CS 410/510: Web Security
A6: Labs and Homework

WFP2: Randomness Issues

- **Example #1**
  - **Developer used 0 to seed PRNG, then generated passwords**
  - **Find the one generated for the admin user**
  - **Primer on Ruby from Python**
    - **http://www.senktec.com/2013/06/ruby-vs-python/**
- **Example #2**
  - **Developer used the number of seconds since the epoch to seed PRNG, then generated passwords**
  - **Find the time used to seed the PRNG via brute-force from the current time.**
  - **Then, calculate admin password**
- **Example #3**
  - **Developer tried to randomize lengths to increase security**
  - **Adapt your scripts from #1 to calculate the admin password**
- **Example #4**
  - **Developer now hits the PRNG a random number of times before generating passwords**
  - **Brute-force until you find the number used to show that a random start does not matter**

Homework

- **Lessons: Insecure Cryptographic Storage**
- **Challenges: Insecure Cryptographic Storage #1-2**