CS 305 Module Three Journal

Jerimey Burnside

09/22/2024

My Job as a Developer

﻿As a developer, my primary responsibility is to ensure the software I create is secure from hackers or unauthorized access. To achieve this, I utilize security tools such as encryption (which conceals data so only specific individuals can view it) and authentication protocols (which verify if someone is who they claim to be). Additionally, I must regularly examine and evaluate my code to identify any potential weaknesses that malicious actors could exploit.

Security in Software Development

Thinking about security should be super important during the whole software development process, from designing and planning to launching and maintaining the program. By always keeping security in mind, developers can create programs that are protected against possible threats.

Transforming a Regular DevOps Pipeline into a Secure DevSecOps Pipeline

To make a regular DevOps pipeline more secure, developers can add several safety measures. First, they can use automated testing tools to look for vulnerabilities. Second, they can do penetration testing, which simulates attacks to find weaknesses. Third, setting up continuous monitoring and logging helps watch the system for any suspicious activity. Finally, using containerization technologies like Docker keeps applications separate from the underlying infrastructure, making it harder for problems in one part to mess up the whole system.

A Comprehensive Security Plan

It’s really important to have a plan to keep the whole DevOps process safe from beginning to end. This plan should include regular checks for weaknesses, looking over code, testing for security holes, and teaching employees about the best ways to stay safe online. By following this detailed approach, developers can better protect their programs from possible dangers.