JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Finding Security Flaws

Security Architecture & Tool Sets

Finding Security Flaws

- Coding flaws are always going to occur
  - Programming and syntax errors
  - Business logic and process errors
  - Error handling
  - Incorrect integration with other services

Static Analysis

- Conducted by reviewing the code manually or with an automated tool
- Code is not run during static analysis
- Form of white-box testing

Dynamic Analysis

- Code is executed while providing specific input
- Uses automated tools or manual input
- Types
  - Fuzzing
  - Fault Injection
  - Mutation Testing
  - Stress Testing (Load Testing)
  - Security Regression Testing

Fuzzing

- Sends invalid or random data to an application to test ability to handle unexpected data
- Typically automated to use large datasets
- Used to detect input validation, logic issues, memory leaks, and error handling

Fault Injections

- Directly inserts faults into error handling parts of the code to test them

- Examples:
  - Compile-time injection
    - Injects faults by modifying source code before compiling
  - Protocol software injection
    - Uses fuzzing to send noncompliant data to a protocol
  - Runtime injection
    - Inserts data into running memory of the program or by sending in a fault to the program to deal with it

Mutation Testing

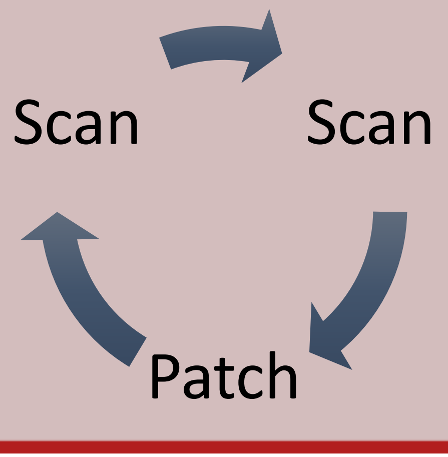
- Makes small changes to the program itself to determine they would cause a failure
- If they cause a failure then they are rejected
- Used to test if code is testing for possible issues with unexpected input types

Stress Testing (Load Testing)

- Ensures applications and systems can support the expected production load
- Uses automated tools to “stress” an expected load and determine if its handled properly
- Test for the worst-case scenario
- Can be conducted against entire system or just a single component

Security Regression Testing

- Ensures that any changes made do not create new problems or issues in the application
- Used most commonly when a new patch or update is added
- Verifies no new vulnerabilities or misconfigurations have been added


Scan
Scan
Patch