Hide Email in Search Results Documentation

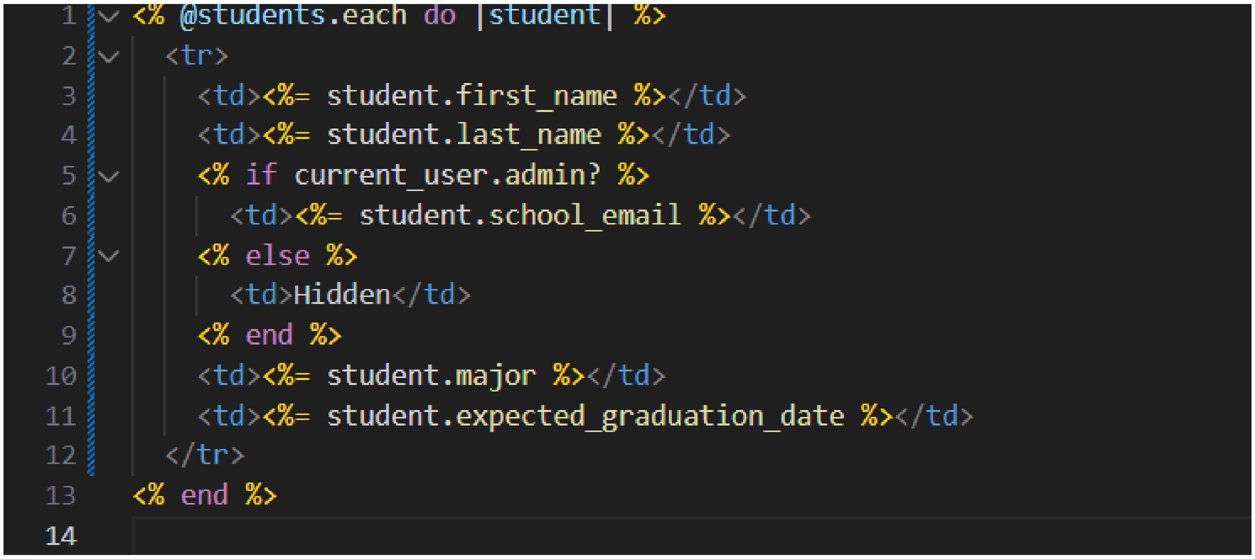
User Goal: Make the privacy of the application better by hiding students' email addresses from general view in search results, making them visible only to users with the appropriate permissions (e.g., administrators).

Implementation Steps

1. Modifications in the View: app\views\students_search_form.html.erb

To prevent unauthorized access to student emails, conditionally render the email field in search results based on the user's permissions. This step requires adding a condition to check if the user has admin or privileged access (or however access is managed) before displaying the email.

Assuming an admin? method or a similar permission check for the user:



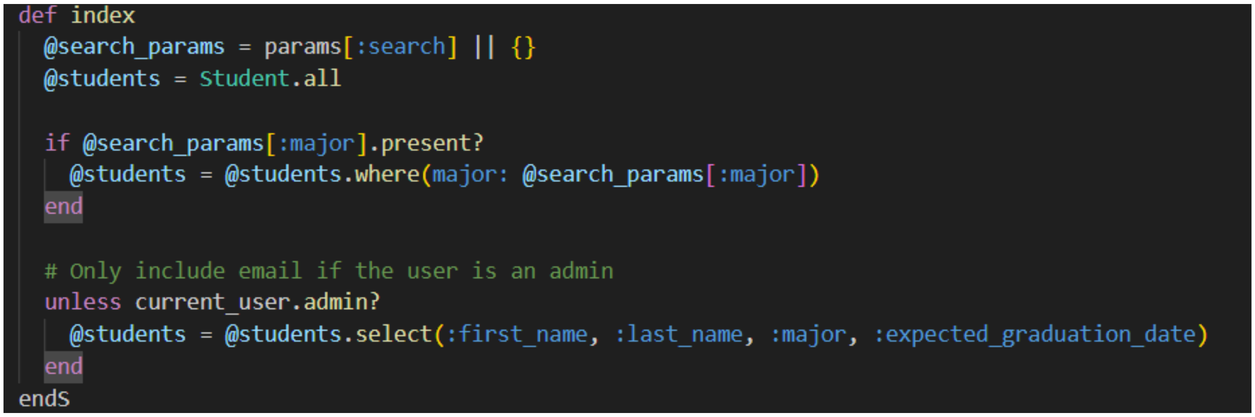
```
<% @students.each do |student| %>
  <tr>
    <td><%= student.first_name %></td>
    <td><%= student.last_name %></td>
    <% if current_user.admin? %>
      <td><%= student.school_email %></td>
    <% else %>
      <td>Hidden</td>
    <% end %>
    <td><%= student.major %></td>
    <td><%= student.expected_graduation_date %></td>
  </tr>
<% end %>
```

Here, current_user.admin? checks whether the user has the necessary privileges to view the email field. For non-admin users, "Hidden" displays instead of the email address.

2. Controller Adjustments: StudentsController.

The StudentsController manages how data is fetched and displayed. Since there isn't a dedicated search results view, verify that the controller isn't over-fetching data that users aren't authorized to view. Implement conditional data filtering if necessary.

For example, in the index action, add logic to exclude email details unless the user has admin rights:



```ruby
def index
  @search_params = params[:search] || {}
  @students = Student.all

  if @search_params[:major].present?
    @students = @students.where(major: @search_params[:major])
  end

  # Only include email if the user is an admin
  unless current_user.admin?
    @students = @students.select(:first_name, :last_name, :major, :expected_graduation_date)
  end
endS
```

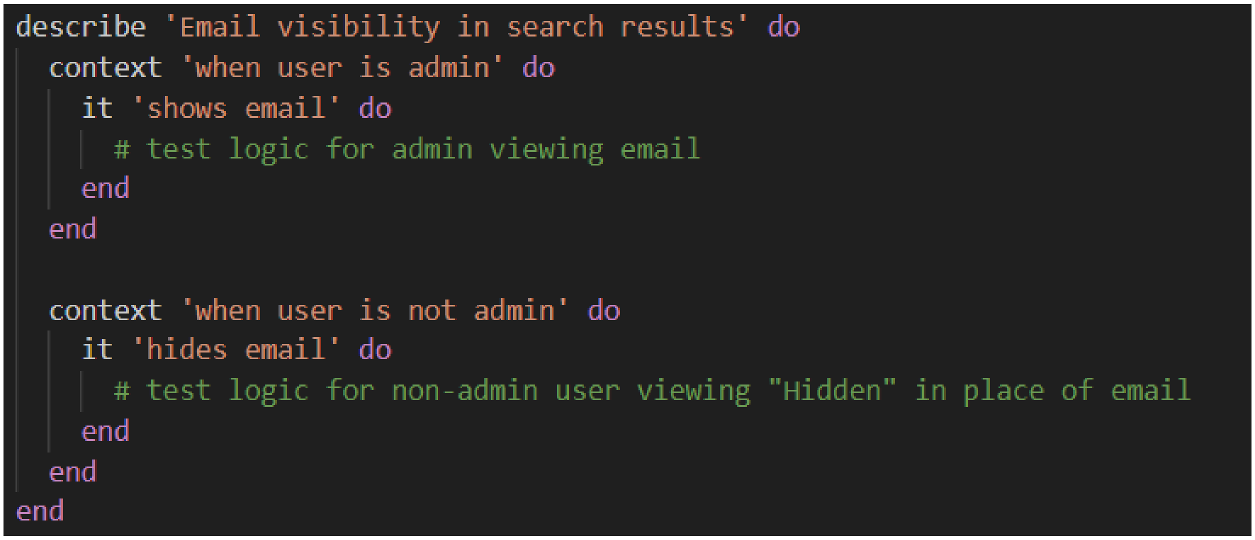
This ensures that if a non-admin user queries the database, they won't retrieve email data, even if they attempt to manipulate parameters.

3. Testing

RSpec Testing:

- Create tests to verify that:
  - Admin users can view the email field in search results.
  - Non-admin users cannot see the email field, and instead see "Hidden."
  - Manipulation of parameters does not expose emails to unauthorized users

Example RSpec test for email visibility:



```ruby
describe 'Email visibility in search results' do
  context 'when user is admin' do
    it 'shows email' do
      # test logic for admin viewing email
    end
  end

  context 'when user is not admin' do
    it 'hides email' do
      # test logic for non-admin user viewing "Hidden" in place of email
    end
  end
end
```