### SNHU

### 8-2 Journal: Portfolio Reflection

Eric Kleihege

### Mike Prasad

### CS 405 – Secure Coding

02/23/2023

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

By adopting a secure coding standard, the first step has been taken to ensure an ordered set of instructions has been put in place to be followed. This standardization allows all team members working on a project to conform to the same set of guidelines, ultimately increasing the amount of similar coding practices to be conducted throughout the lifetime of a project. This goes hand in hand with not leaving security to the end. By not leaving security to the end, a proactive approach to better ensure a secure application will be developed can take place. The adoption of a secure coding standard is a great way to kickstart this mindset of “not leaving security to the end.”

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

When evaluating a system or application from a risk assessment and cost benefit standpoint, it’s best to utilize threat matrixes to ensure proper standards or coding principles are put in place to reduce the likelihood of devastating software attacks. A threat matrix will provide a graphical way to quickly analyze where potential vulnerabilities may lie and allow for more stringent coding standards to be called forth, or stricter guidelines around implementations of current standards already set forth. The evaluation and assessment of any project is a worthwhile task as this can alleviate any unforeseen headaches later in the development process, or after a project is launched.

**Zero trust**

Zero trust is the proper mindset to have when designing and developing an application. We want our applications to allow only those individuals who are authenticated and authorized to use/work with it. By ensuring a zero trust policy is set forth, we can utilize this principle along with AAA to account for any malicious use or attacks of an application throughout its lifetime.

**Implementation and recommendations of security policies**

Security policies are merely written descriptions of what should be done throughout a development process, but are only as good as their implementation. By providing proper training to everyone who will be helping develop or design an application, the implementation can be better perceived to be utilized properly.