Nicholas Wood

CS 405 – Portfolio Reflection

A secured coding standard that I was really intrigued about is the SQL Injection and the prevention of it. When first learning about SQL injection I was unaware of how people can penetrate the system and using a simple trick of manipulating the string inserted into the system can change what is searched. If we would have left security until the end, then you would have to redo a large portion of the string settings and even change how you access the database. Many answer to SQL Injection is to prevent string inputs into the database and doing this requires a lot more rework if left to the end. Integrated security with the design of a system results in a layered system that has defense in depth and makes it easier to go back if a security issue is found. Some of the secure coding standards are needed more than others, the SQL Injection is a high severity item as it is likely to happen and the remediation cost for redoing the program is difficult. This means that SQL Injection is an important standard to adopt.

The use of Zero trust is very useful with SQL Injection as it helps maintain privileges and it also makes sure that if there is a breach then the system is not entirely compromised. The zero trust also monitors users’ activities so if they notice someone trying to access certain information constantly then they can identify an issue much quicker and see what information is exposed. Implementing these type of security policies earlier and making sure they are handled correctly can produce a system that is much more secure and can be easily integrated or updated.