Hanah Deering

6-1 Journal: Don’t Leave Security to the End

CS405 Secure Coding

Southern New Hampshire University

Think about how innovative the world has become, everything we do now-a-days can be done online. We don’t have to balance a checkbook anymore; we can just pull up our mobile app to see how much money we have. We don’t have to be able to navigate a map, we just type the address into our GPS on our smartphone. Security should be one of the top priorities in everything that we do, especially when it comes to infrastructures within programs. But waiting until a program is finished and ready to be taken public to address security concerns is a big no-no! Waiting until the end leaves the entire software program more susceptible to an attack. You want to incorporate and test for security flaws throughout both the pre-production and production cycles, and not leave security until the end.

To prevent threats, we can test early and test often to expose any security vulnerabilities. Addressing security concerns throughout the whole production process makes for a more solid program, protecting all information within databases. Using a layered security system (Defense in Depth) and data encryption to dissuade attackers would be a duo that makes attacks a lot harder and keeps security a top priority.

One example that I can include in my Project Two presentation of how I plan to ensure that security is addressed intrinsically and not left until an issue is discovered is using unit testing, continuously throughout the SDLC. For example, using a unit test to make sure that an SQL Injection isn’t possible on data inputs. This allows for all inputs to be “sanitized” before entering the database. Doing tests often and not waiting until the end ensures that security stays a top priority and ensures that there won’t be an issue down the road.