Defensive Programming

- Way of writing your code
  - Defensive input
    - Terminal
    - Files
    - Places on the stack
    - Other programs
      - Pre/post conditions need to be met
      - Checking everything that may go wrong

- Input (Any source of Data)
  - Need to check the copies
  - Need to validate assumptions
  - Interpretation of Data type
    - Heart Bleed SSL
    - Checking Binary input
      - Hard to verify the type of encoded data

- Injection attacks
  - Different types
    - Command injection
      - Taking users input to create a command to send to the command line
        - Weaknesses is in the input from the user
    - SQL injection
      - Meta characters inserted into the SQL string
    - Code injection
      - Shell code
    - Whenever a program invokes the services from somewhere else (API)
      - Is the communication being treated correctly?
    - Cross Site Scripting
      - Scripts that communicate with other websites
        - XSS (Cross Site)
          - Scripted Web Application
          - Reflection Vulnerability
            - Instead of a comment place code that is executed when viewed

- Input Fuzzing
  - Sending values into a program to expose possible flaws

- Software Security
  - Unlikely to be identified by common testing approaches