CS-410-T2855 Software Reverse Engineering

6-1 Journal

Eric Wallace

Dec. 4, 2022

* **What is a security vulnerability?**

A security vulnerability is a code flaw or misconfiguration which attackers can gain unauthorized access to a system or network. Once inside, attackers leverage authorizations and privileges to compromise systems and assets. In recent years, IoT devices have been the subject of attacks because these devices seem to lack the security of mobile or PC applications.

* **What kind of vulnerabilities would be identifiable in C++ code?**

One of the major vulnerabilities in C++ is buffer overruns, string vulnerabilities, integer overflows. While these vulnerabilities are easily to prevent, they are often overlooked when examining code. The vulnerabilities noted above are all associated with user input, specifically string vulnerabilities, which involves user input being included in string formatting. Invalid or incorrect string formatting is another string vulnerability that leads to application termination and memory corruption.

These vulnerabilities are somewhat easily prevented they are also easily overlooked which is why they are among some of the most common vulnerabilities associated C++ code.

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

Looking for vulnerabilities during conversions would allow code to be updated to meet secure coding standards. Testing really isn’t meant for finding outdated legacy code. So, finding vulnerabilities during conversion could reduce the number of vulnerabilities that could be missed by testing.

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

Determining and fixing vulnerabilities depends on the programming language, Java has a tool which checks a dependency’s CPE is checked against the CVE for vulnerabilities which uses the NVD as the primary source for vulnerabilities. The OWASP guidelines can also help in identifying vulnerabilities. I personally use a plugin called Snyk which covers a variety of programming languages and displays vulnerabilities.