Chris Gollnick

Module 6-1 Journal

CS410-T3717

11 February 2022

**Define: What is a security vulnerability?**

A security vulnerability can be defined as flaw, weakness, and/or error in a systems source code that can be utilized and exploited by a third party to obtain access to a targets’ system or data without the targets permission to access such information.

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

While there are numerous and plentiful vulnerabilities in code, some of which can be things like Buffer Overruns where external data overflows and allows a third party malicious code to run, use of home-made encryption code that is often less secure and easy to crack, and complex code which can allow for more vulnerabilities to exist as the complexity of the code can lead to blind spots that simpler code can find easier.

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

During a conversion you may be working with code that was meant to be patched at a later date and was forgotten about or never done. As a result those vulnerabilities would still potentially exist after the conversion leaving your new code entirely vulnerable to security attacks. By looking for these issues in the legacy we can ensure we do not bring those issues over and when we test later we can focus in on testing and checking security on things in C++ and that we implemented.

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

While you can have multiple vulnerabilities to patch, working at them in the order discovered is not the most prevalent way to work. Rather assigning them risk levels and working on those of the highest risk first is more appropriate manner to work with. This in it of itself is not a standard ranking. While tools exist to show you which are the most critical, some of these may be more serious to you depending on your code and the industry or business it is deployed in. Integer conversion security vulnerabilities may be critical when you deal in a financial industry but may be further down the list if your product is an OCR software for example.