Saram Nadeem

CS-405

4/27/24

Module Eight Reflection

When considering the adoption of a secure coding standard, we need to understand exactly what it does and how it’s important to us as developers. Security is important, but we also need to ensure that our programs and software are running quickly and efficiently. We can throw in a whole bunch of security measures, but if there no real practical application to our system then we need to make sure we’re considering the pro’s and con’s of it’s implementation. On the other hand, not leaving security to the end is something which must be practiced and implemented on a routine basis. Planning ahead is something which all companies need to practice since it can save them a ton of time and effort in the long run. It’s always easier to have a plan and implement it later down the line than it is just to implement something only when it’s needed.

Risk assessment is something which every company must do. This can be conducted at any stage of the of the SDLC and pre-production & production stage which is extremely useful for companies. Zero trust is also something which more companies should aim to implement as they grow in size and have different locations. It can prevent a great deal of threats from both inside and outside the company from occurring as well as privledge creeping which can slowly happen overtime. Limiting your total access to people who have control over private and sensitive information is a great tool. As we mentioned earlier, the implementation and recommendation of security policies is directly correlated to the needs of the company and the software they’re using. We can throw any old policy into place but if we aren’t considering the pro’s and cons of what we’re using and where we’re using it then it could harm us in the long in the run.