# **CS 405 Module 8 Portfolio Reflection**

Secure coding has walked us through some primary concepts to consistently think about while we are working in the field. This primary concern was always implementing security throughout parts of the development process. Even before this course, we have talked about this numerous times but this course also went beyond that. We have always been told not to leave security until the end but we haven’t quite talked about in depth what to do once we do start thinking about security. During this course, we also talked about defense in depth and looked at the many ways that a computer system or asset can be set up to be defended and the layers of security there are that can be added. From the programming side, we set up a secure coding standard based on some risks and the costs of those risk being mitigated.

The secure coding standard has us look at some vulnerability types and had us assess which are the most probably or likely and which will be the most expensive to correct if needed. With this, we can try and lower the risk of those vulnerabilities being exploited by creating this standard that employees would need to follow to ensure that those vulnerabilities do not exists. Although I don’t know this for sure, it appears that most departments that are doing pretty well must have some kind of coding standard in place, whether it is their personal business one that was built from their own departments or ones that they have adopted that are internationally known. If not, now we have the skill set that will help us either contribute or possibly the background to lead such effort if needed. This is simple a form of written policy that is nice to have to refer back to for employees whenever needed.

During this course, we also talked about zero trust framework. Something else we have been told time and time again, is you really can’t trust what is being put into the system. You normally hear this with input validation but now this zero trust framework takes it a step further and just says you can’t trust anyone. Although we did not get to put this into practice very much during the course, the primary concept was understood that many things are put into place so that there are numerous gateways at which identify need to be verified before access is given. This means being able to authenticate users, devices, and IoT. Generally in the past, users would only need one access and then they would have access to the whole network. This change makes it more like a user that only has a few set of keys. Once they are in the building, they can only access rooms they have keys for but nothing else. That way, if this persons credentials or devices are stolen, the hacker has limited access to items and not everything. This process can be more time intensive since compartmentalizing everything and setting up very limited custom user access based on positions or access needs but it may very well be worth the time to set up since any hacks after that set up will be well mitigated or less severe.

Getting a general sense of secure coding and some primary concepts for cyber security, I feel more comfortable being in a room of those talking security. I have some background to be able to ask questions about specific systems or a general knowledge to better understand what is happening and may be useful in some settings for helping with cybersecurity. Although this is the case, I still have an appreciation for those that get super involved with this because it does seem like a large task to take on. I may in the future look to see about getting more education in this space.