William Colon

Portfolio Reflection

**Not Leaving Security to the END**

It is sometimes presumed that security cannot be incorporated during the entire Software Development Lifecycle and is deferred until the conclusion. By integrating security concepts and practices into daily operations, associated risks are mitigated. It is imperative to be proactive and implement secure coding standards from the outset. Security must be addressed prior to the commencement of any coding activities. Implementing the preventative component of Defense in Depth from the outset substantially mitigates security concerns.

**Mitigation of Risk**

Security threats may originate from internal and external sources. Risk assessments should inform daily decision-making procedures. We are often reminded that the threats of today differ from those of tomorrow, and neglecting to address any prospective threat might result in significant repercussions. The cost of resolving dangers is negligible compared to the expense of reducing the hazards linked to each threat. It is imperative to employ straightforward coding methodologies, execute early and regular testing, and carry out static code analysis following each code modification. Furthermore, automated unit testing and penetration testing must be performed routinely.

**Zero Trust**

Given the rapid advancement of technology, it is imperative to consistently implement a zero-trust approach, as conventional authentication methods are becoming inadequate. All users, devices, networks, and data access points must undergo consistent verification. We have instituted user verifications such as biometrics and multifactor authentication, alongside conventional usernames, and passwords. Applications are undergoing updates to incorporate Single-Sign-On access verifications.

**Security Policies**

Security policies establish protocols to safeguard code and data. It is imperative for any organization to establish, uphold, evaluate, and comply with these policies. They encompass fundamental ideas, coding standards, and optimal practices that must be incorporated into every development project. This guarantees uniform safety when these policies are adhered to.

**Best Practices**

With the rapid advancement of technology, the FTC has acquired numerous insights. These insights have resulted in suggestions targeting prevalent weaknesses that have affected numerous companies historically. Essential lessons encompass the management of user access to data, the assurance of user authentication, and the secure storage and transmission of data. Best practices include maintaining updated software and swiftly implementing updates for users. Implementing password regulations is crucial.