Harris McCall

CSIA300

Matt Boehnke

Lab 8

Secure Coding Policy

Objective:

To ensure that all software developed by XYZ Corporation is coded in a way that prioritizes security, minimizes vulnerabilities, and adheres to industry standard security best practices.

Scope:

This policy applies to all programmers, code reviewers, and any other personnel involved in software development within XYZ Corporation.

Policy Statements:

- All code must be written while keeping the OWASP top 10 vulnerabilities in mind, eliminating the most common vulnerabilities.
- Developers must receive regular training on secure coding practices, as directed by SANS Secure Coding Guidelines.
- The code should be reviewed and tested for security vulnerabilities at every stage of development.
- Insecure code should be remediated as promptly as possible.

Enforcement:

Violations of the secure coding policy will result in appropriate disciplinary actions, up to and including termination of employment. Software code will be audited regularly to ensure compliance.

Software Development Lifecycle (SDLC) Security Policy

Objective:

To integrate security checks and measures during the SDLC, ensuring that security is of primary concern throughout the entire process.

Scope:

This policy covers all phases of the SDLC for any software development projects at XYZ Corporation and applies to any personnel involved in the Software Development process.

Policy Statements:

- Security requirements should be defined and integrated from the beginning of the SDLC, according to ISO/IEC 27034-1:2011.
- Risk assessments should be conducted at each phase of the SDLC to identify and mitigate or eliminate potential security risks.
- Each release must undergo thorough security testing, including code review and rigorous application testing before its deployment.
- Incident response and recovery plans must be established to handle potential security breaches.

Enforcement:

Lack of compliance with SDLC security requirements will result in a review of the project status and can lead to project suspension until compliance is achieved. Any individual employee caught not adhering to the SDLC security requirements for XYZ Corporation may be terminated if compliance is not achieved. The security team will monitor for compliance.

Third-Party Library Usage Policy

Objective:

To manage risks associated with the use of third-party libraries and ensure that these libraries do not introduce vulnerabilities into XYZ Corporation's developing software.

Scope:

This policy applies to all employees of XYZ Corporation who select or manage third-party software libraries to be used within the software development process.

Policy Statements:

- Only approved third-party libraries will be used, and they must be regularly checked for updates and security patches.
- Each library must be verified as a secure library by referencing available vulnerability databases and should not be used if vulnerabilities are found.
- A record of all third-party libraries and their versions being used throughout the process should be maintained, along with a history of completed security checks.
- Out-of-date libraries must be updated quickly or replaced with more secure alternatives if a secure update is not available.

Enforcement:

Lack of compliance with the third-party library usage policy will result in immediate review and potential remediation actions, including code refactoring or library replacement. Compliance will be audited monthly.