Southern New Hampshire University

CS - 305 Module Three Journal

Michael Ford

July 16th, 2025

As a developer, I’ve learned that I play an important role in making sure the software I help create is secure. Even if a company has a cybersecurity team or other protection tools in place, the code I write still needs to be safe. That means I need to be careful about how I handle things like user input, system errors, and third-party tools. My job is not just to make the code work, but to make sure it doesn’t leave any doors open for someone to break in. Solving security concerns as a developer can involve writing clean code, checking for vulnerabilities, testing my work, and staying aware of how my code interacts with the rest of the system. It also means learning from tools like OWASP Dependency-Check and not ignoring warnings just because the code still runs.

Security isn’t just in one part of the software, it’s in every layer. Whether it’s the database, the server, or the user interface, each part of the software stack can have its own risks. The same goes for the software development life cycle. Security needs to be part of every step, from planning and designing to writing and testing the code. If we only think about security at the end, we might miss something big. By adding security early in the process, we can prevent problems before they grow into real threats. This makes the whole development process smoother and safer for both users and the team.

One way to bring security into the development process is by turning a DevOps pipeline into a DevSecOps pipeline. In a DevOps setup, we focus on building, testing, and delivering software quickly. But with DevSecOps, we add security to that process, so it doesn’t get left out or treated as an afterthought. This might involve adding automated tools that check code for issues, running security scans during builds, or having regular code reviews with a focus on safety. It also means that security becomes part of the team’s culture where everyone is responsible, not just one person or department.

In the article DevSecOps – A Systemic Approach for Secure Software Development by Seetharaman Jeganathan (2019), the author lays out a plan to make the development process more secure. It includes steps like identifying risks early, using secure coding practices, testing throughout the life cycle, and encouraging developers and security teams to work together. The article also recommends starting small and growing over time as the team gets used to the new way of working. I think this plan is very helpful, especially for teams that are just getting started with DevSecOps. I would recommend following it because it covers everything from planning to operations and encourages teamwork and continuous learning.

Overall, this module helped me realize how important security is in everything I will do as a developer. It’s not just about making software work, it’s about making sure it works safely and protects the people who use it.

**References:**

Jeganathan, S. (2019). *DevSecOps – A Systemic Approach for Secure Software Development*.