11/10/15 Defensive programming

- Regression test – set of tests that are incorporated into a test suite.
- A lot of the bugs found are a direct result of a lack of defensive programming
- Defensive programming - It’s a way of writing your code, with future intentions in mind
- Program input, incorrect handling is probably the most common problem
- Injection attacks – many different types.
  - Command injection – command line
  - SQL injection – meta characters are inserted into a sql string.
  - Code injection – code that is inserted
  - Format string injections
- Cross Site Scripting – javascript that executes, to work on other sites. Can get really messy with multiple XSS’s on multiple sites
  - XSS = cross site scripting
- XSS reflection – someone posts a comment with code that goes to execute something somewhere else, in this case you’ll have the webservers privileges.
- Input fuzzing – rather than having a human write a script, lets generate as much random input as possible and feed it into the system and see how it acts.
- Slides
  - Many vulnerabilities result from poor programming practices
  - Software quality & reliability
    - Concerned with the accidental failure
  - Software security
    - Unlikely to be identified by common testing approaches
  - Defensive programming
    - designing and implanting software so that it continues to work while under attack
    - time consuming
    - conflicts with business pressures to keep development times as short as possible
  - XSS
    - Attacks where input provided by one user is subsequently output to another user
    - Common in Web Applications
    - Reflection vulnerability
      - Attackers include malicious script content in data supplied to a site