Cameron Carr

08/21/2021

CS 405

Adoption of a secure coding standard, and not leaving security to the end

Throughout this course, there have been multiple examples of how security can be applied to the simplest of functions, such as logging into a database. Knowing what types of functions that you will have in a project will help create security strategies. Creating those security strategies and following those that are in place is paramount for keeping a user’s information secure. Having guidelines in place will not only help current employees but also future employees that are still developing their skills.

Evaluation and assessment of risk and cost benefit of mitigation

By implementing secure coding standards while developing a project, a team would be able to plan out how they are going to combat possible security risks. In doing this they can ensure that those that need to be on certain parts of the project have access. This will also help with the cost of providing these services. Time management can be better managed between teammates by know who is in their circle that has access to the task needing to be completed.

Zero trust

While there are many different mindsets when it comes to security, which would be based on an individual’s personal experiences, there is no better method than zero trust. This will keep it even across the board with all divisions. A security model built upon verification and trust will stay true while employees keep up with their equipment. This will allow a company to stay flexible in the everchanging remote landscape.

Implementation and recommendations of security policies

We have been over many different types of security policies, but the best implementation of security comes with accountability. Security and accountability should work together to ensure that standards are followed to the letter.