Mary Vuong

CS-405 Secure Coding

June 30, 2024

8-2 Portfolio Reflection Journal

**Adoption of a secure coding standard, and not leaving security to the end**

Adopting a secure coding standard ensures that security is integrated throughout the software development lifecycle. It emphasizes that security should be a priority from the beginning, not an afterthought. This approach helps identify and mitigate potential vulnerabilities early, making the development process more efficient and cost-effective. Developers can avoid common vulnerabilities like SQL injections and buffer overflows and ensure a more secure end product by implementing secure coding practices, such as input validation and regular security assessments.

**Evaluation and assessment of risk and cost benefit of mitigation**

Evaluating and assessing risk involves identifying potential security threats and determining the likelihood and impact of each. This process allows organizations to prioritize which risks to address first based on their potential damage and the cost of mitigation. Organizations can allocate resources efficiently and guarantee that the most critical vulnerabilities are addressed as soon as possible by performing a thorough cost-benefit analysis. In the end, this strategic approach improves overall security without needless spending by striking a balance between security requirements and financial limitations.

**Zero trust**

Zero Trust is a security model that assumes threats can originate from both inside and outside the network, requiring strict verification for every access request. This approach enforces principles like least privilege and network segmentation, significantly reducing the risk of data breaches and insider threats. Zero Trust reduces vulnerabilities and stops possible threats from spreading throughout the network by enforcing stricter access controls and ongoing monitoring. Its effectiveness is demonstrated by real-world examples, which I believe makes a strong case for its adoption even in spite of the initial inconvenience to users.

**Implementation and recommendations of security policies**

Protecting organizational data and systems requires the implementation of strong security policies. This includes adopting a comprehensive security framework like the Defense in Depth approach, which layers multiple security measures to ensure redundancy and protection. Policies should be regularly reviewed and updated to address emerging threats, and employee training programs should be instituted to raise awareness and preparedness. Effective security policies provide a clear structure for maintaining security standards, ensuring compliance, and responding swiftly to incidents, thus fortifying the organization against potential cyber threats.