DevSecOps Intern Guide

How to Deploy a Service Safely

Purpose

This guide helps new DevSecOps interns understand how to deploy backend services safely, securely, and reliably, focusing on security awareness and operational discipline.

Secure Deployment Flow

Developer -> Git Commit -> CI Pipeline (Build, Test, Security Checks) -> Artifact Validation -> Staging Deployment -> Sanity Tests -> Production -> Monitoring

Core Principles

- Principle of Least Privilege

- Secure Secrets Management

- Environment Isolation

Common Mistakes

- Running services as root

- Hardcoding secrets

- No rollback strategy

- No monitoring or alerts

CI/CD Best Practices

- Automated testing

- Dependency and security scanning

- Least-privilege tokens

- Environment-based deployments

OWASP Top 10 Relevance

CI/CD pipelines are attack surfaces. Key risks include security misconfiguration, vulnerable dependencies, and sensitive data exposure.

Observability

Use logs for errors, metrics for trends, and system stats for infrastructure health.

Testing Strategy

Functional testing ensures correctness.

Load testing ensures scalability and reliability.

Release Checklist

Pre-release: scans, tests, non-root services.

Post-release: monitoring, alerts, rollback readiness.