Alex Surprenant

CS 405

8/15/25

Don’t Leave Security to the End

When building a software solution, security is of the utmost importance. It should never be left to be considered at the very end of the development process, and instead should be considered throughout the development process and beyond.

During the initial design process, when the scope of the project is being thought out, developers should start out thinking of what vulnerabilities might present themselves based on the type of system that it being designed. The secure coding principles designed in this course should be utilized throughout the process to address these possible vulnerabilities, and rigorous testing should occur all through the lifecycle as well, not just at the end before deployment.

Developers should take steps during the development process to mitigate any potential security risks. The planning an design stage of the development lifecycle should be done with security at the forefront and not on the backburner. Secure coding practices should be utilized all through the process that include validation, authentication, data encryption and rigorous QA testing. After the process is complete, security should be maintained with patching and constant security monitoring.

In order to ensure that security it addressed intrinsically, I would integrate unit test throughout the application, which will be designed to validate a users input and checking for proper sanitization. I would also test for proper use of authentication and validate that the functions for doing so are working as they should for the program. Doing so at every stage of the process will ensure that any security issues are found before they become bigger problems and more expensive to fix.