Abu S. Alam

CS 405: Secure Coding: Dr. Sarah North

Southern New Hampshire University

March 3, 2024

Journal: Portfolio Reflection

**Adopt a Secure Coding Standard from the Start**

CS 405: Secure Coding has been an instrumental course in solidifying the importance of proactive security practices, especially in the realm of secure coding. It is imperative to adopt a secure coding standard for building software with robust defenses. These standards provide developers with a framework for secure coding practices, minimizing vulnerabilities which could be later exploited. Traditional approaches often relegate security concerns to the final stages of development. The traditional approach to development is a reactive strategy which leaves the door open for threat attackers. By integrating secure coding standards throughout the development lifecycle, the attack surface can be significantly reduced and build software with security as a core principle (*Secure coding standard*)

**Evaluation and Assessment of Risk**

Security measures come at a cost, both in terms of time and resources. Therefore, a crucial aspect of security implementation is the evaluation and assessment of risk. This involves identifying potential threats, analyzing their likelihood and impact, and prioritizing mitigation efforts based on a cost-benefit analysis. By understanding the potential financial and reputational damage a security breach can cause, we can justify the investment required to implement effective security controls (Thurmond, 2023)

**Zero Trust**

The concept of zero trust represents a significant shift in security philosophy. It dictates that no user or device should be inherently trusted within a network. Every access request, regardless of the origin, must be rigorously authenticated and authorized before granting access to resources. This approach minimizes the damage caused by compromised credentials or malicious actors within the network (*Owasp secure coding practices-quick reference guide*)

**Security Policy Implementation**

The successful implementation of security policy will rely on effective communication, training, and enforcement. Policies should be clear, concise, and readily available to all staff members. Regular security awareness training equips employees with the knowledge to identify and report suspicious activity. Finally, consistent enforcement of the policies ensures that everyone within the organization is accountable for maintaining a strong security posture.

This course has significantly enhanced my understanding of the critical role secure programming standards, risk assessment, zero trust principles, and well-defined security policies play in building and maintaining a secure digital environment. Moving forward, it should be strongly advocated the adoption of these practices within any software development project.

References:

*Owasp secure coding practices-quick reference guide*. OWASP Secure Coding Practices-Quick Reference Guide | OWASP Foundation. (n.d.). https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/

Secure coding standard. (n.d.). https://www.cisecurity.org/wp-content/uploads/2020/06/Secure-Coding-Standard.docx

Thurmond, T. (2023, December 27). *8 best secure coding practices*. KirkpatrickPrice. https://kirkpatrickprice.com/blog/secure-coding-best-practices/