Session I

The following topics are covered in Session I

- Introduction to DevOps
- Need of DevOps
- Continuous Integration and Continuous Delivery
- DevOps stages
    - Plan
    - Code
    - Build
    - Test
    - Deployment
    - Monitoring
- CI/CD Platforms
- DevOps Pipeline examples
- Pipeline as Code

2:56:31

List of labs covered during the session (and homework):

- Django WebApp (https://attackdefense.com/challengedetails?cid=2039)
- Git: Learn Basics with Git CLI (https://attackdefense.com/challengedetails?cid=2022)
- Git: Learn Basics with Git Cola (https://attackdefense.com/challengedetails?cid=2035)
- Build: Java Webapp (https://attackdefense.com/challengedetails?cid=2037)
- Build: Django Webapp (https://attackdefense.com/challengedetails?cid=2036)
- Build: Nginx Software (https://attackdefense.com/challengedetails?cid=2038)
- Test: Pytes (https://attackdefense.com/challengedetails?cid=2260)
- Test: JUnit (https://attackdefense.com/challengedetails?cid=2259)
- Selenium: Basic Automation with Plugin (https://attackdefense.com/challengedetails?cid=2342)
- Selenium: Scripting Interaction (https://attackdefense.com/challengedetails?cid=2343)
- Selenium: Scripting Dictionary Attacks (https://attackdefense.com/challengedetails?cid=2344)
- Ansible: Deploying Apache and MySQL (https://attackdefense.com/challengedetails?cid=2042)
- Ansible: Deploying Tomcat (https://attackdefense.com/challengedetails?cid=2043)
- Jenkins: Java Webapp (https://attackdefense.com/challengedetails?cid=2040)
- Jenkins: Django Webapp (https://attackdefense.com/challengedetails?cid=2039)
- Jenkins: Nginx Software (https://attackdefense.com/challengedetails?cid=2041)
- DevOps Pipeline: Java WebApp (https://attackdefense.com/challengedetails?cid=2064)
- DevOps Pipeline: Nginx (https://attackdefense.com/challengedetails?cid=2070)
- DevOps Pipeline as Code: Java WebApp (https://attackdefense.com/challengedetails?cid=2065)
- DevOps Pipeline as Code: Django WebApp (https://attackdefense.com/challengedetails?cid=2068)

Session II

The following topics are covered in Session II

- Introduction to DevSecOps

        - Threat Modelling
        - Automated Code Review
        - Sensitive information Scan
        - Static Application Security Testing
        - Dynamic Application Security Testing
- DevSecOps Pipelines
- DevSecOps Pipeline as Code
- Fix the Code Pipeline labs

2:30:39

List of labs covered during the session (and homework):

- PMD: Finding Common Vulnerabilities (https://attackdefense.com/challengedetails?cid=2049)
- DevSkim: Code Security Review (https://attackdefense.com/challengedetails?cid=2048)
- FindSecBugs: Securing Java Applications (https://attackdefense.com/challengedetails?cid=2050)
- TruffleHog: Locating Sensitive Information (https://attackdefense.com/challengedetails?cid=2044)
- GitSecrets: Finding Hardcoded Credentials (https://attackdefense.com/challengedetails?cid=2047)
- Talisman: Pre-Commit Code Scanning (https://attackdefense.com/challengedetails?cid=2046)
- Pre-commit: Scanning source code for Sensitive Information (https://attackdefense.com/challengedetails?cid=2266)
- Flawfinder: Statically Scanning C code (https://attackdefense.com/challengedetails?cid=2045)
- Graudit: Hunting Sensitive Information (https://attackdefense.com/challengedetails?cid=2051)
- Bandit: Scanning Python Code for Issues (https://attackdefense.com/challengedetails?cid=2053)
- Spotbugs: Finding Bugs in Java Code (https://attackdefense.com/challengedetails?cid=2054)
- SonarQube: Continuous Code Quality Monitoring (https://attackdefense.com/challengedetails?cid=2052)
- OWASP ZAP: Detecting Vulnerabilities in WebApps (https://attackdefense.com/challengedetails?cid=2055)
- BDD Security: Behaviour Driven Development (https://attackdefense.com/challengedetails?cid=2063)
- Arachini: Automated Vulnerability Scanning (https://attackdefense.com/challengedetails?cid=2056)
- Nikto: Automatic WebApp Scanning (https://attackdefense.com/challengedetails?cid=2057)
- Radamsa: Automated Fuzzing (https://attackdefense.com/challengedetails?cid=2058)
- FuzzDB: Fault Injection Testing (https://attackdefense.com/challengedetails?cid=2059)
- DevSecOps Pipeline: Java Webapp (https://attackdefense.com/challengedetails?cid=2066)
- DevSecOps Pipeline as Code: Django WebApp (https://attackdefense.com/challengedetails?cid=2069)
- DevOps Pipeline as Code: Java WebApp (https://attackdefense.com/challengedetails?cid=2065)
- DevSecOps Pipeline: Nginx Software (https://attackdefense.com/challengedetails?cid=2261)
- Fix the App: Django WebApp (https://attackdefense.com/challengedetails?cid=2174)
- Fix the App: Django WebApp II (https://attackdefense.com/challengedetails?cid=2273)
- Fix the App: Java WebApp (https://attackdefense.com/challengedetails?cid=353)

Session III

The following topics are covered in Session III

- DevSecOps stages
    - Source Component Analysis

- GitHub Actions
- Pipeline using GitHub Actions
- Integrating Security into Pipeline

2:40:56

List of labs covered during the session (and homework):

- OSSAudit: Auditing Python Packages (https://attackdefense.com/challengedetails?cid=2060)
- OWASP Dependency-Check (https://attackdefense.com/challengedetails?cid=2062)
- Inspec: Automating Compliance Checks (https://attackdefense.com/challengedetails?cid=2071)
- ServerSpec: Automating Configuration Tests (https://attackdefense.com/challengedetails?cid=2072)
- Dockerfile Linter (https://attackdefense.com/challengedetails?cid=2161)
- Dockerfilelint (https://attackdefense.com/challengedetails?cid=2161)
- Dockerlint (https://attackdefense.com/challengedetails?cid=2163)
- Hadolint (https://attackdefense.com/challengedetails?cid=2164)
- Docker Bench Security (https://attackdefense.com/challengedetails?cid=1607)
- Dockscan (https://attackdefense.com/challengedetails?cid=1608)
- Amicontained (https://attackdefense.com/challengedetails?cid=1609)
- Clair (https://attackdefense.com/challengedetails?cid=1620)
- Hashicorp Vault: Basics (https://attackdefense.com/challengedetails?cid=2358)
- Vault: Interacting with Python (https://attackdefense.com/challengedetails?cid=2359)
- Vault: OTP Based SSH Access (https://attackdefense.com/challengedetails?cid=2360)
- Archery: Vulnerability Management Framework (https://attackdefense.com/challengedetails?cid=2256)
- Defect Dojo: Managing Vulnerabilities (https://attackdefense.com/challengedetails?cid=2272)

Example Code Repos:

- Template repo: https://github.com/reachnishant/demorepo
- GitHub Actions Example I: https://github.com/reachnishant/test1
- GitHub Actions Example II:https://github.com/reachnishant/test2

Session IV

The following topics are covered in Session IV

- GitLab CI/CD Basics
- Components
- GitLab Runners
- Secret Management
- Implementing Pipeline using GitLab CI
- Integrating security tools

2:09:33

Example Code Repos:

- Template repo: https://gitlab.com/reachnishantsharma/demorepo
- GitLab CI/CD Example I: https://gitlab.com/reachnishantsharma/test-1
- GitLab CI/CD Example II:https://gitlab.com/reachnishantsharma/test-2
- GitLab CI/CD Example III:https://gitlab.com/reachnishantsharma/test-3