Secure Coding

8-2 Journal: Portfolio Reflection

Heriberto Torres

Southern New Hampshire University

Throughout this course, I have learned how important it is to not only implement and design security features, but to begin by setting a secure coding standard that is expected to be followed before development. A secure coding standard outlines important coding concepts and provides examples of code that comply with each standard as well as code that does not. Many of the concepts can seem basic but can easily be overlooked by newer developers. Meanwhile, some standards are more advanced and can even serve as a guideline for more senior developers. By providing a standard at which to code by, any developer can review it and apply these concepts during development whether they are new programmers, experienced programmers, or simple new employees. It is important to create this standard from the very beginning since some security concepts may influence an application’s design such as authorization and authentication.

Much of the motivation and design for security should come from the evaluation and assessment of risk and cost benefit mitigation. Knowing what potential hazards there can be as well as the damage that can come from security vulnerabilities, one can better protect against it and determine how much security that can/should be implemented within a given budget. In addition, it is important to implement a zero-trust policy. It has become far too easy for hackers to gain access to an organization and be trusted simply because they provided basic login credentials and have been able to appear within the office location. By issuing zero trust, no one is trusted inside or outside and must provide additional login credentials that are not so easy stolen. This in itself sets up a much stronger defense; one that can help protect inside and out. I would strongly recommend that any company that cares about their business, customers, or data to implement a security policy, secure coding standards, and zero trust policy as well as practice defense-in-depth and triple A policies. Hackers have only grown more sophisticated over the years. As hackers continue to improve, so must our security and defenses against them.