Tonya Sanders

CS 405

Mimi Tam

10/21/2024

8-2 Journal

Throughout this course, I’ve learned that adopting a secure coding standard early in development is essential for building reliable, secure systems. Security cannot be left until the end of the development lifecycle, as late-stage vulnerabilities are more expensive and difficult to address. Practices such as input validation, following the principle of least privilege, and using default-deny rules prevent common threats like injection attacks and buffer overflows. Automated testing and DevSecOps processes further ensure that security becomes an ongoing part of coding, testing, and deployment. This proactive approach reduces risks early, resulting in better code quality and fewer disruptions, while also cutting down on long-term maintenance costs.

Another key takeaway is the importance of evaluating risks and conducting cost-benefit analyses to guide security decisions. While some security measures may require significant initial investment, they often prevent larger financial losses caused by breaches or system failures. A Zero Trust framework is also critical, emphasizing that no user or system should be trusted by default, whether inside or outside the network. This principle ensures continuous authentication and limits exposure to unauthorized access. The implementation of clear security policies is equally vital, with regular audits, policy reviews, and layered defenses helping organizations adapt to new threats. Ultimately, these strategies work together to build a security-first culture, where risks are anticipated and mitigated effectively throughout the development process.

For a career in computer science, these lessons highlight the need for a security-first mindset across all areas of development. Whether working in software engineering, systems administration, or cybersecurity, integrating secure practices from the start will be crucial for developing reliable applications. Understanding how to assess risks and implement Zero Trust models ensures that we stay ahead of evolving threats, which is essential for building a long-term career in a field where security is always evolving.