Gabrielle Maitland

CS 405 Secure Coding

**Portfolio Reflection**

Throughout this course, I have deepened my knowledge of secure coding practices. This includes adopting a secure coding standard throughout the entirety of code development, rather than just layering it in at the mid to end of the lifecycle.

Implementing practices such as Defense in Depth, Zero Trust, Triple A methodology, and other related methods can greatly strengthen the security of an organization and its products. Early adoption of impactful security practices can strongly lower the risks of breaches by bad actors. Whether they siphoned information through intercepting unencrypted data, or whether they have caused a data breach via SQL injection, the organization will begin to hemorrhage money due to the loss of trust, clientele, and the necessity to fix a severe issue fast. This would not benefit any organization regardless of how large and well known, as these things can sometimes take years to recover from.

Severe aftershock from a breach is why it is important to recommend fresh security policies when an organization is lacking in proper practice. Not only should the current practices be audited by a security professional, but there should be increased awareness of the importance of quick implementation. It is important that organizations understand the gravity of implementing proper protocols before a breach happens rather than afterwards.

Putting many of these things into practice during this course, whether through coding assignments or analysis of mock issues, has put into perspective the importance of secure coding practices throughout the entirety of the software development lifecycle.