In this lecture, we will discuss…

✧ Authentication

What Happened To The Users?

✧ The books/notes stuff is working pretty nicely, but everybody can see and modify everybody else's books and notes?

✧ We need the two security 'A's:

- **A**uthentication
  - Do we know who the user is and are his **credentials valid**?
- **A**uthorization
  - Provide access only to the books/notes a particular logged-in user is **authorized** to modify/see

Authentication Summary

> `has_secure_password` to the rescue!

1. Enable (uncomment) `bcrypt-ruby` (Gemfile)
   - Run $bundle (install)

2. Make sure `password_digest` is table column

3. Account for `password` (not `password_digest`) inside **strong parameters** list in the controller if you plan to use mass assignment when creating users

4. No need for `password` column in the table (virtual attribute)

bcrypt gem

FOLDERS

▼ 📂 i_reviewed
  ▶ 📁 app
  ▶ 📁 bin
  ▶ 📁 config
  ▶ 📁 db
  ▶ 📁 lib
  ▶ 📁 log
  ▶ 📁 public
  ▶ 📁 test
  ▶ 📁 tmp
  ▶ 📁 vendor
    📄 .gitignore
    📄 config.ru
    📄 Gemfile
    📄 Gemfile.lock
    📄 Rakefile

◀ ▶   Gemfile   ✱

```
1   source 'https://rubygems.org'
2
3   gem 'rails', '4.2.3'
4   gem 'sqlite3'
5   gem 'sass-rails', '~> 5.0'
6   gem 'uglifier', '>= 1.3.0'
7   gem 'coffee-rails', '~> 4.1.0'
8   gem 'jquery-rails'
9   gem 'turbolinks'
10  gem 'jbuilder', '~> 2.0'
11  gem 'sdoc', '~> 0.4.0', group: :doc
12
13  # Use ActiveModel has_secure_password
14  gem 'bcrypt', '~> 3.1.7'
15
16  group :development, :test do
17    gem 'byebug'
18    gem 'web-console', '~> 2.0'
19    gem 'spring'
20  end
```

$bundle

Restart the server

has_secure_password

reviewer.rb ✕ ▼   **schema.rb** ✕

```ruby
1  class Reviewer < ActiveRecord::Base
2
3    has_secure_password
4
5    has_many :books
6  end
7
```

```ruby
1  # encoding: UTF-8
2  # This file is auto-generated from the current state of the database. Instead
3  # of editing this file, please use the migrations feature of Active Record to
4  # incrementally modify your database, and then regenerate this schema definition.
5  #
6  # Note that this schema.rb definition is the authoritative source for your
7  # database schema. If you need to create the application database on another
8  # system, you should be using db:schema:load, not running all the migrations
9  # from scratch. The latter is a flawed and unsustainable approach (the more migrations
10 # you'll amass, the slower it'll run and the greater likelihood for issues).
11 #
12 # It's strongly recommended that you check this file into your version control system.
13
14 ActiveRecord::Schema.define(version: 20151015232430) do
15   create_table "books", force: :cascade do |t| ▦
21   end
22
23   add_index "books", ["reviewer_id"], name: "index_books_on_reviewer_id"
24
25   create_table "notes", force: :cascade do |t| ▦
31   end
32
33   add_index "notes", ["book_id"], name: "index_notes_on_book_id"
34
35   create_table "reviewers", force: :cascade do |t|
36     t.string   "name"
37     t.string   "password_digest"
38     t.datetime "created_at",       null: false
39     t.datetime "updated_at",       null: false
40   end
41 end
```

FOLDERS
- ▼ 📂 i_reviewed
  - ▼ 📂 app
    - ▼ 📂 assets
      - ▶ 📁 images
      - ▶ 📁 javascripts
      - ▶ 📁 stylesheets
    - ▶ 📁 controllers
    - ▶ 📁 helpers
    - ▶ 📁 mailers
    - ▼ 📂 models
      - ▶ 📁 concerns
      - 📄 .keep
      - 📄 book.rb
      - 📄 note.rb
      - 📄 reviewer.rb
    - ▶ 📁 views
  - ▶ 📁 bin
  - ▶ 📁 config
  - ▼ 📂 db
    - ▶ 📁 migrate
    - 📄 development.s
    - 📄 schema.rb
    - 📄 seeds.rb
  - ▶ 📁 lib

How It All Works

```
~/sandbox/i_reviewed$ rails c
Loading development environment (Rails 4.2.3)
irb(main):001:0> ActiveRecord::Base.logger = nil
=> nil
irb(main):002:0> Reviewer.column_names
=> ["id", "name", "password_digest", "created_at", "updated_at"]
irb(main):003:0> Reviewer.create! name: "Joe", password: "abc123"
=> #<Reviewer id: 1, name: "Joe", password_digest: "$2a$10$k7JtAb119soo3.ASpIOsqurERRFkzL3vxxlmPMhV423...",
 created_at: "2015-10-19 03:34:54", updated_at: "2015-10-19 03:34:54">
irb(main):004:0> joe = Reviewer.find_by name: "Joe"
=> #<Reviewer id: 1, name: "Joe", password_digest: "$2a$10$k7JtAb119soo3.ASpIOsqurERRFkzL3vxxlmPMhV423...",
 created_at: "2015-10-19 03:34:54", updated_at: "2015-10-19 03:34:54">
irb(main):005:0> joe.authenticate("somepassword")
=> false
irb(main):006:0> joe.authenticate("abc123")
=> #<Reviewer id: 1, name: "Joe", password_digest: "$2a$10$k7JtAb119soo3.ASpIOsqurERRFkzL3vxxlmPMhV423...",
 created_at: "2015-10-19 03:34:54", updated_at: "2015-10-19 03:34:54">
```

Seed Users

```ruby
Reviewer.destroy_all
Book.destroy_all

Book.create! [
  { name: "Eloquent Ruby", author: "Russ Olsen" },
  { name: "Beginning Ruby", author: "Peter Cooper" },
  { name: "Metaprogramming Ruby 2", author: "Paolo Perrotta" },
  { name: "Design Patterns in Ruby", author: "Russ Olsen" },
  { name: "The Ruby Programming Language", author: "David Flanagan" }
]

eloquent = Book.find_by name: "Eloquent Ruby"
eloquent.notes.create! [
  { title: "Wow", note: "Great book to learn Ruby"},
  { title: "Funny", note: "Doesn't put you to sleep"}
]

reviewers = Reviewer.create! [
  { name: "Joe", password: "abc123" },
  { name: "Jim", password: "123abc" }
]

Book.all.each do |book|
  book.reviewer = reviewers.sample
  book.save!
end
```

Seed Users

```
~/sandbox/i_reviewed$ rake db:seed
~/sandbox/i_reviewed$ rails c
Loading development environment (Rails 4.2.3)
irb(main):001:0> Reviewer.first.books.count
  Reviewer Load (0.1ms)  SELECT  "reviewers".* FROM "reviewers"  ORDER BY "reviewers"."id" ASC LIMIT 1
   (0.1ms)  SELECT COUNT(*) FROM "books" WHERE "books"."reviewer_id" = ?  [["reviewer_id", 4]]
=> 2
irb(main):002:0> Reviewer.last.books.count
  Reviewer Load (0.2ms)  SELECT  "reviewers".* FROM "reviewers"  ORDER BY "reviewers"."id" DESC LIMIT 1
   (0.1ms)  SELECT COUNT(*) FROM "books" WHERE "books"."reviewer_id" = ?  [["reviewer_id", 5]]
=> 3
irb(main):003:0> Reviewer.first.books.pluck :name
  Reviewer Load (0.2ms)  SELECT  "reviewers".* FROM "reviewers"  ORDER BY "reviewers"."id" ASC LIMIT 1
   (0.1ms)  SELECT "books"."name" FROM "books" WHERE "books"."reviewer_id" = ?  [["reviewer_id", 4]]
=> ["Eloquent Ruby", "Metaprogramming Ruby 2"]
irb(main):004:0> Reviewer.last.books.pluck :name
  Reviewer Load (0.2ms)  SELECT  "reviewers".* FROM "reviewers"  ORDER BY "reviewers"."id" DESC LIMIT 1
   (0.1ms)  SELECT "books"."name" FROM "books" WHERE "books"."reviewer_id" = ?  [["reviewer_id", 5]]
=> ["Beginning Ruby", "Design Patterns in Ruby", "The Ruby Programming Language"]
irb(main):005:0>
```

Summary

✧ `has_secure_password`, `password_digest` column in a "users" table and `bcrypt` gem is all you need to get going

What's Next?

✧ HTTP Sessions and cookies