Advanced Login

Tuesday, September 27, 2016 9:07 PM

- We are going to enhance the login system, adding a remember functionality via permanent cookies
- This functionality is optional

Remember Me?

- Remember users' login state even after opening/closing browser using a checkbox
- Create a branch (git checkout -b advanced-login)

- The Rails **session** remembers only during the browser session
- Need to create a persistent session via **cookies** method
    - Vulnerable to session hijacking (stealing information)
        - Via packet sniffing cookies via unsecure connections => Resolve with HTTPS (Section 7.5)
        - Compromising a database => Store hash digest of the token
        - XSS => Rails MAGIC via escapes
        - Physical machine access => Token refresh on login/logout
- Code Changes
    - Add remember_digest to User model (rails generate migration add_remember_digest_to_users remember_digest:string) - then rails db:migrate
    - Using **urlsafe_base64** from **SecureRandom** for token generation
    - We'll need to add methods and attributes
        - **Method: New_token**
        - **Attribute: remember_token**
        - **Method: remember_token**
    - The use of **self.** Ensures that assignment sets the attribute

- With **user.remember** we can store the encrypted session information as a permanent cookie
    - Use **cookies** method to store a **value** and an **expires** date
        - Time: cookies[:remember_token] = { value: remember_token,
          expires: 20.years.from_now.utc }
        - Permanent: cookies.permanent[:remember_token] = remember_token
        - Store similar to that of **session** expect we can add a method of **.signed** to encrypt
        - **Cookies.signed** will decrypt to receive as well
    - Tricks of checking
        - The Bcrypt will redefined to see if the digest is equal to the token via **is_password?**
    - The attr_accessor :remember_token is LOCAL and is not the sdame as the authenticated?(remember_token)

- Logic fork for remembered
    - If remembered - Use cookies.signed
    - Otherwise, use find_by(id: user_id)
- Crazy Code***
    - if (user_id = session[:user_id])
    - This is NOT a CHECK but an assignment
    - “If session of user id exists (while setting user id to session of user id)…”

- Forgetting Users

    - Need to a some methods: **user.forget**; opposite of **user.remember**

- **Bugs!**
    - Multiple user sessions; multiple logouts
    - Need to adjust current_user method to handle this
        - Add checks to see if the user is logged in prior to calling logout
        - Need to clear out the remember digest and have authenticated? Return false

Update The GUI!

- Need to add a checkbox and a label to help set up the magic
- Add the necessary HTML and CSS
- The dig deeper we'll need to update the params hash for forms with the new values and handle those within the Session Helper method, **create**

Remember Tests

- Tricky to test remember functions, but planning helps
  In this context, **params[:session][:remember_me]** is either **'0'** or **'1'**, both of which are **true** in a boolean context, so the resulting expression is *always true*, and the application acts as if the checkbox is always checked. This is exactly the kind of error a test can catch.

  From <https://www.railstutorial.org/book/advanced_login>

- We'll need to tie up our test_helper.rb and add a log_in_as method to check specific users
- And add an ActionDispatch off to integration to login as a specific user

- Cookies method does not work with symbols as keys 0 need to work with strings
    - Cookies['rember_token']

- Testing the branch
    - The relevant branch in the current_user method is not being tested right now.
    - Easy fix: Raise an exception in the untested block of code
        - Allows for a pass if not covered, otherwise, trips an error
    - It's hard to test persistent sessions
    - Test out current_user method; directly call out the method on testing

Deploying

- Top: Switch heroku to maintenance mode via
    - Heroku maintenance: on/off
    - This will help with changes during maintenance, disabling the site