Joshua Battaglia

Professor Esendemir

CS-405: Secure Coding

27OCT2024

**Journal 8-2: Reflection**

As developers and computer scientists, it is our responsibility not to leave security to the end. Everyone plays a part in ensuring that a product or application is safe for our users. There are numerous resources available for making sure code is secure, especially with high-risk programming languages such as C and C++ known for memory leaks and prone to buffer overflow/underflow. A standard should be made to ensure the common developer can secure exploitable portions of an application or system.

            Evaluating a system or application can mitigate the risk of hacking. An assessment can determine the risk level of a system or application and begin work to secure it. The cost of leaked sensitive information usually outweighs the cost of investing in security. Security should be a priority when developing software.

            Zero trust is a great policy to adopt because anyone can be a threat to the system or its applications. Due to many different motives, there is always a risk of insider threats, so you should practice only providing the necessary permissions to certain users both inside and outside of the development team.

            Implementing a security policy takes time. A team must be trained and establish a plan. Assessment of the product and the company's threat landscape should be made to ensure common or existing exploits can be mitigated, monitored, and eliminated. A policy needs to be created for developers to follow when writing code because security is everyone’s responsibility. The team needs to be educated and if an attack does occur an action plan must be in place to handle the incident. Once the incident is closed the team will also need to reassess and begin planning for the next cycle.