Benjamin Abbott

CS 405

Secure Coding

December 17, 2022

Portfolio Reflection

* Adoption of a secure coding standard, and not leaving security to the end

The adoption of a secure coding standard and not leaving security to the end will lead to the development of stronger and more secure systems and applications. Developing with security in mind will allow you to think of ways that your code can be exploited during development to allow you to prevent them from happening.

* Evaluation and assessment of risk and cost benefit of mitigation

Developing with coding standards and using a DevSecOps pipeline that integrates secure coding into the development process will lead to less vulnerabilities and more secure code. This type of development may have higher initial costs and take longer to develop but the end result is actually the opposite. With more secure code the testers are able to focus on the bigger picture and a stronger product will be produced.

* Zero trust

Zero trust framework is a security measure that protects users and their information. The triple-A framework combines authentication, authorization, and accounting to control access to system resources. It is important to always verify and authenticate to ensure that the user has the proper permissions and access.

* Implementation and recommendations of security policies

Some recommendations that I believe that will help produce the most secure and highest quality code are:

Create standards for future development.

Develop with DevSecOps pipeline.

Use encryption for all data in flight, at rest, and in use.

Use the Triple-A framework strategy

Use unit testing

Use external tools