Joseph A. Urso

CS 405 – Secure Coding

Southern New Hampshire University

10/23/2021

**8-2 Journal: Portfolio Reflection**

Adopting a secure coding standard and not leaving security to the end are principle practices that should be implemented at any organization that seeks to deliver efficient and secure software architecture. Coding standards help to standardize one’s product as well as aid in the development of software engineers in their capability to discern and mitigate vulnerabilities in code. Not leaving security to the end involves instituting a DevSecOps pipeline that incorporates security alongside product development. This is important when considering remediation costs and flaws that could be left unseen if security is visited *after* the end of production cycle.

Evaluating and assessing risks should be compared to cost benefits when considering how likely or unlikely a risk is, as well as the complexity of rectification. All risks should be avoided if possible, but there could exist some that would be considered highly unlikely that could be left alone for the time being if rectifying it would push back deadlines and increase maintenance cost significantly. In essence, Zero Trust should be employed in order to prevent inadvertent execution of code or potential avenues for user attack on the system. Default deny and principle of least privilege should be employed as coding standards to mitigate such risks.

Implementing security policies should be at the forefront of product design and planning. It’s important that security white papers are drafted in order to deliver the best recommendation moving forward in accordance with the functionality of the product in question. Such papers should then be revised as the organization scales and its various pieces of functionality diversify. This would essentially foster a positive, efficient and productive environment for both the product and developers alike. In the same vein, the organization could use this as a marketing tool of sorts, being able to boast a secure and modern system that their users could trust.