Paloma Rodriguez

CS410 Software Reverse Engineering

02/11/2024

Journal Six

* Define: What is a security vulnerability?

A security vulnerability is a weakness or a flaw in a system that can be then taken advantage of or “exploited” by an attacker to create issues with the CIA triad, which is the confidentiality, integrity, or availability of the system or its data to its users. These vulnerabilities can be in any part of a system like the software itself or its physical hardware parts. In general, these all can arise concerns when it comes to the data and securing itself.

* Identify: What kinds of vulnerabilities would be identifiable in C++ code?

Some vulnerabilities can be buffer overflows, memory leaks, integer overflows, input validation issues, SQL injections, XSS attacks, and lack of proper error handling.

* Purpose: Why would you be looking for vulnerabilities during legacy to C++ conversion rather than during testing?

We look for vulnerabilities during the legacy to C++ conversion process rather than during testing because addressing vulnerabilities during conversion allows us to make sure that the codebase is secure from the beginning of launch in the new language. Developers can also prevent security flaws from carrying over into the new code and finding vulnerabilities early in the process allows developers to include security best practices in the code and not create it later, as a sort of afterthought.

* Solutions: How do you determine the appropriate fix to a security vulnerability?

Determining the appropriate fix for a security vulnerability requires us to have a clear understanding of the vulnerability and its potential impact on the system. Developers can use practices like input validation, proper error handling, secure coding practices, and the use of security libraries and frameworks like RMF, CSF or reference to best practices created from the NIST.