Manual Security Code Reviews

Software Manual Code Review

AUBURN

- Properly conducted code reviews can find and fix common security issues before code is integrated or tested
- Code review techniques can be cost effective and fast when automated tools are used and integrated into an overall build pipeline.
- Also provides an opportunity for senior software engineers to mentor and train less experience software engineers

Prior to Inspection During SDLC Process

AUBURN

- Architectural Design
- Application Documentation
- Coding Standards & Policies
- Security Requirements
- “Trust but Verify” mentality

Good Practices

AUBURN

- Manually found security flaws should be incorporated into automate tools.
- A set of common validation routines that your software can call as soon as it receives any untrusted data should be available which will give your software product a central validation area that can be updated as new information is discovered.
- Review related top security vulnerability lists
  - 10-20 CVE
  - OWasp for web applications
  - Coding Language top vulnerabilities
- Security Issues unique to an system architecture
  - Privileged vs non-privileged application functions
  - Security implementations (LDAP, OAuth, SAML, Encryption, API Keys, etc.)
  - Access to external resources (Database, APIs, Storage, Secrets Mgmt Tools)

Common Questions for Manual Inspection

AUBURN

- Control Flow
  - Examine a function and determine each branch condition. These may include loops, switch statements, “if” statements, and “try/catch” blocks.
  - Understand the conditions under which each block will execute.
  - Move to the next function and repeat.

- Data Flow
  - For each input location, determine how much you trust the source of input. When in doubt, you should give it no trust.
  - Trace the flow of data to each possible output. Note any attempts at data validation.
  - Move to the next input and continue.

AUBURN UNIVERSITY