Brandon Ayers

CS-405

Module 8 Journal

27-June-2025

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

In the course we learned quite a lot about coding standards and not leaving security to the end. The biggest take away for me was that security cannot be an after thought and needs to be foundational. Secure coding standards are also something that needs to be implemented at the beginning of the development cycle. Developers must understand that mitigating risk at an early stage can help prevent issues. This also includes “Defense in depth” which is something we covered multiple times. Doing all of these and using a proactive approach will greatly reduce risk.

Evaluation and assessment of risk and cost benefit of mitigation

Another topic that was covered is the risk and cost benefit of mitigation. Understanding that not all risks/threats can be covered at the same time is important so ranking these and handling the most important first is key. We covered this in an assignment where we ranked the risk as likely, priority, low priority, or unlikely. These rankings ensure resources are being used effectively and the most important issues are fixed first. You must weigh out security and budget to have a good balance that’s not too expensive but also doesn’t lack security.

Zero trust

Zero trust was interesting and a concept that was new to me. The model for this concept is “never trust, always verify”. We cant just assume that people can be trusted but rather they need to gain trust. This leans into the least privilege concept of only giving users access to things they really need. This helps change the way we perceive threats thus improving security. Zero trust implementation seems like its too much to most people but internal threats of security lead to lots of breeches. It’s important to inform people on the importance of zero trust.

Implementation and recommendations of security policies

The implementation of security policies is important and need to evolve, clear, and enforceable. They should cover a range of things that we learned such as encryption, access controls, and coding reviews both automatic and manual. These policies need to be created and backed by leadership to ensure that are enforced. The policies as mentioned before should be monitored and updated accordingly as new threats arise and issues are found.