Portfolio Reflection

Throughout this course, we worked to refine our knowledge and understanding of secure coding principles and strategies. The culmination of this practice was the creation and presentation of a mock security policy document for a fictional company. There were many concepts which we were to apply such as a zero trust policy, risk assessment, and not leaving security to the end. While none of those concepts were entirely new, the importance of proper implementation was most certainly reinforced. In the creation of the security policy document, it really became clear on why security must begin at the start of a project. Our studies have shown that the entire organization must be on board and on the same page when it comes to security. This project also demonstrated why understanding the motivations of attackers and the potential risks to the integrity of code are critical. One has to understand what assets are in need of protection and what vulnerabilities may lead to an unsecure system in order to properly identify which areas are in need of attention. There are simply too many risks and vulnerabilities to plan and prepare for all which necessitates that developers identify the risks with the highest likelihood to focus their resources.

In the first half of the term, we worked extensively on tools and ways to identify these vulnerabilities within a program. This proved to be especially beneficial when working on the final project and it was good experience to practice static testing, encryption, and unit testing methods of security and verification. The programs that exist today are very layered and complex which further demands that multiple security tools are used at each stage. Along this thought, modern programs are very much in the same category as a steel chain; they are only as strong as their weakest link.