**CS-305 Software Security**

**3-2 Journal: Reflection**

**James Kofa**

**September 21, 2025**

First, being a developer is a dream come through. Just being able to work on new projects, new technologies, invent new tools and build business for clients, is truly great. Security is an essential part of a software quality. The role of a developer is quite hectic. On a daily basis, one will be bouncing between different situations. One will be developing applications with threats in mind, choosing safe defaults that will protect information and systems, enforcing strong authentications, handling errors safety, managing dependence, and much more. Security is a core part of an application/software, it prevents, reduces, and provide specific access to certain individuals given the right credentials. There are many forms of security within an application/software. Some of those forms include but not limited to monitoring, logging, least privilege, and much more.

As a developer, one is responsible or writing secure code, regularly updating the overall system/applications, conduct security testing, and sometimes code review. It is a non-stop work, because people are constant sly trying to breach a security system. Especially if that organization is wealthy. Solving security concerns as a developer means understanding the system, and what is needed. It is about implementation secure code situations/practices. Also, you will need to collaborate with other security teams and understand potential risk. I believe that at every stage of an applications, security should be a huge concern. And it should be implemented in some way. In the initial designing of an application, security should be concern. Regular security testing should be a practice at an organization. It is better to hack your own system then a stranger. Writing a secure code and following those practicing should be highly encouraged. In terms of production, security system needs to be considered as well.

When it comes to DevOps pipeline into a DevSecOps pipeline, there are things that need to be consider. First, management need to foster a security culture awareness and responsibilities. Managing security in every aspect of the applications helps build that culture and awarenesses. I believe that implementing a security check need to be a priority. Implementing security in every stage of the development/DevOps life cycle helps. When it comes to the suggested plan, I will recommend it. The plan is worth following because it presents some concrete ways to adopt. The plan mention Vulnerability management, Monitoring & response, Governance & training, and even Risk assessment & threat. All of these recommendations are essential for a quality functional application/software.

**Citation**

*Software secured: Why Developer Security Awareness IS MORE THAN JUST OWASP top 10: USA*. Software Secured | Why Developer Security Awareness is More Than Just OWASP Top 10 | USA. (n.d.). https://www.softwaresecured.com/post/why-developer-security-awareness-is-more-than-just-owasp-top-10

ISC2. (2025, June 30). *The importance of security in the Software Development Lifecycle*. Cybersecurity Certifications and Continuing Education. https://www.isc2.org/Insights/2025/06/Security-in-the-Software-Development-Lifecycle

Atlassian. (n.d.). *DevOps Best Practices*. https://www.atlassian.com/devops/what-is-devops/devops-best-practices