8-2 Journal: Portfolio Reflection

Sean Glass

CS-405: Secure Coding

Southern New Hampshire University

October 27, 2024

In software development, security needs to be integrated from the beginning, not left as an afterthought. Adopting secure coding standards helps ensure vulnerabilities are avoided early in the process. Addressing security early is both cost-effective and essential. Secure coding standards help mitigate common issues like SQL injection and buffer overflows, reducing the need for costly rebuilding later.

This approach aligns with the zero-trust model, which assumes that no component can be trusted without constant verification. Including secure coding practices early supports zero trust by ensuring systems are durable against threats. Regular code assessments are important in maintaining this model and ensure that all components are treated as potential risks.

Risk evaluation is necessary to determine which vulnerabilities to address first. By analyzing the impact of vulnerabilities instead of the cost of fixing them, organizations can prioritize high-risk issues that could lead to breaches. For example, automated tools for static code analysis can detect vulnerabilities early, which makes them a great investment compared to the potential costs of a data breach.

Security policies provide a consistent framework for applying security practices across an organization. These policies should include secure coding guidelines, code reviews, and automated testing practices to ensure compliance with industry standards. These policies ensure security is integrated into every phase of development, reducing risks and improving resilience.