Week 7

CSPP 52553: Web Development
Winter 2013

- Code Review
- User Authentication
- User Authorization
- Search Functionality
- Gems
- Model Callbacks
- Deployment, Part 1

Code Review

Prefer #each instead of a for... loop

Copy array elements with #slice or [i,n] syntax

Read Poker controller code in forks of Week3

Secure User Accounts

Require a password (or some sort of user authentication) to guard private data.

Best Option: Do not store the password in your database or anywhere on your server.

2nd Option: Use a very strong one-way function to encrypt passwords. Use bcrypt.

User Authentication

Authentication answers the following question:
"Are you really who you say you are?"

Symptoms of bad authentication strategies:

1. **Too easy to guess ("password")**
2. **Password hints can give out unnecessary clues**
3. **Users can get "locked out" after a certain number of tries**
4. **Changed and forgotten passwords cause user frustration**

User Authentication

Authentication answers the following question:
"Are you really who you say you are?"

In Rails, the best practice is a combination of:

1. **Using the `bcrypt` gem to encrypt passwords**
2. **Using the `has_secure_password` feature**

User Authorization

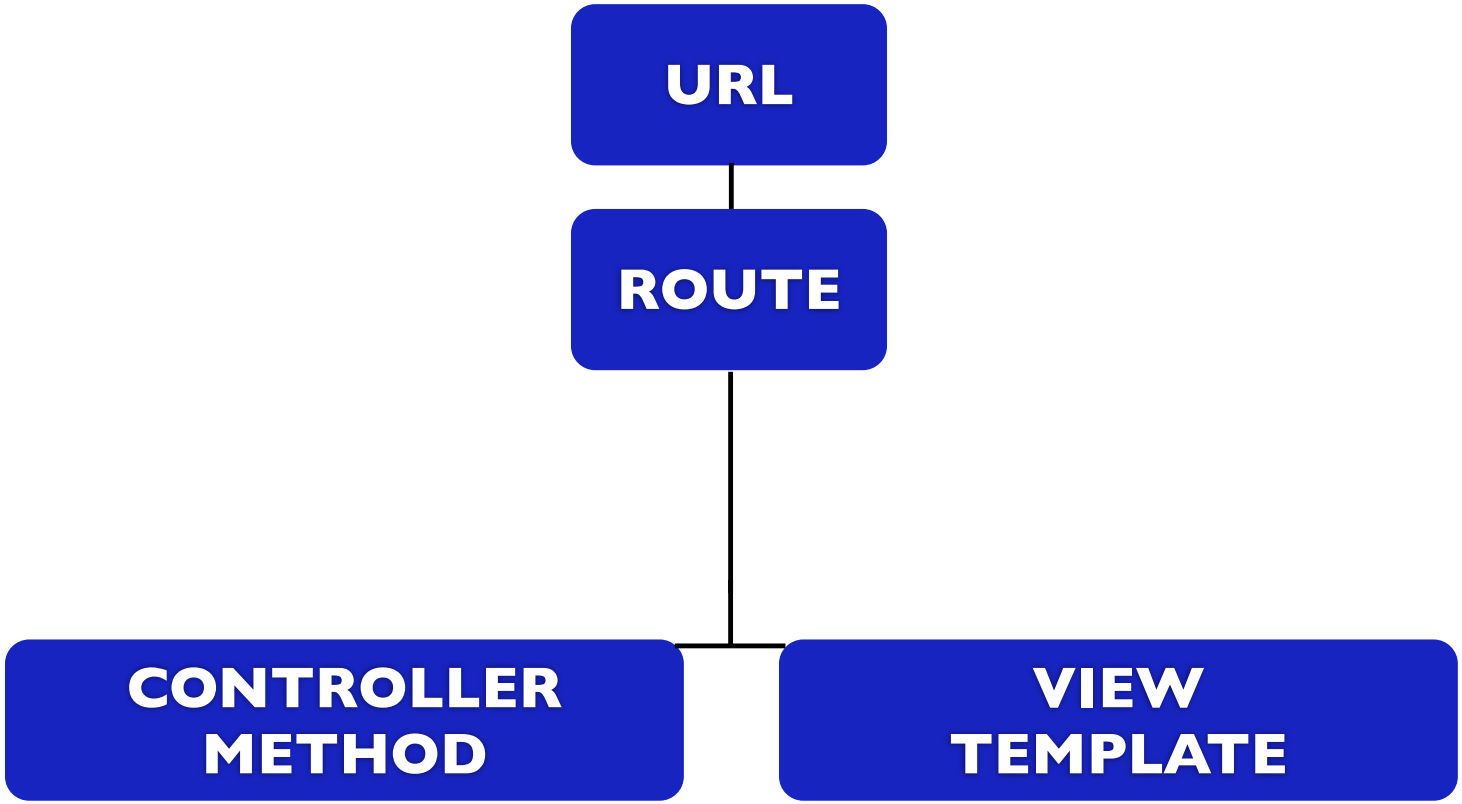
Authorization answers the following question:
"Are you allowed to be here?"

Authorization is about permissions, not identification.

Two primary strategies:

1. **Filter actions from unauthorized use**
2. **Use template logic to control what's visible**

Controller Filters



Controller Filters