Southern New Hampshire University

CS 405 Secure Coding

Journal 6-1

George Harrison Jr

What does the phrase “Don’t leave security until the end” really mean? It simply means that when using secure coding standards, the security of the code should not be left till the end of development. The objective is to write code that detect vulnerabilities and mitigate these attacks as early as possible. Therefore, code should always be written with security in mind. One article read during research use a clever analogy to explain by saying you wouldn’t put a deadbolt on a cardboard door to make it more secure when it’s not a matter of adding more locks but, improving the door instead.

There are many threats that can prevents with the use of secure coding practices. For example, SQL injections prevention. An SQL injection is when an intruder uses server input to trick the server into returning information he is not authorized to have like private functions and variables. With this information the intruder could use the returned information to create a buffer overflow which could be harmful to the organization’s application functionality.

The example above mentions SQL injections and how intruders can use the information. Prevention of SQL injections could be accomplished in code using a bind statement. This is hard coded statement that only submits the use data after cleansing occurs. The data should also be take through a check that looks for 1=1 and name=name type injection attempts.