Lecture 28 Outline

June 6, 2018

Reading: §24

Assignments: Lab 4, due on June 6, 2018 at 11:59pm
Homework 5, due on June 7, 2018 at 11:59pm

1. Vulnerability models
   a. PA model
   b. RISOS
   c. NRL
   d. Aslam
2. Some common vulnerabilities
   a. Catalogues: CVE (Common Vulnerabilities and Exposures), CWE (Common Weakness Enumeration)
   b. 2011 MITRE/SANS Top 25 Most Dangerous Software Errors
   c. OWASP Top 10 – 2017 The Ten Most Critical Web Application Security Risks
3. MITRE/SANS list
   a. Insecure interactions among components (injection is first here)
   b. Risky resource management
   c. Porous defenses
4. OWASP list
   a. Injection
   b. Broken authentication and session management
   c. Sensitive data exposure
   d. XML external entities
   e. Broken access cointrol
   f. Security misconfiguration
   g. Cross-site scripting
   h. Insecure deserialization
   i. Using components with known vulnerabilities
   j. Insufficient logging and monitoring
5. Comparison
   a. Everything on the OWASP list is also on the MITRE/SANS list
   b. Injection is #1 on both lists
   c. The MITRE/SANS list covers vulnerabilities generally; OWASP covers only web vulnerabilities