Southern New Hampshire University

CS 405 Secure Coding

Professor Mike Prasad

Student: Tyanna Prince

12/17/2022

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

Incorporating security throughout the Development lifecycle of software is not something we often think about. But, by incorporating security principles into the everyday processes helps to reduce risks that may be associated with security. Being able to adopt a secure coding standard from the beginning is something that every developer needs to do. Discussing security code along with principles and standards should be done before the code begins to be written. By doing so any risk that may be associated with security is reduced and the prevention facet of defense in depth is implemented even before the project begins.

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

You cannot predict where security threats will be, rather they are internal or external. There are always risks with decisions made daily and should be what drives any force during the decision making. It is a daily reminder that any thread today may or may not be the threats we face in the future, and we must understand that there are consequences if a potential threat is not addressed. Not to mention the cost for addressing said threats is extremely small if you compare it to the cost of mitigating the risks that come with a threat. By implementing code techniques, testing starting from beginning to end, and performing code analyses helps prevent these threats.

**Zero Trust**

Technology is always expanding and moving forward, it is something that will continue throughout our lives in developing and improving. By always implementing zero trust, it helps where the traditional authentication methods may fail. We must always verify with every user, device, network, and data access to any application. 2 step authentication, biometric authentication, as well as usernames and password verifications are implemented. With the modern times we have adapted single sign on verifications as well.

**Implementation and recommendations of security policies**

Security policies are very important as they give a guideline that helps ensure that our code as well as our data stay safe and secure. Reviewing, Creating, Maintaining, and following these security policies are something every company should have adopted by now. These security policies contain the core principles, best practices, and coding standards to be implemented into any and every development project being created. This helps with consistency with implementing safe and secure code. The FTC has learned many lessons with the evolving technology and risks. This helped them lean of common vulnerabilities through real life lessons. Things like controlling a user’s access to any data, storing as well as transmitting any data safe and securely, and user authentication. There are many best practices that should be followed to keep software and data up to date. Such practices like patching and requiring a password for any user accessing systems.