

Lecture 5 Outline (April 8, 2015)

Reading: [Chr11,OWA13]

Assignment: Program 1, due April 15, 2015

1. Discussion problem of the day
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 – 2013 rc1 The Ten Most Critical Web Application Security Risks
3. MITRE/SANS list
 - a. Insecure interactions among components
 - i. SQL injection
 - ii. OS command injection
 - iii. Cross-site scripting
 - iv. Unrestricted upload of file with dangerous type
 - v. Cross-site request forgery
 - vi. URL redirect to untrusted site
 - b. Risky resource management
 - i. Buffer copy without checking size of input
 - ii. Improper limitation of a pathname to a restricted directory
 - iii. Download of code without integrity check
 - iv. Inclusion of functionality from untrusted control sphere
 - v. Use of potentially dangerous function
 - vi. Incorrect calculation of buffer size
 - vii. Uncontrolled format string
 - viii. Integer overflow or wraparound
 - c. Porous defenses
 - i. Missing authentication for critical function
 - ii. Missing authorization
 - iii. Use of hard-coded credentials
 - iv. Missing encryption of sensitive data
 - v. Reliance on untrusted inputs in a security decision
 - vi. Execution with unnecessary privileges
 - vii. Incorrect authorization
 - viii. Incorrect permission assignment for critical resource
 - ix. Use of a broken or risky cryptographic algorithm
 - x. Improper restriction of excessive authentication attempts
 - xi. Use of a one-way hash without a salt
4. OWASP list
 - a. Injection
 - b. Broken authentication and session management
 - c. Cross-site scripting
 - d. Insecure direct object references
 - e. Security misconfiguration
 - f. Sensitive data exposure
 - g. Missing function level access control
 - h. Cross-site request forgery
 - i. Using known vulnerable components
 - j. Unvalidated redirects and forwards
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
-

Discussion Problem. You discover a security flaw in the operating system on your company's computer. The flaw enables any user to read any other user's files, regardless of their protection. You have several choices: you can keep quiet and hope no-one else discovers the flaw, or tell the company, or tell the system vendor, or announce it on the Internet.

1. Suppose an exploitation of the vulnerability could be prevented by proper system configuration. Which of the above courses of action would you take, and why?
2. If an exploitation of the vulnerability could be detected (but not prevented) by system administrators, how would this change your answer to the first question?
3. Now suppose no exploitation of the vulnerability can be detected or prevented. Would this change your answer, and if so, how?