8-2 Journal: Portfolio Reflection

Duane Wegner

Southern New Hampshire University

CS-405 Secure Coding

Alan Spencer, Adjunct Instructor (M.S)

August 19, 2025

**Journal Reflection: Secure Coding, Risk Assessment, and Security Policies**

Secure coding is an essential part of software development. It should be applied from the beginning of a project and not left to the end. Adopting a secure coding standard helps prevent vulnerabilities that could be exploited later. Practices such as input validation, proper authentication, and encryption protect user data and maintain trust. For example, the LinkedIn data leak showed how failing to address security early can have long-term consequences for users and organizations (Cyber News Live, 2025).

Evaluating and assessing risk is another key part of maintaining strong security. Organizations should consider the potential impact of a security threat against the cost and effort required to prevent it. The FortiOS SSL VPN vulnerability required urgent attention because of its potential impact on many systems (Ford, 2022, Henderson, 2023). By assessing risk, companies can prioritize the most serious vulnerabilities and use their resources effectively. This ensures that security actions are both practical and meaningful.

Zero trust is a security concept that assumes no user or system should automatically be trusted. Every access request must be verified, and activity should be continuously monitored. Applying zero trust reduces the chance of unauthorized access and limits potential damage from threats inside or outside a network. This approach supports secure coding practices and risk assessment by creating a framework for real-time protection.

Finally, implementing strong security policies is critical. Policies provide clear guidance on secure coding, risk evaluation, and incident response. They must be updated regularly to address new threats, such as vulnerabilities in software like FortiOS (Fortinet, n.d.). When combined with developer training, security policies ensure that security becomes a part of everyday development rather than an optional task.

In conclusion, secure coding, risk assessment, zero trust, and effective security policies work together to protect systems and data. Addressing security from the start, evaluating risks carefully, verifying all access, and enforcing clear policies allows organizations to prevent breaches, respond quickly to threats, and maintain user trust. These practices help build strong and reliable software.

**References**

Cyber News Live. (2025, January 1). LinkedIn data leak: 3 years later. https://cybernewslive.com/linkedin-data-leak/

Ford, E. (2022, December 13). Customer Advisory: FortiOS SSL VPN Vulnerability (CVE 2022 42475) exploited in the wild. Deepwatch. https://www.deepwatch.com/labs/customer-advisory-fortios-ssl-vpn-vulnerability-cve-2022-42475-exploited-in-the-wild/

Fortinet. (n.d.). FortiOS Operating System. Fortinet. https://www.fortinet.com/products/fortigate/fortios

Henderson, S., Kittner, C., Hawley, S., & Lechtik, M. (2023, January 19). Suspected Chinese threat actors exploiting FortiOS vulnerability (CVE 2022 42475). Google Cloud. https://cloud.google.com/blog/topics/threat-intelligence/chinese-actors-exploit-fortios-flaw