Daoud Sogoba

CS-405: Secure Coding

Professor Trevor Hodde

November 22, 2021

Don’t leave security to the end is a statement that communicates the need for security to part of the process of development. It is much easier to secure software as it is being developed instead of after it is largely complete. The sooner that focusses can be put on reducing the number of attack vectors a software stack will face, the sooner a secure product can be completed and delivered to a customer. Take for example the creation of a data storage facility that houses servers with sensitive information. Security apparatuses are most effective when used in the defense in depth strategy. This meaning a redundant multilayered defense. In software development this ranges from the use of input verification at the code level to the physical barriers and security guards found in the data storage facilities of cloud service companies.

One of the most useful tools that software developers can make use of is unit testing. It allows developers to test their methods and classes to ensure that only the expected behavior occurs. It may also allow developers to identify security flaws with how they manipulate data and memory in the software. One of the other great tools developers can make use of is the principle of list privilege. This principle says that people should be given the least number of privileges required to complete the work they need to do. This limits the security risks of users making improper use of their permissions and prevents threat actors from making use of compromised privileged accounts.

One example that I include for threat prevention would be that of default deny where permissions may be managed. The used of the default deny allows developers to remove any chance that they may forget to disable anyone permissions for users. It allows developers to only turn on the permissions that people actually need.