This class has taught me that having a good security policy is an important step in the development process and should be thought of throughout every step. Security should not be left to the end because by building good security throughout developers can avoid common mistakes like injection attack vulnerabilities or buffer flow overflows. One way to think of security at every step is to evaluate risk and cost benefit of mitigation of those risks. This way of addressing issues allows developers to focus on the most pressing issues first as well as the most cost-effective fixes.

Having a policy of zero trust assumes that no user can be trusted in a system and that anyone can be a threat. This way of thinking when it comes to security prevents attackers from the inside, which are more common than people might think. Zero trust means having good access controls, monitoring logs for any unusual activity, and having good identification processes like multifactor authentication and good passwords. Furthermore, creating good policies to ensure that the entire team is on the same page is equally important as implementing good security controls and practices. These policies should include specific details about the company’s security controls as well as a risk and mitigation analysis.