Brooke Slampak

CS 305

As a developer, my role in addressing security concerns is to make sure the software I build is secure before launch. This involves writing clean, safe code by following best secure coding practices like input validation, encryption, and setting up proper authentication and authorization systems. It’s not just about fixing issues later but ensuring that security is built into the code from the start. I also use tools to review and analyze code for vulnerabilities, keeping security my forethought throughout the development process.

Security plays a role at every stage of the software stack and life cycle. During development, developers have to focus on writing secure code and testing it for vulnerabilities. Once the software is built, it’s important to continuously monitor it for potential vulnerabilities. This means running automated security checks, scanning for vulnerabilities, and staying alert to any issues once the app is live. The goal is to keep things secure before, during, and after deployment.

Turning a DevOps pipeline into a DevSecOps pipeline is all about integrating security into every part of the development process. This means automating security testing, ensuring infrastructure is secure, and monitoring for threats in real-time. It’s a team effort with everyone involved in maintaining the security of the software. The plan to secure the DevOps life cycle suggests securing things early, automating vulnerability checks, and collaborating across teams to stay ahead of vulnerabilities. Following this approach is key because it makes the development process safer and ensures that security is never an afterthought.