string quartet

Code Critique by Consonance

User Email Validation

Sashko Stubailo

```
# query mit people search to confirm valid mit email
@kerberos = @user.email.split('@')[0]
@info = RestClient.get 'http://web.mit.edu/bin/cgicso?' ,
    {:params => {:options => "general", :query => @kerberos, :output =>
'json'}}

responseEmail = @kerberos + "@MIT.EDU"
respond_to do |format|
  if @info.include? responseEmail
    if @user.save # ...truncated
```

The intention is to check whether the email address submitted is a real MIT email address.

However, this only checks the characters in the email string up to the first ‘@’ symbol against the people search API.

Even if a regex was added to check for “@mit.edu”, this validation scheme would accept substrings of valid MIT emails.

Invalid Email Addresses Accepted:

- **sashko@gmail.com**
- **ashko@mit.edu** # doesn’t exist
- **o@more@symbols@please**
- **sashko** # not an email address

(tested on the live site)

Incoming Emails Creation

Victor Pontis

```
# Incoming Emails Controller
skip_before_filter :verify_authenticity_token

# GET /locations/new
def new
  @incomingemails = Incomingemail.new
end
```

Lack of Authenticity Checking

I am able to post to create and trigger the create offering code without being logged in. The incoming emails controller skips verifying the authenticity token, but this method hasn't even been created. A user should be verified before letting them create an offering as the prescribed behavior in the design doc

Invalid Migrations

When I run rake db:migrate, an Incomingemails table is not created. This is because the migration files that create the Incomingemails table are corrupted. This breaks Incomingemails#new.

The schema file is correct but the migrations do not create the correct schema file.

Building Numbers

Santhosh Narayan

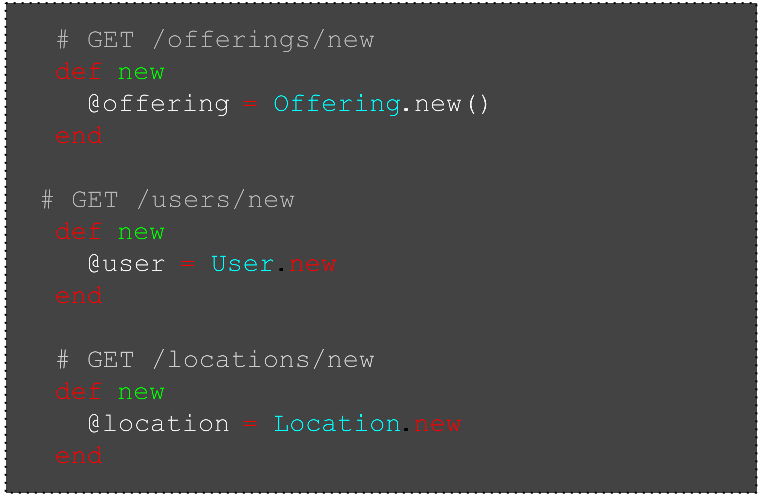
```
/Users/santhoshnarayan/Desktop/Ido-Efrati_cyjing_nitya-
subramanian_cjcai_final/app/assets/javascripts/location.js:
   89       if(signed_in){
   90         var infoWindowContent = [
   91        "<h2><b> Building "+String(bldgnum) + " - " + String(location_name)
+ "</b></h2>",
   92         "<h2>Post A New Byte </h2>",
   93         "<form id='map-form'>",
```

Undefined Building Numbers

While it is helpful to have both building numbers and names (i.e. Building 14 - Hayden Memorial Library), not all buildings have both a number and a name. Should check if bldgnum is defined as well or if the number is contained in the location name.

Examples

Search:	Result:
Pi Beta Phi	Building undefined - W51C
Theta	Building undefined - Theta Delta Chi (TDC)
Kappa Sigma	Building undefined - Phi Kappa Sigma (PKS)



```
  # GET /offerings/new
  def new
    @offering = Offering.new()
  end

 # GET /users/new
  def new
    @user = User.new
  end

  # GET /locations/new
  def new
    @location = Location.new
  end
```

Access to pages that shouldn’t exist:

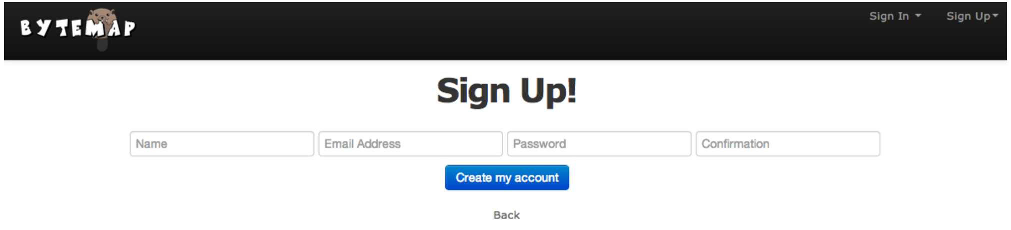
- new offering
- new user
- new location

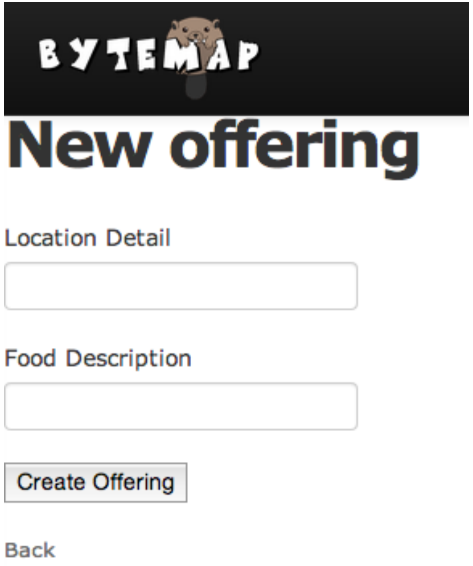
can all be accessed by hardcoding the url (i.e. .. /offerings/new)

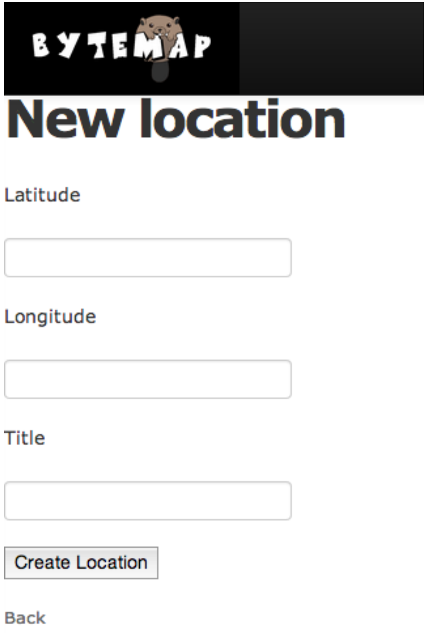
- When accessing form at ..location/new, it is possible to create a location that doesn’t fit within the map borders as well.

Examples:

David Sessoms


BYTEMAP
Sign In
Sign Up
Sign Up!
Name
Email Address
Password
Confirmation
Create my account
Back


BYTEMAP
New offering
Location Detail
Food Description
Create Offering
Back


BYTEMAP
New location
Latitude
Longitude
Title
Create Location
Back