CS-405 8-2 Journal

It is crucial to adopt a secure coding standard and not leave security to the end. One reason is that it gives developers guidelines to follow during development that help enforce a more securely coded application. Furthermore, not leaving security to the end endures that costly hard to hard-to-identify security flaws are fixed and handled in a quick manner which could help negate expensive development costs. This also leads to evaluating and assessing the risk and cost-benefit of mitigating security risks, which can be less impactful if security is not left until the end of the software development life-cycle. Furthermore, implementing a zero-trust security policy can further help prevent security threats by adhering to this methodology through development. In conclusion, implementing and following the recommendations of security policies can help lead to a more secure application, which is not only beneficial to the user but also for the company.