6-1 Journal: Don’t Leave Security to the End

The practice of secure coding doesn’t begin when an application is complete. In fact, it begins in the planning stages of software development. During this stage it’s imperative that developers identify things like variables, how the program should work, and how it should not work. Other items that should also be considered are who has access to data, how user information is stored, does our data need encryption, do we need to obtain un-necessary information like passwords or debit card information and if so, we need encryption security.

Some ways to prevent threats from being a nuisance are to practice safeguard measures. One way to think about security is threw the vision of automation. Since humans are prone to errors, automation can reduce the risks of human error and make security measures more manageable. Another way to reduce risks is to Keep it Secure and Simple (KISS) so that there the code is not complex making it easy to understand secure methods being implemented. As developers we often overthink our logic and make things to complex inducing harder to write secure code.

When implanting these secure methods at the beginning of code, there are additional ways to ensure, or application is as secure as possible. One of those ways is having a security policy in place to ensure there are statements about the information stored. These statements normally outline who should have access to that data as well as what data they shall have access to.

Personally, when writing new code its important to understand the ask. What is the company asking the code to do? Once we understand the logic, we need to identify the variable that will be stored and where they will be stored. In most cases, software is collecting data from user input. Once we’ve identified our potential threats we can then begin writing code that contains secure methods like logic to reduce runtime errors, fallbacks, and return error messages to mitigate application crashes.