Braden Whitcher

Dr. Ogoh

CS-405

28 June 2025

Module Eight Journal

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

Thorough research and meetings with the team should be done before adopting a new secure coding standard, to make sure that it is appropriate and fits well with the current project. Not leaving security to the end is one of the major ways to reduce security vulnerabilities in software applications. Way too often teams wait until the very end to test the features before shipping to production, only to find that they still have a lot of work to do. By implementing security and testing it after each iteration, it greatly reduces the time and cost to fix any errors and bugs in production and increases the integrity of the system.

* Evaluation and assessment of risk and cost benefit of mitigation

Integrating security at the very beginning and throughout the project can help the company save hundreds of hours of developer time and thousands of dollars from bugs and errors in production. One bad security break-in from a malicious attacker can cause serious damage to the application, privacy of its users, and integrity of the company.

* Zero trust

Zero trust is a common security policy that assumes everyone is a malicious attacker. No matter the user or role, it provides strict identification, and authorization features and implements the principle of least privilege.

* Implementation and recommendations of security policies

All ten security policies should closely be followed and implemented in any software application. For teams who normally don’t practice it, it should slowly be introduced and integrated in. This way, everyone gets a chance to thoroughly learn it and the benefits it offers.