HooBank

Secure CI/CD Pipeline with CircleCi

ABDULLAH 21k4783

ABDULGHANI 21k3598

Rafay Hussain 21k3560

Rafay Akbar 21k4776

Supervisor: Sir Ali Thawerani

Department of Computer Science

National University of Computer and Emerging Sciences

May 12, 2025

Table of Contents

[1. Project Overview 3](#_Toc197980557)

[2. Application Overview 3](#_Toc197980558)

[2.1 Architecture 3](#_Toc197980559)

[3. Workflow Overview 3](#_Toc197980560)

[4. CI/CD Security Pipeline 4](#_Toc197980561)

[4.1 Pipeline Access url: 4](#_Toc197980562)

[4.2 CircleCi Logs: 4](#_Toc197980563)

[5. Detailed Findings & Output: 5](#_Toc197980564)

[5.1 ESLint Report: 5](#_Toc197980565)

[5.2 Dependency-Check HTML report: 5](#_Toc197980566)

[5.3 Snyk Monitor Dashboard: 5](#_Toc197980567)

[5.4 Sonar Cloud Report: 6](#_Toc197980568)

[5.5 ZAP Report: 6](#_Toc197980569)

[5.6 SQLMap Output: 7](#_Toc197980570)

[5.7 Trivy JSON Report: 7](#_Toc197980571)

[5.8 Bandit Report: 8](#_Toc197980572)

[5.9 Checkov Report: 8](#_Toc197980573)

[5.10 Docker: 9](#_Toc197980574)

[6. Conclusion 9](#_Toc197980575)

# **1. Project Overview**

This project implements a DevSecOps pipeline using CircleCI to automate secure software delivery. The pipeline integrates code quality checks, vulnerability scanning, and security analysis tools across multiple stages of a typical CI/CD workflow.

# **2. Application Overview**

* Name: Hoobank
* Type: React Web Application
* Repository: [https://github.com/xAbdullahShaikh/DevSecOps\_finalProject]
* Deployment: Netlify ([https://hoobank.netlify.app](https://hoobank.netlify.app/))

## **2.1 Architecture**

* Frontend: React (JavaScript/JSX)
* CI/CD: GitHub + CircleCI
* Container Build: Docker

# **3. Workflow Overview**

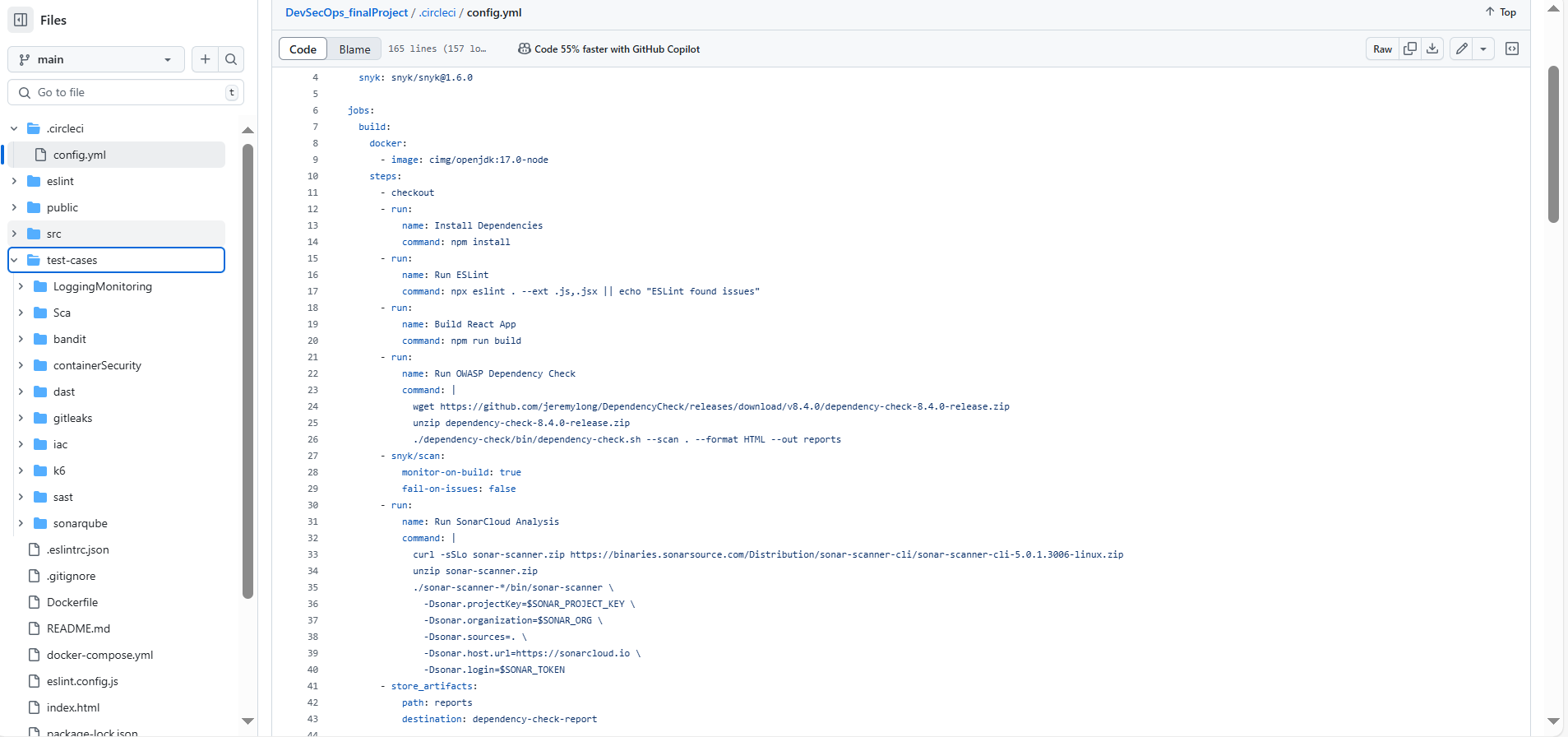
The CircleCI workflow is named secure\_build\_pipeline and is composed of the following jobs:

1. build – Dependency installation, linting, building the app, and running multiple security checks.
2. zap\_scan – Scans the deployed site using OWASP ZAP.
3. sqlmap\_scan – Tests for SQL injection vulnerabilities.
4. docker\_build – Builds and scans a Docker image, and pushes it to Docker Hub.
5. bandit\_scan – Scans Python test cases for security issues.
6. checkov\_scan – Scans Infrastructure as Code (IaC) files using Checkov.

# **4. CI/CD Security Pipeline**

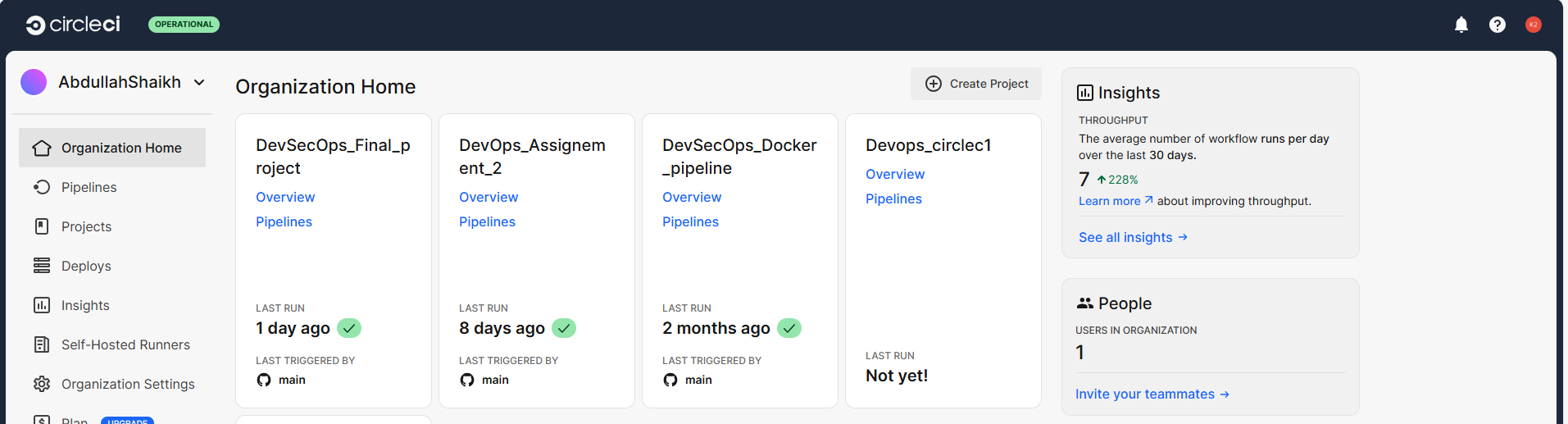
## **4.1 Pipeline Access url:**

* [Workflow - DevSecOps\_Final\_project/172/7ccd9995-d943-4326-92b3-7fc0a2d68881`](https://app.circleci.com/pipelines/circleci/LyiHW6wUbnMew9vrVRwATF/MZcvGWFGCBc6TRSn5HBtKz/172/workflows/7ccd9995-d943-4326-92b3-7fc0a2d68881)



**Figure 1: Config File**

## **4.2 CircleCi Logs:**



**Figure 2: LOG1**

A screenshot of a computer

AI-generated content may be incorrect.

**Figure 3:LOG2**

A multi-job workflow that orchestrates the following security checks:

| Job Name | Purpose | Tool/Service |
| --- | --- | --- |
| build | Dependency audit, code lint, build, SAST & SCA | ESLint, OWASP Dependency-Check, Snyk, SonarCloud |
| zap\_scan | Web vulnerability baseline scan | OWASP ZAP BaseLine |
| sqlmap\_scan | Automated SQL injection testing | SQLMap |
| docker\_build | Container build and image vulnerability scan | Docker, Trivy, Snyk Docker Scan |
| bandit\_scan | Python code SAST on test cases (if any) | Bandit |
| checkov\_scan | IaC (Terraform) static analysis | Checkov |

# **5. Detailed Findings & Output:**

* 1. **ESLint Report:** located in CI logs
  2. **Dependency-Check HTML report**: [Dependency-Check Report](https://output.circle-artifacts.com/output/job/fdc0a5d9-ab7b-4b68-b01e-328ed36bd6c5/artifacts/0/dependency-check-report/dependency-check-report.html)
  3. **Snyk Monitor Dashboard:** [xAbdullahShaikh/DevSecOps\_finalProject | Snyk](https://app.snyk.io/org/xabdullahshaikh/project/85406dc5-3c32-493a-8a7c-9680266f18de?fromGitHubAuth=true)

A screenshot of a computer

AI-generated content may be incorrect.

* 1. **Sonar Cloud Report:** [Security Hotspots - DevSecOps\_finalProject in C0D3NaM3AB SonarQube Cloud](https://sonarcloud.io/project/security_hotspots?id=xAbdullahShaikh_DevSecOps_finalProject)

A screenshot of a computer

AI-generated content may be incorrect.

* 1. **ZAP Report:** [**ZAP Scanning Report**](https://output.circle-artifacts.com/output/job/28dc8b99-18bb-4c92-acb2-d35743533fa7/artifacts/0/zap-report)

A screenshot of a computer

AI-generated content may be incorrect.

## **SQLMap Output**

**A white background with black text

AI-generated content may be incorrect.**

* 1. **Trivy JSON Report: located in CI**



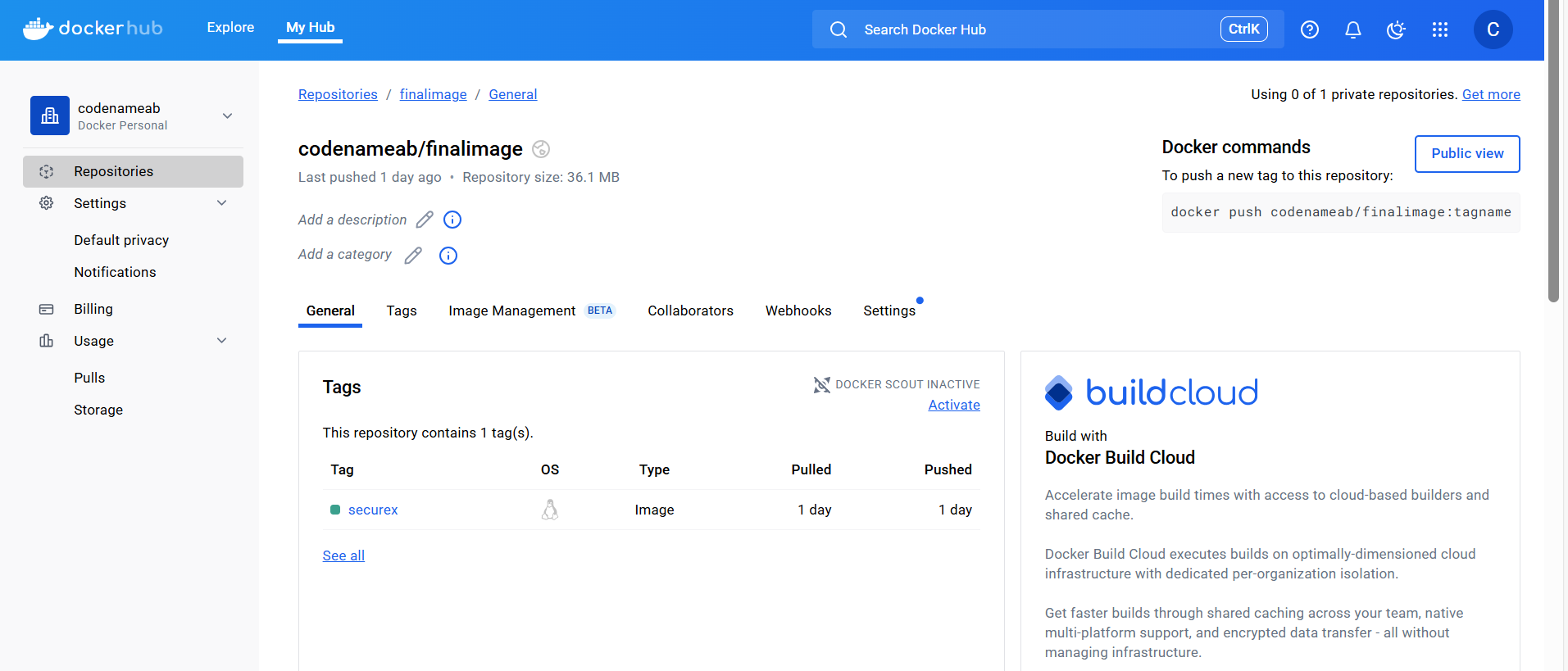
* 1. **Bandit Report:** [**Bandit Report**](https://output.circle-artifacts.com/output/job/5c872bbc-fa25-4ebb-ade3-230374ba77a2/artifacts/0/bandit-report)



A white background with black text

AI-generated content may be incorrect. **5.9 Checkov Report**: checkov-report/checkov-report.json

## **5.10 Docker:**



# **6. Conclusion**

This CircleCI-powered DevSecOps pipeline effectively shifted security left, reducing risks early in development. It established a secure-by-design culture, allowing the team to deploy software faster and more securely.

**References:**

[1] Snyk Ltd., “Snyk | Develop fast. Stay secure.,” *Snyk*, [Online]. Available: <https://snyk.io/>. [Accessed: 09-May-2025].

[2] SonarSource SA, “SonarQube - Static Code Analysis,” *SonarSource*, [Online]. Available: <https://www.sonarsource.com/products/sonarqube/>. [Accessed: 09-May-2025].

[3] Docker Inc., “Docker - Build, Share, and Run Applications,” *Docker*, [Online]. Available: <https://www.docker.com/>. [Accessed: 09-May-2025].

[4] OWASP Foundation, “OWASP Dependency-Check,” *OWASP*, [Online]. Available: <https://owasp.org/www-project-dependency-check/>. [Accessed: 09-May-2025].

[5] Aqua Security, “Trivy: Vulnerability Scanner for Containers and Other Artifacts,” *Trivy*, [Online]. Available: <https://trivy.dev/>. [Accessed: 09-May-2025].

[6] Bridgecrew, “Checkov: Infrastructure as Code Static Analysis,” *Checkov by Bridgecrew*, [Online]. Available: <https://www.checkov.io/>. [Accessed: 09-May-2025].

[7] Circle Internet Services, Inc., “CircleCI: Continuous Integration and Delivery,” *CircleCI*, [Online]. Available: <https://circleci.com/>. [Accessed: 09-May-2025].

[8] Damm, B., and Stampar, B., “sqlmap - Automatic SQL Injection and Database Takeover Tool,” *sqlmap.org*, [Online]. Available: <https://sqlmap.org/>. [Accessed: 09-May-2025].

[9] Datadog, Inc., “Datadog: Cloud Monitoring as a Service,” *Datadog*, [Online]. Available: <https://www.datadoghq.com/>. [Accessed: 09-May-2025].

[10] OWASP Foundation, “ZAP - Zed Attack Proxy,” *ZAP Proxy*, [Online]. Available: <https://www.zaproxy.org/>. [Accessed: 09-May-2025].