Brian Engel

Module 6 Journal

Define: What is a security vulnerability? A security vulnerability is a weakness or flaw in a system that can be exploited by attackers to allow access or take down an application. This can be done with buffer overflows, injection attacks, authentication bypass, and many other techniques.

Identify: What kinds of vulnerabilities would be identifiable in C++ code? Security vulnerabilities that can occur in C++ most frequently are related to memory management. Buffer overflows, dangling pointers, and memory leaks are common since C++ does not clean up after the coder. In addition to this, string concatenation injection attacks are also a possibility. Another vulnerability to watch out for is integer overflow / underflow.

Purpose: Why would you be looking for vulnerabilities during legacy to C++ conversion rather than during testing? Finding vulnerabilities in conversion allows for early correction of the problem. Why wait till the program is done to correct something you already know is broken? It makes no sense to let a known vulnerability pass through and hope it gets caught later and then fix it.

Solutions: How do you determine the appropriate fix to a security vulnerability? To fix a security vulnerability, you first need to understand the root of the problem. Then you can decide if input validation, encryption, access controls, or other secure coding practices are needed to fix the problem, or if a Defense in Depth stategy is more appropriate and have several overlapping layers of security.

VPNoverview.com. (2024, June 10). What is Secure Coding and Why is It Important? [Webpage]. Retrieved from https://vpnoverview.com/internet-safety/business/what-is-secure-coding/#:~:text=Secure%20code%20will%20help%20to,Software%20vulnerabilities%20are%20rampant.