# DevSecOps Security Report

**Project:** devsecops-microservice
**Date:** 2025-09-10
**Prepared by:** Nilesh Dhumal.

---

## 1. Executive Summary

This report summarizes the implementation of security measures in the DevSecOps pipeline for the **devsecops-microservice** project.

---

## 2. Security Tools Used

- **Static Application Security Testing (SAST):** SonarQube
  Used to detect code quality and security issues.
- **Dependency Scanning:** OWASP Dependency-Check
  Scanned project dependencies to identify known vulnerabilities.
- **Container Scanning:** Trivy
  Scanned Docker images for vulnerabilities before deployment.
- **Infrastructure as Code (IaC) Scanning:** Terraform Validator and Checkov
  Validated Terraform scripts to ensure security best practices in cloud infrastructure provisioning.

---

## 3. Pipeline Overview

- **Source Control:** GitHub with branch protection rules enforcing pull requests and code reviews.
- **CI/CD:** GitHub Actions pipeline automating build, test, security scans, and deployments.
- **Container Registry:** Docker Hub with integrated vulnerability scanning on images.
- **Deployment:** Kubernetes cluster configured with RBAC .
- **Artifact Management:** Git Large File Storage (Git LFS) used for large binaries to keep repo size manageable.