James Galbreath

6/29/25

CS-405

Security first in coding is the same and equally as important as saying safety first on a construction site. Both should be treated with the upmost importance and priority from the start of the project. Keeping this mindset can greatly reduce the possibility of rewriting if the vulnerability is detected late in the project and attacks when the project is completed.

Risk evaluation and cost-benefit analysis have also become essential tools in my security mindset. Every vulnerability has different levels of severity, likelihood, and remediation cost. By applying a structured assessment such as a threat matrix prioritize and an schedule the appropriate fix for these vulnerabilities.

Instead of assuming internal systems or users are inherently safe, the Zero Trust model requires strict identity verification for every request. It enforces the principle of least privilege and assumes breaches will occur. I love this concept because it leaves no room for mistakes to be made by giving too much access.

implementing effective security policies must be paired with thoughtful recommendations. Encryption policies, Triple-A (Authentication, Authorization, Accounting), and secure coding practices need to be clearly documented, communicated, and enforced through automation tools. Having a well written coding standards document is crucial for success.