CS-405 Secure Coding

8-2 Journal: Portfolio Reflection

Anthony Lewandowski

December 19, 2021

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

Throughout my experience in this course, I have learned that adopting a secure coding standard is incredibly important. A secure coding standard provides each person on a development team with guidance for implementing secure coding practices and principles. If everyone on the team abides by these practices, the product as a whole will be much more secure.

Following a secure coding standard also sets the developer up to have secure coding in mind throughout the development of a project. If followed correctly, the security policy will prevent the act of leaving security to the end and help the developer think about the security of the program throughout each stage of development.

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

While reviewing a security policy, it is crucial to understand the risk and cost involved when dealing with coding vulnerabilities. Businesses spend a lot of money to make sure that their technology meets a certain standard, and it is the developer's job to understand the risks involved when using unsecured code. Coding vulnerabilities can lead to a company losing a lot of money and a damaged reputation, so it is absolutely crucial to be educated in this aspect of software development.

***Zero Trust***

The Zero Trust Architecture is based on the idea of not trusting any user or device on a network. A business should know every device on its network, know every user that accesses the network, and know how to protect its assets. I believe a Zero Trust Architecture is probably the wisest decision a company could make regarding its information. Every user, device, and network connection will be authorized, making it more secure.

***Implementation and recommendation of security policies.***

Throughout this course, I went through the process of creating and implementing my own security policy. I now understand what goes into making a security policy, and there are a lot of factors to consider with each development environment. Overall I believe that a security policy could be fine-tuned to match a specific development environment but in reality, I think it is best to keep it generalized and straightforward according to the programming language being used.