8-2 Journal: Portfolio Reflection

Terry Bishop

Secure Coding

SNHU

Professor Prasad

April 19th, 2023

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

There is a correlation between time and cost regarding software security. If a software engineer waits until the end to secure their program, then they will have to go through the structure of the application which might have effects on other parts of the structure. This will be time-consuming which in turn will be costly. Additionally, if the engineer has a deadline, they might feel rushed and might overlook a vulnerability in their application.

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

It is important to evaluate the coding standards for the application you are building and ensure the code is in compliance. Additionally, you can make an assessment on the threat level of each coding standard such as the severity, likelihood, remediation cost, priority, and level.

* **Zero trust**

It is important to have a zero-trust policy in place. This will help prevent any unauthorized person from accessing sensitive information. This can be accomplished by using the Triple-A framework (Authentication, Authorization, Accounting) in conjunction with defense in depth. Additionally having an encryption policy in place such as Encryption at rest, encryption at flight, and Encryption in use can help in this area.

* **Implementation and recommendations of security policies**

There are four Implementations and recommendations I would consider when applying security policies:

* 1. Front-end security (input/validation constraints)
  2. Backend Security (protecting your server)
  3. In transit (sending sensitive information over the net)
  4. In-house (sensitive information laying around)