

Chapter 9

Advanced login

The basic login system developed in [Chapter 8](#) is fully functional, but most modern websites include the ability to “remember” users when they visit the site again even if they’ve closed their browsers in the interim. In this chapter, we use *permanent cookies* to implement this behavior. We’ll start by automatically remembering users when they log in ([Section 9.1](#)), a common model used by sites such as Bitbucket and GitHub. We’ll then add the ability to *optionally* remember users using a “remember me” checkbox, a model used by sites such as Twitter and Facebook.

Because the [Chapter 8](#) login system is complete by itself, the core of the sample application will work fine without it, and if desired you can skip right to [Chapter 10](#) (and from there to [Chapter 13](#)). On the other hand, learning how to implement the “remember me” feature is both highly instructive by itself and lays an essential foundation for account activation ([Chapter 11](#)) and password reset ([Chapter 12](#)). Moreover, the result is an outstanding example of **computer magic**: You’ve seen a billion of these “remember me” login forms on the Web, and now’s your chance to learn how to make one.

9.1 Remember me

In this section, we’ll add the ability to remember our users’ login state even after they close and reopen their browsers. This “remember me” behavior will

happen automatically, and users will automatically stay logged in until they explicitly log out. As we'll see, the resulting machinery will make it easy to add an optional “remember me” checkbox as well (Section 9.2).

As usual, I suggest switching to a topic branch before proceeding:

```
$ git checkout -b advanced-login
```

9.1.1 Remember token and digest

In Section 8.2, we used the Rails `session` method to store the user's id, but this information disappears when the user closes their browser. In this section, we'll take the first step toward persistent sessions by generating a *remember token* appropriate for creating permanent cookies using the `cookies` method, together with a secure *remember digest* for authenticating those tokens.

As noted in Section 8.2.1, information stored using `session` is automatically secure, but this is not the case with information stored using `cookies`. In particular, persistent cookies are vulnerable to [session hijacking](#), in which an attacker uses a stolen remember token to log in as a particular user. There are four main ways to steal cookies: (1) using a [packet sniffer](#) to detect cookies being passed over insecure networks,¹ (2) compromising a database containing remember tokens, (3) using [cross-site scripting \(XSS\)](#), and (4) gaining physical access to a machine with a logged-in user.

We prevented the first problem in Section 7.5 by using [Secure Sockets Layer \(SSL\)](#) site-wide, which protects network data from packet sniffers. We'll prevent the second problem by storing a hash digest of the remember tokens instead of the token itself, in much the same way that we stored password digests instead of raw passwords in Section 6.3.² Rails automatically prevents the third problem by escaping any content inserted into view templates. Finally, although there's no iron-clad way to stop attackers who have physical access to a logged-in computer, we'll minimize the fourth problem by changing tokens every time

¹Session hijacking was widely publicized by the [Firesheep](#) application, which showed that remember tokens at many high-profile sites were visible when connected to public Wi-Fi networks.

²Rails 5 introduced a `has_secure_token` method that automatically generates random tokens, but it stores the *unhashed* values in the database, and hence is unsuitable for our present purposes.

a user logs out and by taking care to *cryptographically sign* any potentially sensitive information we place on the browser.

With these design and security considerations in mind, our plan for creating persistent sessions appears as follows:

1. Create a random string of digits for use as a remember token.
2. Place the token in the browser cookies with an expiration date far in the future.
3. Save the hash digest of the token to the database.
4. Place an encrypted version of the user's id in the browser cookies.
5. When presented with a cookie containing a persistent user id, find the user in the database using the given id, and verify that the remember token cookie matches the associated hash digest from the database.

Note how similar the final step is to logging a user in, where we retrieve the user by email address and then verify (using the **authenticate** method) that the submitted password matches the password digest (Listing 8.7). As a result, our implementation will parallel aspects of **has_secure_password**.

We'll start by adding the required **remember_digest** attribute to the User model, as shown in Figure 9.1.

To add the data model from Figure 9.1 to our application, we'll generate a migration:

```
$ rails generate migration add_remember_digest_to_users remember_digest:string
```

(Compare to the password digest migration in Section 6.3.1.) As in previous migrations, we've used a migration name that ends in **_to_users** to tell Rails that the migration is designed to alter the **users** table in the database. Because we also included the attribute (**remember_digest**) and type (**string**), Rails generates a default migration for us, as shown in Listing 9.1.

users	
id	integer
name	string
email	string
created_at	datetime
updated_at	datetime
password_digest	string
remember_digest	string

Figure 9.1: The User model with an added **remember_digest** attribute.

Listing 9.1: The generated migration for the remember digest.

```
db/migrate/[timestamp]_add_remember_digest_to_users.rb
```

```
class AddRememberDigestToUsers < ActiveRecord::Migration[6.0]
  def change
    add_column :users, :remember_digest, :string
  end
end
```

Because we don't expect to retrieve users by remember digest, there's no need to put an index on the **remember_digest** column, and we can use the default migration as generated above:

```
$ rails db:migrate
```

Now we have to decide what to use as a remember token. There are many mostly equivalent possibilities—essentially, any long random string will do. The **urlsafe_base64** method from the **SecureRandom** module in the Ruby standard library fits the bill:³ it returns a random string of length 22 composed

³This choice is based on the [RailsCast on remember me](#).

of the characters A–Z, a–z, 0–9, “-”, and “_” (for a total of 64 possibilities, thus “base64”). A typical base64 string appears as follows:

```
$ rails console
>> SecureRandom.urlsafe_base64
=> "brl_446-8bqHv87AQzUj_Q"
```

Just as it’s perfectly fine if two users have the same password,⁴ there’s no need for remember tokens to be unique, but it’s more secure if they are.⁵ In the case of the base64 string above, each of the 22 characters has 64 possibilities, so the probability of two remember tokens colliding is a negligibly small $1/64^{22} = 2^{-132} \approx 10^{-40}$.⁶ As a bonus, by using base64 strings specifically designed to be safe in URLs (as indicated by the name `urlsafe_base64`), we’ll be able to use the same token generator to make account activation and password reset links in [Chapter 12](#).

Remembering users involves creating a remember token and saving the digest of the token to the database. We’ve already defined a `digest` method for use in the test fixtures ([Listing 8.22](#)), and we can use the results of the discussion above to create a `new_token` method to create a new token. As with `digest`, the new token method doesn’t need a user object, so we’ll make it a class method.⁷ The result is the User model shown in [Listing 9.2](#).

Listing 9.2: Adding a method for generating tokens.

app/models/user.rb

```
class User < ApplicationRecord
  before_save { self.email = email.downcase }
  validates :name, presence: true, length: { maximum: 50 }
```

⁴In any case, with bcrypt’s [salted hashes](#) there’s no way for us to tell if two users’ passwords match.

⁵With unique remember tokens, an attacker always needs *both* the user id and the remember token cookies to hijack the session.

⁶This hasn’t stopped some developers from adding a check to verify that no collision has occurred, but such efforts result from failing to grasp just how small 10^{-40} is. For example, if we generated a billion tokens a second for the entire age of the Universe (4.4×10^7 s), the expected number of collisions would still be on the order of 2×10^{-23} , which is zero in any operational sense of the word.

⁷As a general rule, if a method doesn’t need an instance of an object, it should be a class method. Indeed, this decision will prove to be wise in [Section 11.2](#).

```

VALID_EMAIL_REGEX = /\A[\w+\-\.]+\@[a-z\d\-\.\.][a-z]+\z/i
validates :email, presence: true, length: { maximum: 255 },
              format: { with: VALID_EMAIL_REGEX },
              uniqueness: true

has_secure_password
validates :password, presence: true, length: { minimum: 6 }

# Returns the hash digest of the given string.
def User.digest(string)
  cost = ActiveSupport::SecurePassword.min_cost ? BCrypt::Engine::MIN_COST :
          BCrypt::Engine.cost

  BCrypt::Password.create(string, cost: cost)
end

# Returns a random token.
def User.new_token
  SecureRandom.urlsafe_base64
end
end

```

Our plan for the implementation is to make a `user.remember` method that associates a remember token with the user and saves the corresponding remember digest to the database. Because of the migration in Listing 9.1, the User model already has a `remember_digest` attribute, but it doesn't yet have a `remember_token` attribute. We need a way to make a token available via `user.remember_token` (for storage in the cookies) *without* storing it in the database. We solved a similar issue with secure passwords in Section 6.3, which paired a virtual `password` attribute with a secure `password_digest` attribute in the database. In that case, the virtual `password` attribute was created automatically by `has_secure_password`, but we'll have to write the code for a `remember_token` ourselves. The way to do this is to use `attr_accessor` to create an accessible attribute, which we saw before in Section 4.4.5:

```

class User < ApplicationRecord
  attr_accessor :remember_token
  .
  .
  .
  def remember
    self.remember_token = ...
    update_attribute(:remember_digest, ...)
  end
end

```

Note the form of the assignment in the first line of the `remember` method. Because of the way Ruby handles assignments inside objects, without `self` the assignment would create a *local* variable called `remember_token`, which isn't what we want. Using `self` ensures that assignment sets the user's `remember_token` attribute. (Now you know why the `before_save` callback from Listing 6.32 uses `self.email` instead of just `email`.) Meanwhile, the second line of `remember` uses the `update_attribute` method to update the remember digest. (As noted in Section 6.1.5, this method bypasses the validations, which is necessary in this case because we don't have access to the user's password or confirmation.)

With these considerations in mind, we can create a valid token and associated digest by first making a new remember token using `User.new_token`, and then updating the remember digest with the result of applying `User.-digest`. This procedure gives the `remember` method shown in Listing 9.3.

Listing 9.3: Adding a `remember` method to the User model. GREEN

`app/models/user.rb`

```
class User < ApplicationRecord
  attr_accessor :remember_token
  before_save { self.email = email.downcase }
  validates :name, presence: true, length: { maximum: 50 }
  VALID_EMAIL_REGEX = /\A[\w+\-\.]+\@[a-z\d\-\.\.][a-z]+\z/i
  validates :email, presence: true, length: { maximum: 255 },
    format: { with: VALID_EMAIL_REGEX },
    uniqueness: true
  has_secure_password
  validates :password, presence: true, length: { minimum: 6 }

  # Returns the hash digest of the given string.
  def User.digest(string)
    cost = ActiveSupport::SecurePassword.min_cost ? BCrypt::Engine::MIN_COST :
      BCrypt::Engine.cost
    BCrypt::Password.create(string, cost: cost)
  end

  # Returns a random token.
  def User.new_token
    SecureRandom.urlsafe_base64
  end

  # Remembers a user in the database for use in persistent sessions.
  def remember
```

```
self.remember_token = User.new_token
update_attribute(:remember_digest, User.digest(remember_token))
end
end
```

Exercises

Solutions to the exercises are available to all Rails Tutorial purchasers [here](#).

To see other people's answers and to record your own, subscribe to the [Rails Tutorial course](#) or to the [Learn Enough All Access Bundle](#).

1. In the console, assign `user` to the first user in the database, and verify by calling it directly that the `remember` method works. How do `remember_token` and `remember_digest` compare?
2. In [Listing 9.3](#), we defined the new token and digest class methods by explicitly prefixing them with `User`. This works fine and, because they are actually *called* using `User.new_token` and `User.digest`, it is probably the clearest way to define them. But there are two perhaps more idiomatically correct ways to define class methods, one slightly confusing and one extremely confusing. By running the test suite, verify that the implementations in [Listing 9.4](#) (slightly confusing) and [Listing 9.5](#) (extremely confusing) are correct. (Note that, in the context of [Listing 9.4](#) and [Listing 9.5](#), `self` is the `User` class, whereas the other uses of `self` in the User model refer to a user object *instance*. This is part of what makes them confusing.)

Listing 9.4: Defining the new token and digest methods using `self`. GREEN

`app/models/user.rb`

```
class User < ApplicationRecord
  .
  .
  .
  # Returns the hash digest of the given string.
  def self.digest(string)
    cost = ActiveSupport::SecurePassword.min_cost ? BCrypt::Engine::MIN_COST :
```



```

    BCrypt::Password.create(string, cost: cost)
  end

  # Returns a random token.
  def self.new_token
    SecureRandom.urlsafe_base64
  end
  .
  .
  .
end

```

Listing 9.5: Defining the new token and digest methods using `class << self`. GREEN
app/models/user.rb

```

class User < ApplicationRecord
  .
  .
  .
  class << self
    # Returns the hash digest of the given string.
    def digest(string)
      cost = ActiveSupport::SecurePassword.min_cost ? BCrypt::Engine::MIN_COST :
        BCrypt::Engine.cost

      BCrypt::Password.create(string, cost: cost)
    end

    # Returns a random token.
    def new_token
      SecureRandom.urlsafe_base64
    end
  end
end
  .
  .
  .

```

9.1.2 Login with remembering

Having created a working `user.remember` method, we can now create a persistent session by storing a user's (encrypted) id and remember token as permanent cookies on the browser. The way to do this is with the `cookies` method,

which (as with **session**) we can treat as a hash. A cookie consists of two pieces of information, a **value** and an optional **expires** date. For example, we could make a persistent session by creating a cookie with value equal to the remember token that expires 20 years from now:

```
cookies[:remember_token] = { value: remember_token,  
                             expires: 20.years.from_now.utc }
```

(This uses one of the convenient Rails time helpers, as discussed in [Box 9.1](#).) This pattern of setting a cookie that expires 20 years in the future is so common that Rails has a special **permanent** method to implement it, so that we can simply write

```
cookies.permanent[:remember_token] = remember_token
```

This causes Rails to set the expiration to **20.years.from_now** automatically.

Box 9.1. Cookies expire **20.years.from_now**

You may recall from [Section 4.4.2](#) that Ruby lets you add methods to *any* class, even built-in ones. In that section, we added a `palindrome?` method to the `String` class (and discovered as a result that "deified" is a palindrome), and we also saw how Rails adds a `blank?` method to class `Object` (so that `"".blank?`, `" ".blank?`, and `nil.blank?` are all `true`). The `cookies.permanent` method, which creates "permanent" cookies with an expiration `20.years.from_now`, gives yet another example of this practice through one of Rails' *time helpers*, which are methods added to `Fixnum` (the base class for integers):

```
$ rails console  
>> 1.year.from_now  
=> Wed, 21 Jun 2017 19:36:29 UTC +00:00  
>> 10.weeks.ago  
=> Tue, 12 Apr 2016 19:36:44 UTC +00:00
```

Rails adds other helpers, too:

```
>> 1.kilobyte
=> 1024
>> 5.megabytes
=> 5242880
```

These are useful for upload validations, making it easy to restrict, say, image uploads to `5.megabytes`.

Although it should be used with caution, the flexibility to add methods to built-in classes allows for extraordinarily natural additions to plain Ruby. Indeed, much of the elegance of Rails ultimately derives from the malleability of the underlying Ruby language.

To store the user's id in the cookies, we could follow the pattern used with the **session** method (Listing 8.14) using something like

```
cookies[:user_id] = user.id
```

Because it places the id as plain text, this method exposes the form of the application's cookies and makes it easier for an attacker to compromise user accounts. To avoid this problem, we'll use a *signed* cookie, which securely encrypts the cookie before placing it on the browser:⁸

```
cookies.signed[:user_id] = user.id
```

Because we want the user id to be paired with the permanent remember token, we should make it permanent as well, which we can do by chaining the **signed** and **permanent** methods:

⁸Signing and encrypting are different operations in general, but as of Rails 4 the **signed** method **does both** by default.

```
cookies.permanent.signed[:user_id] = user.id
```

After the cookies are set, on subsequent page views we can retrieve the user with code like

```
User.find_by(id: cookies.signed[:user_id])
```

where `cookies.signed[:user_id]` automatically decrypts the user id cookie. We can then use `bcrypt` to verify that `cookies[:remember_token]` matches the `remember_digest` generated in [Listing 9.3](#). (In case you're wondering why we don't just use the signed user id, without the remember token, this would allow an attacker with possession of the encrypted id to log in as the user in perpetuity. In the present design, an attacker with both cookies can log in as the user only until the user logs out.)

The final piece of the puzzle is to verify that a given remember token matches the user's remember digest, and in this context there are a couple of equivalent ways to use `bcrypt` to verify a match. If you look at the [secure password source code](#), you'll find a comparison like this:⁹

```
BCrypt::Password.new(password_digest) == unencrypted_password
```

In our case, the analogous code would look like this:

```
BCrypt::Password.new(remember_digest) == remember_token
```

If you think about it, this code is really strange: it appears to be comparing a `bcrypt` password digest directly with a token, which would imply *decrypting* the digest in order to compare using `==`. But the whole point of using `bcrypt` is for hashing to be irreversible, so this can't be right. Indeed, digging into

⁹As noted in [Section 6.3.1](#), "unencrypted password" is a misnomer, as the secure password is *hashed*, not encrypted.

the [source code of the bcrypt gem](#) verifies that the comparison operator `==` is being *redefined*, and under the hood the comparison above is equivalent to the following:

```
BCrypt::Password.new(remember_digest).is_password?(remember_token)
```

Instead of `==`, this uses the boolean method `is_password?` to perform the comparison. Because its meaning is a little clearer, we'll prefer this second comparison form in the application code.

The above discussion suggests putting the digest–token comparison into an `authenticated?` method in the User model, which plays a role similar to that of the `authenticate` method provided by `has_secure_password` for authenticating a user (Listing 8.15). The implementation appears in Listing 9.6. (Although the `authenticated?` method in Listing 9.6 is tied specifically to the remember digest, it will turn out to be useful in other contexts as well, and we'll generalize it in Chapter 11.)

Listing 9.6: Adding an `authenticated?` method to the User model.

app/models/user.rb

```
class User < ApplicationRecord
  attr_accessor :remember_token
  before_save { self.email = email.downcase }
  validates :name, presence: true, length: { maximum: 50 }
  VALID_EMAIL_REGEX = /\A[\w+\-\.]+\@[a-z\d\-\.\.][a-z]+\z/i
  validates :email, presence: true, length: { maximum: 255 },
    format: { with: VALID_EMAIL_REGEX },
    uniqueness: true
  has_secure_password
  validates :password, presence: true, length: { minimum: 6 }

  # Returns the hash digest of the given string.
  def User.digest(string)
    cost = ActiveModel::SecurePassword.min_cost ? BCrypt::Engine::MIN_COST :
      BCrypt::Engine.cost
    BCrypt::Password.create(string, cost: cost)
  end

  # Returns a random token.
  def User.new_token
    SecureRandom.urlsafe_base64
  end
end
```

```

end

# Remembers a user in the database for use in persistent sessions.
def remember
  self.remember_token = User.new_token
  update_attribute(:remember_digest, User.digest(remember_token))
end

# Returns true if the given token matches the digest.
def authenticated?(remember_token)
  BCrypt::Password.new(remember_digest).is_password?(remember_token)
end
end

```

Note that the `remember_token` argument in the `authenticated?` method defined in Listing 9.6 is not the same as the accessor that we defined in Listing 9.3 using `attr_accessor :remember_token`; instead, it is a variable local to the method. (Because the argument refers to the remember token, it is not uncommon to use a method argument that has the same name.) Also note the use of the `remember_digest` attribute, which is the same as `self.remember_digest` and, like `name` and `email` in Chapter 6, is created automatically by Active Record based on the name of the corresponding database column (Listing 9.1).

We're now in a position to remember a logged-in user, which we'll do by adding a `remember` helper to go along with `log_in`, as shown in Listing 9.7.

Listing 9.7: Logging in and remembering a user. RED

app/controllers/sessions_controller.rb

```

class SessionsController < ApplicationController

  def new
  end

  def create
    user = User.find_by(email: params[:session][:email].downcase)
    if user && user.authenticate(params[:session][:password])
      log_in user
      remember user
      redirect_to user
    else
      flash.now[:danger] = 'Invalid email/password combination'
      render 'new'
    end
  end
end

```

```
    end
  end

  def destroy
    log_out
    redirect_to root_url
  end
end
```

As with `log_in`, Listing 9.7 defers the real work to the Sessions helper, where we define a `remember` method that calls `user.remember`, thereby generating a remember token and saving its digest to the database. It then uses `cookies` to create permanent cookies for the user id and remember token as described above. The result appears in Listing 9.8.

Listing 9.8: Remembering the user. GREEN*app/helpers/sessions_helper.rb*

```
module SessionsHelper

  # Logs in the given user.
  def log_in(user)
    session[:user_id] = user.id
  end

  # Remembers a user in a persistent session.
  def remember(user)
    user.remember
    cookies.permanent.signed[:user_id] = user.id
    cookies.permanent[:remember_token] = user.remember_token
  end

  # Returns the current logged-in user (if any).
  def current_user
    if session[:user_id]
      @current_user ||= User.find_by(id: session[:user_id])
    end
  end

  # Returns true if the user is logged in, false otherwise.
  def logged_in?
    !current_user.nil?
  end

  # Logs out the current user.
  def log_out
```

```

    session.delete(:user_id)
    @current_user = nil
  end
end

```

With the code in [Listing 9.8](#), a user logging in will be remembered in the sense that their browser will get a valid remember token, but it doesn't yet do us any good because the `current_user` method defined in [Listing 8.16](#) knows only about the temporary session:

```
@current_user ||= User.find_by(id: session[:user_id])
```

In the case of persistent sessions, we want to retrieve the user from the temporary session if `session[:user_id]` exists, but otherwise we should look for `cookies[:user_id]` to retrieve (and log in) the user corresponding to the persistent session. We can accomplish this as follows:

```

if session[:user_id]
  @current_user ||= User.find_by(id: session[:user_id])
elsif cookies.signed[:user_id]
  user = User.find_by(id: cookies.signed[:user_id])
  if user && user.authenticated?(cookies[:remember_token])
    log_in user
    @current_user = user
  end
end
end

```

(This follows the same `user && user.authenticated` pattern we saw in [Listing 8.7](#).) The code above will work, but note the repeated use of both `session` and `cookies`. We can eliminate this duplication as follows:

```

if (user_id = session[:user_id])
  @current_user ||= User.find_by(id: user_id)
elsif (user_id = cookies.signed[:user_id])
  user = User.find_by(id: user_id)
  if user && user.authenticated?(cookies[:remember_token])
    log_in user
    @current_user = user
  end
end
end

```


This uses the common but potentially confusing construction

```
if (user_id = session[:user_id])
```

Despite appearances, this is *not* a comparison (which would use double-equals `==`), but rather is an *assignment*. If you were to read it in words, you wouldn't say "If user id equals session of user id...", but rather something like "If session of user id exists (while setting user id to session of user id)...".¹⁰

Defining the `current_user` helper as discussed above leads to the implementation shown in Listing 9.9.

Listing 9.9: Updating `current_user` for persistent sessions. RED

`app/helpers/sessions_helper.rb`

```
module SessionsHelper

  # Logs in the given user.
  def log_in(user)
    session[:user_id] = user.id
  end

  # Remembers a user in a persistent session.
  def remember(user)
    user.remember
    cookies.permanent.signed[:user_id] = user.id
    cookies.permanent[:remember_token] = user.remember_token
  end

  # Returns the user corresponding to the remember token cookie.
  def current_user
    if (user_id = session[:user_id])
      @current_user ||= User.find_by(id: user_id)
    elsif (user_id = cookies.signed[:user_id])
      user = User.find_by(id: user_id)
      if user && user.authenticated?(cookies[:remember_token])
        log_in user
        @current_user = user
      end
    end
  end
end
```

¹⁰I generally use the convention of putting such assignments in parentheses, which is a visual reminder that it's not a comparison.

```
# Returns true if the user is logged in, false otherwise.
def logged_in?
  !current_user.nil?
end

# Logs out the current user.
def log_out
  session.delete(:user_id)
  @current_user = nil
end
end
```

With the code as in [Listing 9.9](#), newly logged in users are correctly remembered, as you can verify by logging in, closing the browser, and checking that you’re still logged in when you restart the sample application and revisit the sample application.¹¹ If you want, you can even inspect the browser cookies to see the result directly ([Figure 9.2](#)).¹²

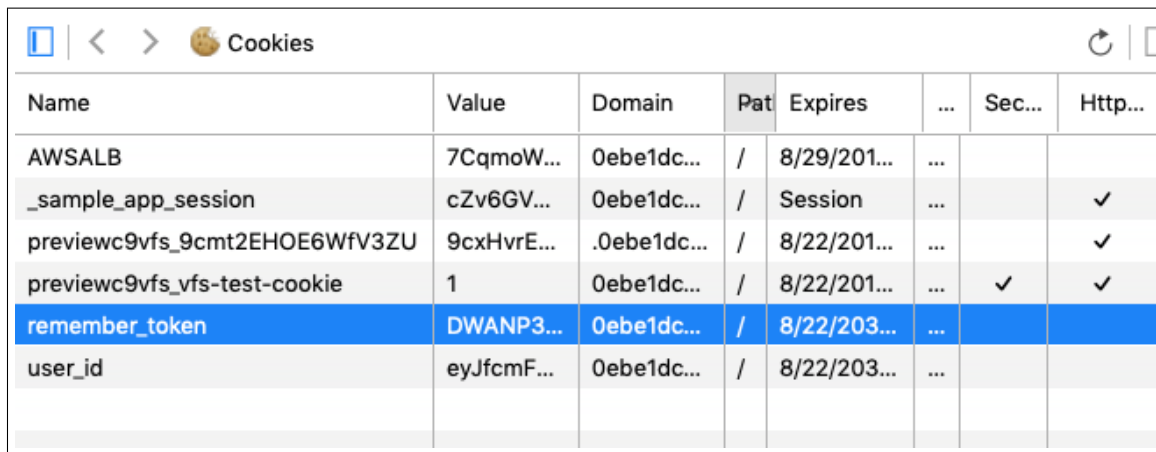
There’s only one problem with our application as it stands: short of clearing their browser cookies (or waiting 20 years), there’s no way for users to log out. This is exactly the sort of thing our test suite should catch, and indeed the tests should currently be **RED**:

¹¹Alert reader Jack Fahnestock has noted that there is an [edge case](#) that isn’t covered by the current design:

1. Log in with “remember me” checked in browser A (saving hashed remember token A to **remember_digest**).
2. Log in with “remember me” checked in browser B (saving hashed **remember_token B** to **remember_digest**, overwriting remember token A saved in browser A).
3. Close browser A (now relying on permanent cookies for login—second conditional in **current_user** method).
4. Reopen browser A (**logged_in?** returns false, even though permanent cookies are on the browser).

Although this is arguably a more secure design than remembering the user in multiple places, it violates the expectation that users can be permanently remembered on more than one browser. The solution, which is substantially more complicated than the present design, is to factor the remember digest into a separate table, where each row has a user id and a digest. Checking for the current user would then look through the table for a digest corresponding to a particular remember token. Furthermore, the **forget** in [Listing 9.11](#) method would delete only the row corresponding to the digest of the current browser. For security purposes, logging out would remove all digests for that user.

¹²Google “<your browser name> inspect cookies” to learn how to inspect the cookies on your system.



Name	Value	Domain	Pat	Expires	...	Sec...	Http...
AWSALB	7CqmoW...	0ebe1dc...	/	8/29/201...	...		
_sample_app_session	cZv6GV...	0ebe1dc...	/	Session	...		✓
previewc9vfs_9cmt2EHOE6WfV3ZU	9cxHvrE...	.0ebe1dc...	/	8/22/201...	...		✓
previewc9vfs_vfs-test-cookie	1	0ebe1dc...	/	8/22/201...	...	✓	✓
remember_token	DWANP3...	0ebe1dc...	/	8/22/203...	...		
user_id	eyJfcmF...	0ebe1dc...	/	8/22/203...	...		

Figure 9.2: The remember token cookie in the local browser.

Listing 9.10: RED

```
$ rails test
```

Exercises

Solutions to the exercises are available to all Rails Tutorial purchasers [here](#).

To see other people's answers and to record your own, subscribe to the [Rails Tutorial course](#) or to the [Learn Enough All Access Bundle](#).

1. By finding the cookie in your local browser, verify that a remember token and encrypted user id are present after logging in.
2. At the console, verify directly that the `authenticated?` method defined in [Listing 9.6](#) works correctly.

9.1.3 Forgetting users

To allow users to log out, we'll define methods to forget users in analogy with the ones to remember them. The resulting `user.forget` method just undoes

`user.remember` by updating the remember digest with `nil`, as shown in Listing 9.11.

Listing 9.11: Adding a `forget` method to the User model. RED

app/models/user.rb

```
class User < ApplicationRecord
  attr_accessor :remember_token
  before_save { self.email = email.downcase }
  validates :name, presence: true, length: { maximum: 50 }
  VALID_EMAIL_REGEX = /\A[\w+\-\.]+\@[a-z\d\-\.\.][a-z]+\z/i
  validates :email, presence: true, length: { maximum: 255 },
                  format: { with: VALID_EMAIL_REGEX },
                  uniqueness: true

  has_secure_password
  validates :password, presence: true, length: { minimum: 6 }

  # Returns the hash digest of the given string.
  def User.digest(string)
    cost = ActiveSupport::SecurePassword.min_cost ? BCrypt::Engine::MIN_COST :
                                                    BCrypt::Engine.cost

    BCrypt::Password.create(string, cost: cost)
  end

  # Returns a random token.
  def User.new_token
    SecureRandom.urlsafe_base64
  end

  # Remembers a user in the database for use in persistent sessions.
  def remember
    self.remember_token = User.new_token
    update_attribute(:remember_digest, User.digest(remember_token))
  end

  # Returns true if the given token matches the digest.
  def authenticated?(remember_token)
    BCrypt::Password.new(remember_digest).is_password?(remember_token)
  end

  # Forgets a user.
  def forget
    update_attribute(:remember_digest, nil)
  end
end
```

With the code in Listing 9.11, we're now ready to forget a permanent session by adding a `forget` helper and calling it from the `log_out` helper (List-

ing 9.12). As seen in Listing 9.12, the `forget` helper calls `user.forget` and then deletes the `user_id` and `remember_token` cookies.

Listing 9.12: Logging out from a persistent session. GREEN*app/helpers/sessions_helper.rb*

```
module SessionsHelper

  # Logs in the given user.
  def log_in(user)
    session[:user_id] = user.id
  end
  .
  .
  .
  # Forgets a persistent session.
  def forget(user)
    user.forget
    cookies.delete(:user_id)
    cookies.delete(:remember_token)
  end

  # Logs out the current user.
  def log_out
    forget(current_user)
    session.delete(:user_id)
    @current_user = nil
  end
end
```

At this point, the tests suite should be GREEN:

Listing 9.13: GREEN

```
$ rails test
```

Exercises

Solutions to the exercises are available to all Rails Tutorial purchasers [here](#).

To see other people's answers and to record your own, subscribe to the [Rails Tutorial course](#) or to the [Learn Enough All Access Bundle](#).

1. After logging out, verify that the corresponding cookies have been removed from your browser.

9.1.4 Two subtle bugs

There are two closely related subtleties left to address. The first subtlety is that, even though the “Log out” link appears only when logged-in, a user could potentially have multiple browser windows open to the site. If the user logged out in one window, thereby setting `current_user` to `nil`, clicking the “Log out” link in a second window would result in an error because of `forget(current_user)` in the `log_out` method (Listing 9.12).¹³ We can avoid this by logging out only if the user is logged in.

The second subtlety is that a user could be logged in (and remembered) in multiple browsers, such as Chrome and Firefox, which causes a problem if the user logs out in the first browser but not the second, and then closes and re-opens the second one.¹⁴ For example, suppose that the user logs out in Firefox, thereby setting the remember digest to `nil` (via `user.forget` in Listing 9.11). The application will still work in Firefox; because the `log_out` method in Listing 9.12 deletes the user’s id, both highlighted conditionals are `false`:

```
# Returns the user corresponding to the remember token cookie.
def current_user
  if (user_id = session[:user_id])
    @current_user ||= User.find_by(id: user_id)
  elsif (user_id = cookies.signed[:user_id])
    user = User.find_by(id: user_id)
    if user && user.authenticated?(cookies[:remember_token])
      log_in user
      @current_user = user
    end
  end
end
```

As a result, evaluation falls off the end of the `current_user` method, thereby returning `nil` as required.

¹³Thanks to reader Paulo Célio Júnior for pointing this out.

¹⁴Thanks to reader Niels de Ron for pointing this out.

In contrast, if we close Chrome, we set `session[:user_id]` to `nil` (because all `session` variables expire automatically on browser close), but the `user_id` cookie will still be present. This means that the corresponding user will still be pulled out of the database when Chrome is re-launched:

```
# Returns the user corresponding to the remember token cookie.
def current_user
  if (user_id = session[:user_id])
    @current_user ||= User.find_by(id: user_id)
  elsif (user_id = cookies.signed[:user_id])
    user = User.find_by(id: user_id)
    if user && user.authenticated?(cookies[:remember_token])
      log_in user
      @current_user = user
    end
  end
end
```

Consequently, the inner `if` conditional will be evaluated:

```
user && user.authenticated?(cookies[:remember_token])
```

In particular, because `user` isn't `nil`, the *second* expression will be evaluated, which raises an error. This is because the user's remember digest was deleted as part of logging out (Listing 9.11) in Firefox, so when we access the application in Chrome we end up calling

```
BCrypt::Password.new(remember_digest).is_password?(remember_token)
```

with a `nil` remember digest, thereby raising an exception inside the `bcrypt` library. To fix this, we want `authenticated?` to return `false` instead.

These are exactly the sorts of subtleties that benefit from test-driven development, so we'll write tests to catch the two errors before correcting them. We first get the integration test from Listing 8.35 to `RED`, as shown in Listing 9.14.

Listing 9.14: A test for logging out in a second window. **RED**

test/integration/users_login_test.rb

```
require 'test_helper'

class UsersLoginTest < ActionDispatch::IntegrationTest
  .
  .
  .
  test "login with valid information followed by logout" do
    get login_path
    post login_path, params: { session: { email: @user.email,
                                         password: 'password' } }

    assert is_logged_in?
    assert_redirected_to @user
    follow_redirect!
    assert_template 'users/show'
    assert_select "a[href=?]", login_path, count: 0
    assert_select "a[href=?]", logout_path
    assert_select "a[href=?]", user_path(@user)
    delete logout_path
    assert_not is_logged_in?
    assert_redirected_to root_url
    # Simulate a user clicking logout in a second window.
    delete logout_path
    follow_redirect!
    assert_select "a[href=?]", login_path
    assert_select "a[href=?]", logout_path, count: 0
    assert_select "a[href=?]", user_path(@user), count: 0
  end
end
```

The second call to **delete logout_path** in Listing 9.14 should raise an error due to the missing **current_user**, leading to a **RED** test suite:

Listing 9.15: **RED**

```
$ rails test
```

The application code simply involves calling **log_out** only if **logged_in?** is true, as shown in Listing 9.16.

Listing 9.16: Only logging out if logged in. GREEN
app/controllers/sessions_controller.rb

```
class SessionsController < ApplicationController
  .
  .
  .
  def destroy
    log_out if logged_in?
    redirect_to root_url
  end
end
```

The second case, involving a scenario with two different browsers, is harder to simulate with an integration test, but it's easy to check in the User model test directly. All we need is to start with a user that has no remember digest (which is true for the `@user` variable defined in the `setup` method) and then call `authenticated?`, as shown in Listing 9.17. (Note that we've just left the remember token blank; it doesn't matter what its value is, because the error occurs before it ever gets used.)

Listing 9.17: A test of `authenticated?` with a nonexistent digest. RED
test/models/user_test.rb

```
require 'test_helper'

class UserTest < ActiveSupport::TestCase

  def setup
    @user = User.new(name: "Example User", email: "user@example.com",
                    password: "foobar", password_confirmation: "foobar")
  end
  .
  .
  .
  test "authenticated? should return false for a user with nil digest" do
    assert_not @user.authenticated?('')
  end
end
```

Because `BCrypt::Password.new(nil)` raises an error, the test suite should now be RED:

Listing 9.18: RED

```
$ rails test
```

To fix the error and get to GREEN, all we need to do is return **false** if the remember digest is **nil**, as shown in Listing 9.19.

Listing 9.19: Updating **authenticated?** to handle a nonexistent digest.

GREEN

app/models/user.rb

```
class User < ApplicationRecord
  .
  .
  .
  # Returns true if the given token matches the digest.
  def authenticated?(remember_token)
    return false if remember_digest.nil?
    BCrypt::Password.new(remember_digest).is_password?(remember_token)
  end

  # Forgets a user.
  def forget
    update_attribute(:remember_digest, nil)
  end
end
```

This uses the **return** keyword to return immediately if the remember digest is **nil**, which is a common way to emphasize that the rest of the method gets ignored in that case. The equivalent code

```
if remember_digest.nil?
  false
else
  BCrypt::Password.new(remember_digest).is_password?(remember_token)
end
```

would also work fine, but I prefer the explicitness of the version in Listing 9.19 (which also happens to be slightly shorter).

With the code in Listing 9.19, our full test suite should be GREEN, and both subtleties should now be addressed:

Listing 9.20: GREEN

```
$ rails test
```

Exercises

Solutions to the exercises are available to all Rails Tutorial purchasers [here](#).

To see other people’s answers and to record your own, subscribe to the [Rails Tutorial course](#) or to the [Learn Enough All Access Bundle](#).

1. Comment out the fix in [Listing 9.16](#) and then verify that the first subtle bug is present by opening two logged-in tabs, logging out in one, and then clicking “Log out” link in the other.
2. Comment out the fix in [Listing 9.19](#) and verify that the second subtle bug is present by logging out in one browser and closing and opening the second browser.
3. Uncomment the fixes and confirm that the test suite goes from **RED** to **GREEN**.

9.2 “Remember me” checkbox

With the code in [Section 9.1.3](#), our application has a complete, professional-grade authentication system. As a final step, we’ll see how to make staying logged in optional using a “remember me” checkbox. A mockup of the login form with such a checkbox appears in [Figure 9.3](#).

To write the implementation, we start by adding a checkbox to the login form from [Listing 8.4](#). As with labels, text fields, password fields, and submit buttons, checkboxes can be created with a Rails helper method. In order to get the styling right, though, we have to *nest* the checkbox inside the label, as follows: