**Portfolio Reflection**

Joseph Veneski

Department of Computer Science, Southern New Hampshire University

CS-405 Secure Coding

Professor Kaan Esendemir

April 28, 2024

**Portfolio Reflection**

**Adoption of Coding Standard:** Secure coding standards are essential as they provide developers with guidelines to reduce vulnerabilities from the outset of development. These guidelines ensure security is not left as an afterthought by integrating it throughout the development process. Standards can help identify and mitigate common issues such as buffer overflows or SQL injections, enhance code quality, and ensure compliance with regulatory requirements (Sec1, 2024).

**Evaluation and Assessment:** Risk assessment is crucial for identifying, evaluating, and estimating the levels of risk involved in a project. A threat model should be maintained and updated throughout the development of a project as it evolves (OWASP, 2024). Various industries may face different threats, making risk assessment vital for improving resource allocation to prevent the most likely threats in each case. Threat modeling identifies potential threats where risk assessment estimates the likelihood and impact of the threats (SecureCoding, n.d.). This can lead to earlier detection of security issues with less cost to fix them.

**Zero Trust:** Zero trust is a security concept that insists systems should trust nothing, either internal or external, without verification of any access requests. The use of multi-factor authentication to verify identity can drastically reduce unauthorized access. Micro-segmentation limits lateral movement of potential attackers, greatly enhancing system security (Microsoft, 2021). Additionally, continuous monitoring as part of the Triple A (Authentication, Authorization, and Accounting) framework helps identify unusual activity and threats early, before more damage is done.

**Implementation and Recommendations:** Security policies set the rules and standards for developers to create more secure and robust systems. These policies ensure compliance with regulations and should be comprehensive and regularly updated to stay relevant. In addition to a security policy, it is beneficial to invest in regular security awareness training and participate in security audits. Regular training and auditing ensure that security remains a priority for the team. Additionally, having an incident response plan for when disasters eventually strike can help mitigate damage significantly and decrease system downtime.

**References**

Microsoft. (2021). *Evolving Zero Trust*. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>

OWASP. (2024). *Threat Modeling Cheat Sheet*. <https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html>

SecureCoding. (n.d.). *Threat Modeling and Risk Assessment*. <https://www.securecoding.org/threat-modeling-risk-assessment/>

Sec1. (2024). *The Importance of Secure Coding Standards*. <https://sec1.io/blog/the-importance-of-secure-coding-standards/>