Samuel Bailey

Week 6 Journal

A security vulnerability is a weakness that can be exploited by hackers or those wanting to do damage.

Quite frankly the world is ran on either C or Java. So when there is a problem with C there is many languages under it that have problems. For C++ specifically the largest problem is that it is vulnerable to LDAP injections. LDAP sits on top of TCP and can see everything that the program is doing including down to binary. During legacy to C++ is when the most problems occur for those who are going to be hacked. There is always updates being done to code to fix bugs and there’s many security bugs that happen that need to be patched. There’s always stories of companies not updating their software to a newer version that fixes bugs and because of that they get hacked. Testing is series and a big deal but so is updating your code from legacy code that has known vulnerabilities in it. If your code has a vulnerability I would check to see if there is a software patch for it if the source of the bug is coming from another module. If it’s your code that has a bug you need to isolate what the exact problem is. Once you know exactly what it is you can fix it and put it into testing to be released or in some cases just release it immediately. In majority of the cases the bug is usually discovered in testing or within a day or two of release.