This class has somewhat changed my perspective on developing software and the steps taken to ensure that my code is secure. I will apply the concepts I learned in this course to write code that is as secure as possible. I do understand that it is almost impossible to write code that is 100% free of vulnerabilities or does not introduce bugs, mostly due to how rapid technology is advancing. This may thwart possible hackers from using the software in nefarious ways or to gain unauthorized access to systems it may be associated with. Performing such things a penetration testing and unit testing will go a long way is the security and strengthening of code.

Explain this to a new developer? I would start off by explaining the different types of hackers if they don’t already know and then move into the different types of attacks and how they are perpetrated. Then I may touch on the motives of hackers as I don’t feel that information is as important as the previous two. This should give them a good understand as why secure coding is so important. I would then emphasize the importance of secure coding and some of the things that us as developers can do to produce secure code and the tools we have at our disposal that will make it easier to detect vulnerabilities and possible bugs.

The example I may use in my reflection for module eight would be adopting least privileges to software development. Despite the motives or which hat an attacker may wear, an inside threat is the most difficult to detect and protect against. By approaching development with that mentality and producing code that takes that into account may restrict unauthorized access to data. With the knowledge I have gained from this course I believe I may be able to put that into practice.