Dreadnought Lab – Week 05: DevSecOps & Code Review

# 🎯 Objectives

Automate security checks in code pipelines using GitHub Actions, Semgrep, and secrets detection tools.

# 📋 Lab Tasks

* ☐ Clone a sample repo with intentional security issues.
* ☐ Add a GitHub Actions pipeline that runs Semgrep and a secret scanner (e.g., truffleHog).
* ☐ Push code changes and interpret the scan results.

# 💡 Challenge Task

☐ Write a custom rule for Semgrep to catch insecure shell execution.

# 🧠 Reflection

How can CI/CD security fail if scanning is only added at the end of development?