**CS 405: 8-2 Journal: Portfolio Reflection Assignment**

Mohammed Khan

Bachelor of Science in Computer Science, SNHU

CS 405: Secure Coding

Prof. Dewin Andujar

April 20, 2025

**CS 405: 8-2 Journal: Portfolio Reflection Assignment**

Adopting a secure coding standard is crucial for preventing common web application vulnerabilities. By following a set of guidelines and best practices, developers can make sure that their code is secure and reliable. This approach helps to reduce the risk of security breaches and vulnerabilities. In fact, many common web application vulnerabilities are caused by insecure coding practices. Think of it like building a house. If you don't follow building codes and best practices, you might end up with a house that's prone to collapse or fires. Similarly, if you don't follow secure coding standards your software might be vulnerable to security breaches.

Evaluating and assessing risk and cost benefit of mitigation is important to make sure that security measures are effective and cost efficient. This involves identifying potential risks and assessing the cost of mitigating them. By doing so, organizations can determine whether the cost of mitigation is worth the benefits of reducing the risk.

Zero trust is a security model that assumes all users and devices are untrusted and grants access to resources on a least privilege basis. This approach reduces the risk of security breaches and unauthorized access to sensitive information.

Implementing and recommending security policies is important to make sure that security measures are effective and aligned with business objectives. This involves developing and implementing policies that outline security procedures and guidelines. By doing so, organizations can make sure that security measures are consistent and effective across the organization. To improve security, it's a good idea to create clear rules for writing safe code. You should also look for possible security problems and figure out how serious they are and what it would take to fix them. Using a Zero Trust approach means only giving people access to what they absolutely need and nothing more. It’s also helpful to write down basic security rules and steps so everyone knows what to follow. Lastly, it’s important to think about security from the very start of building any software so that it’s protected right from the beginning.