Jordan Crisler

Professor Battle

CS-405-10427-M01 Secure Coding 2025 C-5

October 22, 2025

8-2 Journal: Portfolio Reflection

The adoption of a secure coding standard should be implemented by an organization to help outline a formal process to highlight their secure coding standards, principles, and best practices for their development teams to implement and follow. In addition, it is important to not leave security to the end, but rather incorporate security throughout the software development process. This includes incorporating security within the planning and design, development and testing, and post-launch phases. In addition, another best security practice is eliminating trust of all devices connected to a network to prevent security breaches. The zero-trust policy is where internal and external access attempts require verification before the user is granted access to the system, which helps to prevent security breaches. (Brook, 2024).

Evaluation and assessment of risk and cost benefit of mitigation is important to consider when developing a program. It is important to understand the risks and vulnerabilities that may exist within a program and then to evaluate those risks and assess what level of risk they pose, the cost of remediation, the severity of the risk, and how likely the risk is to result in an attack. From this evaluation, steps can be taken to prevent security vulnerabilities. Some of these steps that can be taken to prevent security vulnerability threats include building the architecture of the program with security in mind, using threat modeling to identify potential security vulnerabilities, using encryption to protect sensitive data, validating any input from users, implementing strong authentication methods such as multi-factor authentication, session management, only allowing users to have enough access needed for their role within the system, and securely handling any errors or exceptions that may arise (OWASP, n.d.).

The implementation and recommendations of known security policies should follow well known and recognized standards, such as OWASP. These security policies should be continually updated and added upon as security evolves, and new vulnerabilities are discovered. Some examples of security policies that can be implemented include the use of input validation methods, encryption, the Triple-A framework (authentication, authorization, and accounting), and security reviews and testing methods.

References

Brook, C. (2024, October 23). *Understanding the Zero Trust Security Model to Safeguard Digital*

*Infrastructure*. Fortra. https://www.digitalguardian.com/blog/understanding-zero-trust-security-model-safeguard-digital-infrastructure

OWASP. (n.d.). *Secure Coding Practices*. OWASP. Accessed on October 8, 2025, from:

https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/02-checklist/05-checklist