Rails - Password Reset

Overview

How to create a password reset process in a Ruby on Rails 6.0 authentication system.

What's Required

A user wants to reset a forgotten password, so the required UI is:

* Forgotten password link on login page
* Forgotten password page where user can enter email, complete a captcha, and then request a password reset email
* Email to be sent to user when email entered is correct, including a password reset link with time based expiry
* Password reset form which can only be accessed by user with link allowing a user to submit a new password for user, then redirect back to login with notice of sucess

From the above required UI, the required backend is:

* Password reset token and sent date in the database, related to user
* Password controller:
  + GET /forgotten-password - Shows user form to reset password, generate a captcha to stop bots
  + POST /fogotten-password - Checks captcha, checks email, creates password reset token and sent at, creates and sends reset email, redirect user back to login with 'If user exists they will get a password reset link'
  + GET /reset-password - Checks token valid (if not redirects to login), displays reset form for username, adds token and username as hidden field to verify post request
  + POST /reset-password - Verifys token and user, resets password, redirects to login with message of sucess
* User model
  + Method to generate reset token and sent time
  + Method to check reset token in date and valid for username
  + Method to generate reset password link for email
* user-mailer
  + forgotten password email related to @user with expiry link

Process

User submits forgotten password form >> New async ResetPasswordJob created to check if user exists and if so tell model to send password reset email >> User model generates tokens and then tells PasswordMailer to send email >> PasswordMailer generates email from views and sends email

Create New Database Entries

Add new colums password\_reset\_token and password\_reset\_expiry to user table in database:

rails g migration AddPasswordResetToUsers password\_reset\_token:string password\_reset\_expiry:datetime

rails db:migrate

Create Password Controller

Generate new controller for password resets:

rails g controller password

Add forgotten-password action, route, and view, and request spec.

Create form and stylesheet for forgotten password.

Create POST route for forgotten-password.

add reCaptcha to form.

Create Model Methods

Add generate URL safe reset token method to User model.

Create a New Job for Sending Email

Add new job to rails, so password reset is performed outside of the request response cycle:

rails g job password\_reset

Include method to find user, then call email password reset mailer if user found.

Create PasswordMailer

Add new Mailer to rails to send password reset,:

rails g mailer password

Call mailer in controller and test call