Jesse Kniss

CS-405

Portfolio Reflection

Throughout this course, we have discussed many topics and ideas that relate to secure coding. But what exactly is secure coding? Secure coding is typically understood as the practice of developing software in a way that guards against the introduction of security vulnerabilities. (Bellairs, 2019) Whether the application is run on a personal computer, mobile phone, enterprise server, or some other device, secure coding practices should be followed to safeguard against attacks.

Technology has advanced at a rapid pace, and so has our reliance on these systems. Software is integrated into applications across many fields, some of which contain sensitive personal data, financial data, and even data that can be lethal in the wrong hands. If not secured properly, hackers can attack systems and take control of systems that can lead to compromised secrets, loss of service, financial loss and fines, and even death. (Bellairs, 2019) Fortunately, there are practices developers can follow to protect and eliminate code vulnerabilities.

A common best practice of secure coding is not leaving security until the end. Cyber-attacks have increased in frequency and sophistication every year. In 2021, 37% of global organizations said they were the victim of some form of ransomware. (Frank Dickson, 2021) Another study showed over the last five years, that up to 76% of all vulnerabilities were from applications. If organizations choose to implement security from the beginning, shifting left can start addressing that 76% in just one step. (Mellen, 2021)

Organizations should also adopt policies and practices that are proven to be effective in limiting vulnerabilities. Defense-in-depth is the idea that security should be implemented in layers to mitigate attacks and reduce the impact of an attack if successful in getting through one or more layers. A solid defense-in-depth strategy incorporates an adoption of secure coding standards and best practices, evaluation and threat assessments, automation tools and, training employees on common vulnerabilities and defense methods.

The threat of cyber-attack goes more sophisticated each day, and it’s important to act before it’s too late. Just two weeks ago, some of the largest U.S. airports were hit by cyber-attacks. Though these attacks did not tamper with systems such as air traffic control, or airline communications, they highlight the importance of secure coding. (Josh Margolin, 2022) Security is everyone’s responsibility, and developers should always keep these practices in mind.