**Don’t Leave Security to the End**

James Porter

Department of Computer Science, Southern New Hampshire University

CS 405 Secure Coding

Professor Wasim Alim

October 9, 2022

**Don’t Leave Security to the End**

The statement “don’t leave security to the end” is one that seems very simplistic but is very important. At its most basic, this statement means that security should be considered during all steps of the development process and should not be left all until the end. This is like another analogy that I have been told before, and that is that you can’t brush your teeth 10 times in one day and expect the same result as taking steps to brush your teeth one time 10 different days.

**Preventative Steps**

There are several different steps that can be taken to make sure that security can be considered during all parts of the development process. During the process of writing code, we can write out test cases to see if the code is spitting out results that are expected with the purpose of the code. We can also use theses tests to make sure that the proper exception is called when code is executed

Another way that security can be considered during the entire development process would be with proper encryption techniques. This is a step that would be dependent upon the code that is being written but depending on the process could be essential. For example, if you were writing code for a bank encryption would be an essential step, but if you were writing code needed to see if a liquor log needed to be filled out (not the actual form, just whether one needed to be filled out) encryption would not be necessary.

One last way that security should be considered is using try/catch blocks in coding projects. If these blocks are used properly, we can make sure that any input that the user provides is correct and will execute properly. If this step was ignored, any wrong input could crash the entire project or, more detrimentally, lead to security breaches where information is leaked that could adversely affect the user.

**Project Two Plan**

For project two, we are asked to address how we will intrinsically include security measures so that it is not left to the end. The first step to this would be to make sure that unit tests are included where possible to make sure that any problems could be identified earlier. Though it is not as obvious, we can make sure to follow the principle of least privilege to make sure that individuals do not have access to information that they should not have access to. One last way to make sure that security is considered during all steps of the development process is to run testing in multiple different apps. For example, we used CppCheck to double check errors that might not have been caught in our IDE environment. This allowed us to check for errors that might not have been errors in the IDE, but could cause errors later on.