Matthew Vollkommer 11/2/2014 MIST 4630

Fundamental Practices for Secure Software Development Reading Sections:

- Secure Design Principl1es

1) What does STRIDE stand for?

Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and elevation of privilege

2) What is an advantage to Threat Modeling?

a) identifies issues before code is written

b) uncover insecure business logic or workflow

c) a and b correct Answer

d) none of the above

- Secure Coding Practices

1) Which is a safer function in the C/C++ standard library?
   a. strcat_s Correct Answer
   b. gets
   c. memcpy
   d. strncpys

2) A _______ filter should be applied to limit input to allowed values and types. For data where defining it the first way is not possible, the data validation should be performed against a ______ of disallowed values and data types.
   a) Blacklist, whitelist
   b) Whitelist, blacklist
   c) Saltedlist, unsaltedlist
   d) Unsaltedlist, saltedlist

- Testing Recommendations

1) What is the goal of penetration testing?

The goal of penetration testing is to break the system by applying testing techniques usually employed by attackers, either manually or by using attacking tools.

2) _______ testing is a reliability and security testing technique that relies on building intentionally malformed data and then having the software under test consume the malformed data to see how it responds.
   a) Robustness
   b) Fuzz Correct Answer

c) Penetration
d) SQL Injection

- Technology Recommendations

1) Buffer overruns and underruns are a common source of vulnerabilities in C and C++ code. What issue is this an example of?
    a) Memory deletion
    b) Memory corruption correct answer
    c) Memory concatenation
    d) Memory writing
2) Which scenarios may result in false negatives from limited data flow and control flow analysis and other problems that full-codebase and/or main branch analysis would otherwise find?

    I) Developers are using static analysis tools on all of code.

    II) Developers have a modified view of code.

    III) Developers only dealing with a limited set of source code.

A) I and II
B) I and II
C) I
D) II and III correct answer

Data Validation:

- Client Side

1) What are advantages of using client-side validation?
Increased speed. Can filter legitimate input from genuine users.

2) What are disadvantages of using only server-side validation?
May be circumvented by people using a malicious app that interfaces in a way that mirrors your own application.

- Server-Side Validation

1) What are advantages of using server-side validation?
All checks occur on the server which is more secure. And Helps protect against malicious users who may not even be using your interface. You have control of the final step before anything is accessed.

2) What are disadvantages of using only server-side validation?

Additional resources are consumed by the server, making them take longer.