CS405 8-2 Journal Entry

Throughout this course I have learned some important concepts, standards and best practices surrounding security. I feel like adopting a secure coding standard in today’s world is less of a bonus and more of a necessity, whereas a decade or two ago it was definitely more thought of as a bonus. With the increase in cyber threats and the ever increasing risk of data breaches it is becoming necessary for developers and organizations to be sure the work they are doing is secure so that they are not risking any of theirs or their clients’ data from being leaked into the wrong hands. All of this stems from the idea of coding with security in mind from the beginning. We should not be leaving security to the end as this is a likely way of leaving gaps in our security or overall just overcomplicating our code. By integrating this from the beginning we are more likely to cover all bases when developing a secure system.

Another key takeaway from this course has been learning how to evaluate and accurately asses risk and cost benefit of mitigation. One thing we know for sure is that businesses always want to do what is in their best interests first and protect the bottom line. By evaluating tools that can help automate the security process this can help determine how much money is required to adequately secure their data. Learning how to determining where the greatest risks for your organization lie and what tools best help to protect those areas is key and will be incredibly valuable moving forward in my professional career.

Zero trust policies have helped me realize that the threat is not always an external individual who is actively trying to break into your systems to steal your data. It can also come from a otherwise “trusted” source to plant the seed for data leaks or to help creak that backdoor open for hackers to access later. By trusting no user, or any data that is trying to come into your system you can be sure that you are actively slowing down and in most cases, preventing malicious persons or programs from accessing your data.

From creating the security policy documentation I have become familiar with how to structure recommendations on adopting security policies and new coding standards. Being able to help layout section by section in the security policy document has helped me understand how to transcribe this specific type of information so that it can be accurately portrayed to other individuals within the organization.