Gabriel Balicki

CS-405-T4239

Aaron Demory, M.S., M.B.A., CISSP, CEH

7 April 2023

Module 8 Journal: Portfolio Reflection

Throughout this course, I have learned about the criticality of adopting a secure coding standard and prioritizing security in the development process. The integration of secure coding practices, such as input validation and output encoding, is necessary to prevent common vulnerabilities such as cross-site scripting and SQL injection. Additionally, security testing and vulnerability scanning should be conducted early in the development process to identify and address potential security issues.

It is crucial to evaluate and assess the risk and cost benefit of mitigation when implementing security measures. A comprehensive risk assessment helps to identify potential threats and vulnerabilities, as well as analyzing the potential impact of each threat and the cost of implementing mitigation measures.

The concept of zero trust is another essential aspect I have learned throughout this course. The zero trust model assumes that all devices, users, and networks are untrusted, and implementing security measures such as multi-factor authentication and network segmentation to protect sensitive information.

Finally, implementing and recommending security policies based on industry standards and best practices, tailored to the specific needs of an organization is crucial. These policies should be communicated and educated to stakeholders, and monitored and enforced through regular security assessments.

Overall, by adopting a comprehensive security strategy that integrates secure coding practices, evaluates and assesses risk and cost benefit, implements zero trust measures, and develops and enforces security policies, organizations can better protect their sensitive information and mitigate the risks of potential security breaches.