Jiayu Lin

Portfolio Reflection

CS-405

6/23/23

Throughout this course, I have gained much knowledge about secure coding. This includes the adoption of secure coding standards and not leaving security until the end. Security is a fundamental component of many industries, and for good reason. Data is one of the most important things companies can hold as hackers can capitalize on this for personal gain or to ruin individuals and companies. Because of this, security should not be left till the end but instead be a core part in all aspects of software development. By not conforming to this, we leave ourselves a victim of an attack at any moment. This can be displayed with the many attacks onto large corporations over the years such as on Yahoo or LinkedIn. From this, we must think to ourselves that if multi-million-dollar companies are susceptible to attacks, so are you.

To better protect ourselves, there are many things we can do. For one, the zero-trust principle is a great mentality to have. Attacks can come from anywhere and by anyone, therefore, it is better to be safe than sorry. To accomplish this, the principle of least privilege is a large component. By keeping access to only what is needed to perform the functionality, we limit the potential entry ways attackers can utilize. Another way is the creation of security policies. These policies will define standards to follow and vulnerabilities to look out for. With standards, we create a more consistent environment for development as well as making developers more aware of areas of attacks.