8-2 Journal: Portfolio Reflection

Colton Thompson

April 10th, 2021

CS-405-H4327

**Adoption of a Secure Coding Standard and Not Leaving Security to the End**

One of the most important secure coding standards that I follow even before I took this course was to prevent SQL injection attacks in all my projects that interacted with code and databases. I always use prepared statements where I can. These coding standards I learned in this course have helped to broaden my skills however with understand buffers with underflow and overflows as well as memory protection.

Security being involved from the beginning of a design makes a lot of sense especially after having gone through this course. I used to think that security type changes could come after the functionality was complete, but it is one of the fundamentals of any software’s design and should be treated as such.

**Evaluation and assessment of risk and cost management of mitigation**

Assessing risk and cost for mitigating an attack is not an easy task especially while under pressure of a current attack. I believe that cost should be more acceptable as a choice when it comes to mitigation because the risk is likely far more expensive in the long run as it could cost you the business in general.

**Zero Trust**

Zero trust means no one is safe in terms of networking security. Trust needs to move beyond the network and to follow the concept of trust no one, validate everyone. This type of model of security was created due to the ever-moving concepts of today’s technology and workforce being more mobile than ever.

**Implementation and recommendation of security policies**

There were a lot of security policies to follow from the Defense-In-Depth diagram that we used for the presentation and the policy template. I think one of the most important policies was to rely on encryption when it comes to sensitive data that you do not want people to see.