Software Security
Roy McElmurry
General Principles
Assets, Adversaries & Threats

1) What things of value does your app have?
2) Who would gain by attacking your system?
3) How might someone go about attacking you?
Whitelist Over Blacklist

1) Validate all input
2) Do not trust the user
3) Escape all data
Safe Defaults

Make the default options the safe or restricted options. Users will notice if they are restricted, but are less likely to notice if they have unrestricted.
Least Privilege Principle

Give users the least amount of privilege that they need to get their job done.
Some Specific Concerns
User Authentication

- Passwords
- Two-step authentication
  - Second Password
  - Mobile Passcode
  - OTP
- Captcha
XSS

Executing fraudulent script code on another users web experience.

ex) sql injection
XSSI

Including code from one domain in the execution of another.

ex) Scripts can be included in pages without respect to the same domain policy
XSRF

Making requests to another domain on the behalf of the user.

ex) click jacking
Exercises

- Gruyere, a Google codelab about web security
  - File Upload XSS
  - Reflected XSS
  - Stored XSS
  - XSRF
  - XSSI