Journal: don’t Leave Security to the end

The saying “Don’t leave security to the end” simply means that a software programmer should be properly securing their project throughout the creation process, and not waiting until the end to properly secure it. Writing programs in a matter that allows security throughout the project will ensure that the client data that is stored will be secured. Without this important step, the data can easily be accessed by a hacker. There are many tests that can be done to prevent a hacker from getting into the program. Unit Testing is a great method that programmers use to see the overall scope of security on the project. It will allow the programmer to test small sections of code. The smaller sections that are tested can be more easily debugged if needed. Also, it allows the programmer to break the project down into much smaller sections.

The best way to help prevent threats on a software design is to create secure code that can protect the information in all phases of the project. For example, a programmer should be utilizing proper coding methods that support the use of a secure program. Also, a programmer should take the time to read through their code to determine the level of risk that is associated with the program. This style can also help a programmer see the issues that their program has. Testing is a key contributor to securing a program successfully.

The use of Unit Testing is a great way to ensure that your code is properly written with the security that it needs. Unit testing allows the programmer to see how secure their code is and will also help the programmer debug issues if they are present. This style of testing should be done throughout the project. It shouldn’t be the last part of the project. As stated before, if a programmer waits on testing, it can lead more much bigger headaches.