Jada Thibodeaux

8-2 Journal: Portfolio Reflection

CS-405 T5640 Secure Coding

Professor Trevor Hodde

June 25, 2022

Adopting a Zero Trust policy can allow the security of access to those that are only authorized to do so. It also ties into the Triple AAA (authorization, authentication, and accounting) which keeps track of who, what, when, where, how, and why having to do with history of the software access. In a nutshell, limiting and tracking the audience and network of which the data is being accessed by, because not every computer in the network needs to have access to the data provided by all other computers in that same network.

When testing in the design phase, adhering to security policies recommended are crucial, because code is only good if it runs correctly, and if it does not, we must find out why it does not to do so. Adding assertions within code is important because this allows us to verify and test our expressions as we go along. Involving unit tests and making sure all assertions and tests pass allow for a well-defined product. Testing earlier on should be an included factor, because if we wait until later in our DevSecOps cycle closer to implantation, we may notice things that we did not before, costing wasted time, and money.

The coding principles and standards mission can be used to create a stable foundation to ensure security and prevent vulnerabilities that are often missed. These fundamentals are good for a beginning software developer to change their software from DevOps to a full scaled DevSecOps software. In conclusion, it is recommended to keep up with all the security practices whenever you think that you know enough that means that you should learn more because nothing is ever 100% secure.