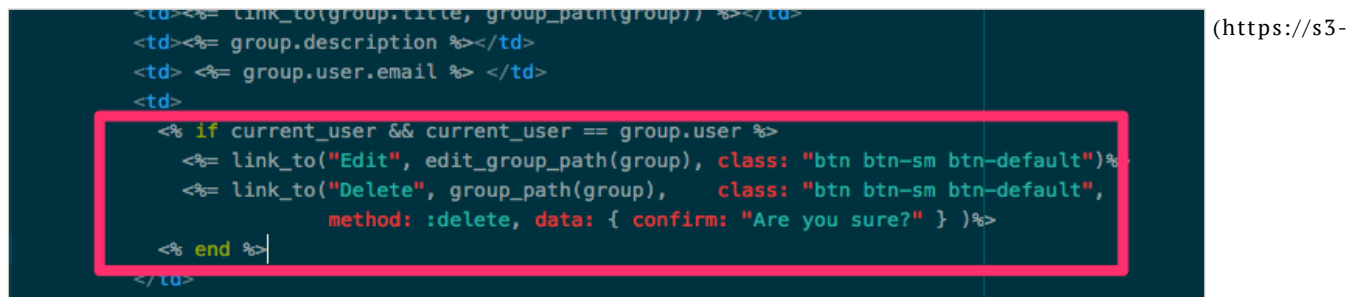
才能看得到这个两个按钮，否则路人是看不到的。

修改 app/views/groups/index.html.erb

加入 `<% if current_user == group.user %>` 的判断式

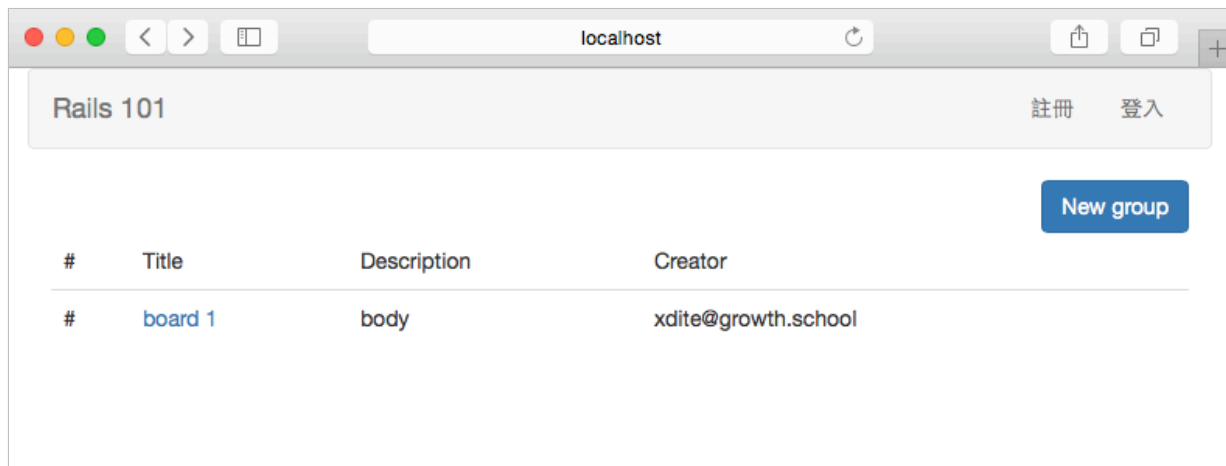
```
app/views/groups/index.html.erb

<td>
+   <% if current_user == group.user %>
+     <%= link_to("Edit", edit_group_path(group), class: "btn btn-sm btn-default")%>
+     <%= link_to("Delete", group_path(group), class: "btn btn-sm btn-default",
+       method: :delete, data: { confirm: "Are you sure?" } )%>
+   <% end %>
</td>
```



ap-northeast-1.amazonaws.com/ontrackapp-production/uheHTau6QMS4ALdpjTEG\_current\_user\_index.png)

重新刷新首页，路人现在就看不到按钮了。



(https://s3-ap-northeast-1.amazonaws.com/ontrackapp-production/1IpxQvwNQmQ854xXdUd\_%E8%9E%A2%E5%B9%95%E5%BF%AB%E7%85%A7%202016-07-11%20%E4%B8%8B%E5%8D%88.32.54.png)

## Step 2: git 存档

```
git add .
git commit -m "people can't see edit button unless he is group owner"
```

## Step 3: 路人不应该也可以“直接输入网址”去存取 edit / update / destroy action

除了将按钮对路人隐藏外，我们还要考虑到一个情形，假设这个路人是知道 Rails 规则的，那么他可能输入

```
http://localhost:3000/groups/某笔数据的ID/edit
```

网址，就直接可以编辑数据。

我们也要在 controller 做权限判断，滤掉这种人。

首先，我们先限定 edit / update / destroy 这三个操作动作，必须要是“登入”的使用者才能存取。

修改 app/controllers/groups\_controller.rb 在 before\_action :authenticate\_user! 列表中，加入 :edit, :update, :destroy

```
app/controllers/groups_controller.rb
class GroupsController < ApplicationController
  before_action :authenticate_user! , only: [:new, :create, :edit, :update, :destroy]
```

这样“没登录”的路人，就进不来了。但这只是第一步。

#### Step 4: 必须要是 group 拥有人，才能进入 edit，否则会被重导至首页，并显示错误信息。

修改 app/controllers/groups\_controller.rb 加入权限，如果不是“创始者”去存取，会显示没有权限的错误信息。

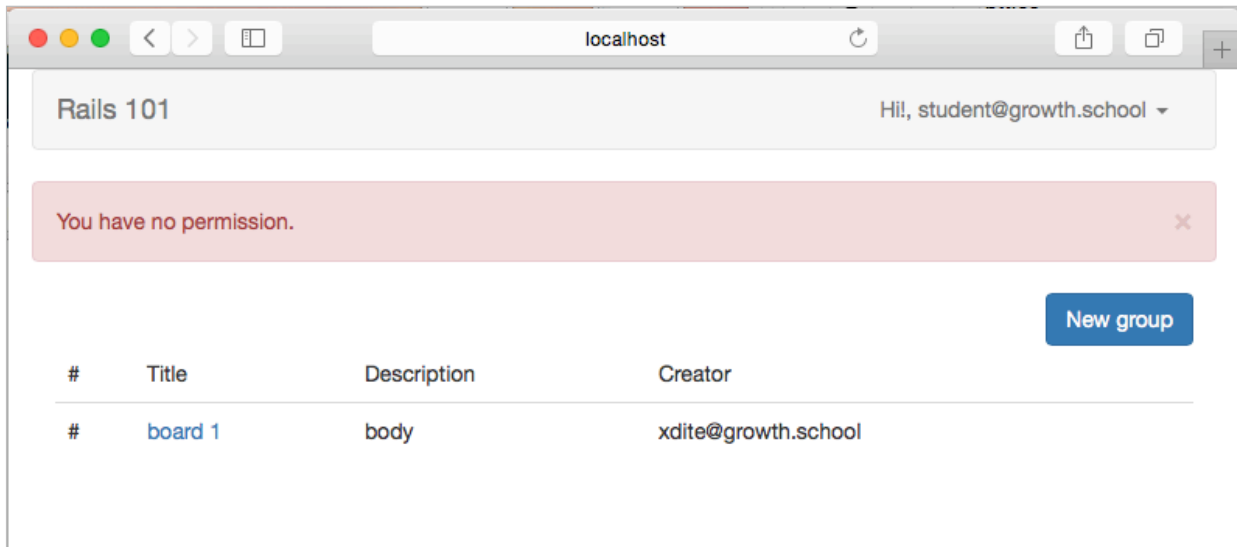
```
app/controllers/groups_controller.rb
def edit
  @group = Group.find(params[:id])

  if current_user != @group.user
    redirect_to root_path, alert: "You have no permission."
  end
end
```

这样当其他人，试图输入

```
http://localhost:3000/groups/某笔数据的ID/edit
```

这样的网址，想要编辑数据，就会被挡住。



(https://s3-ap-northeast-1.amazonaws.com/ontrackapp-production/zH1yGZ9OTXiSXeIaCgdE\_%E8%9E%A2%E5%B9%95%E5%BF%AB%E7%85%A7%202016-07-11%20%E4%B8%8B%E5%8D%88.48.01.png)

## Step 5: 依样画葫芦的把“权限检查”的代码，套用到 update / destroy 上

修改 app/controllers/groups\_controller.rb 中的 update 与 destroy 部分。

```
app/controllers/groups_controller.rb

def update
  @group = Group.find(params[:id])

  if current_user != @group.user
    redirect_to root_path, alert: "You have no permission."
  end

  if @group.update(group_params)
    redirect_to groups_path, notice: "Update Success"
  else
    render :edit
  end
end

def destroy
  @group = Group.find(params[:id])

  if current_user != @group.user
    redirect_to root_path, alert: "You have no permission."
  end

  @group.destroy
  redirect_to groups_path, alert: "Group deleted"
end
```

## Step 6: git 存档

```
git add .
git commit -m "check owner permission when access edit/update/destroy"
```

## Step 7: 制作 find\_group\_and\_check\_permission

---

我们发现 edit、update、destroy 这三个 action 都有一样的代码，看起来有点冗。

```
@group = Group.find(params[:id])

if current_user != @group.user
  redirect_to root_path, alert: "You have no permission."
end
```

其实我们可以透过把它包装成一个函式的方式 find\_group\_and\_check\_permission 去省略这段冗余代码。

打开 app/controllers/groups\_controller.rb 在 private 下，新增一个 find\_group\_and\_check\_permission

```
app/controllers/groups_controller.rb

private

def find_group_and_check_permission
  @group = Group.find(params[:id])

  if current_user != @group.user
    redirect_to root_path, alert: "You have no permission."
  end
end

def group_params
  params.require(:group).permit(:title, :description)
end

end
```

再修正 edit

```
app/controllers/groups_controller.rb

def edit
  find_group_and_check_permission
end
```

修正 update

```
app/controllers/groups_controller.rb

def update

  find_group_and_check_permission

  if @group.update(group_params)
    redirect_to groups_path, notice: "Update Success"
  else
    render :edit
  end
end
```

修正 destroy

```
app/controllers/groups_controller.rb
```

```
def destroy
  find_group_and_check_permission

  @group.destroy
  redirect_to groups_path, alert: "Group deleted"
end
```

## Step 8: 把 find\_group\_and\_check\_permission 挂到 before\_action

---

开发到这里你会发现一件事，find\_group\_and\_check\_permission 其实都是在这三个 action 的最前面开头执行的，所以你甚至可以这样写，把 find\_group\_and\_check\_permission 挂到 before\_action

```
app/controllers/groups_controller.rb
class GroupsController < ApplicationController

  before_action :authenticate_user! , only: [:new, :create, :edit, :update, :destroy]
  before_action :find_group_and_check_permission, only: [:edit, :update, :destroy]
```

然后再把 edit update destroy 里的 find\_group\_and\_check\_permission 砍掉。变成这样：

```
app/controllers/groups_controller.rb

def edit
end

def update
  if @group.update(group_params)
    redirect_to groups_path, notice: "Update Success"
  else
    render :edit
  end
end

def destroy
  @group.destroy
  redirect_to groups_path, alert: "Group deleted"
end
```

## Step 9: git 存档

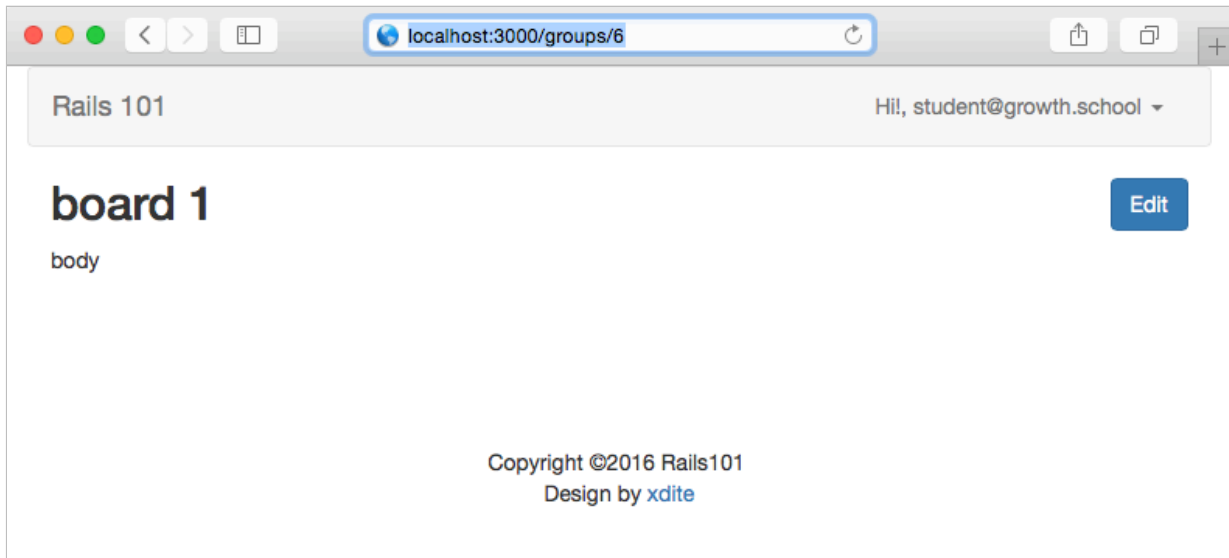
---

```
git add .
git commit -m "use before_action to find_group_and_check_permission"
```

## Step 10 : 修掉 show 里面的 Edit 按钮

---

做到这里，我们还发现一个地方，我们漏了改，那就是 show.html.erb 上面，还有一个 Edit 按钮我们还没有拔掉。



(https://s3-ap-northeast-1.amazonaws.com/ontrackapp-production/qpaQo94hQ0Cj48Bq69fI\_%E8%9E%A2%E5%B9%95%E5%BF%AB%E7%85%A7%202016-07-11%20%E4%B8%8B%E5%8D%889.26.46.png)

修改 app/views/groups/show.html.erb , 然后加入

加入 `<% if current_user && current_user == @group.user %>` 的判断式

```
<div class="col-md-12">
  <div class="group">
    <% if current_user && current_user == @group.user %>
      <%= link_to("Edit", edit_group_path(@group), class: "btn btn-primary pull-right")%>
    <% end %>
  </div>
  <h2><%= @group.title %></h2>
  <p><%= @group.description %></p>
</div>
```

(https://s3-ap-

northeast-1.amazonaws.com/ontrackapp-production/cbnKVjtaT1Cn9rz3mIQB\_show\_html\_erb.png)

app/views/groups/show.html.erb

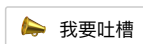
```
<div class="group">
  <% if current_user && current_user == @group.user %>
    <%= link_to("Edit", edit_group_path(@group), class: "btn btn-primary pull-right")%>
  <% end %>
</div>
```


如此按钮就被修掉了。

## Step 11: git 存档


```
git add .
git commit -m "add permission check on show page"
```

对本页内容的感受如何?



 So easy

 还OK

 崩溃了

← 上一页 (/posts/73)

🔍 可以使用 ← → 键进行翻页

下一页 → (/posts/75)

🔍 本节常见问题

= 与 == 与 != 他们三者是什么?

\* = 是指派。@groups = Group.all, 把 Group.all 数值 指派给 @groups 的意思。

\* == "等于"

\* != "不等于"

<div>全栈营</div> <div>课程介绍</div> <div>(/pages/course_intro)</div> <div>教学团队</div> <div>(/pages/teachers)</div> <div>学员心得</div> <div>(/pages/students)</div>	<div>课程资源</div> <div>学习中心</div> <div>(/dashboard)</div> <div>帮助文档</div> <div>(http://docs.qzy.camp/)</div> <div>交流论坛</div> <div>(http://forum.qzy.cn/)</div>	<div>关于我们</div> <div>公司介绍</div> <div>(/pages/about)</div> <div>常见问题</div> <div>(/pages/faq)</div> <div>联系方式</div> <div>(/pages/contact)</div>	<div>💬 在线客服 (非技术答疑, 工作日10:00-19:00)</div> <div> 新生大学 - 软件学院是李笑来对未来世界的实验计划, 旨在改变中国的计算机教育。 (http://www.xinshengdaxue.com/)</div>
-----------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------