OWASP DEPENDENCY-CHECK TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to OWASP Dependency-Check

- What is OWASP Dependency-Check (ODC)
- Role of SCA (Software Composition Analysis) in application security
- Common supply-chain attacks and vulnerable libraries
- Where Dependency-Check fits in DevSecOps

How Dependency-Check Works Internally

- CVE, NVD, CPE, and vulnerability data sources
- Dependency identification techniques
- False positives and confidence scoring
- Limitations and assumptions of ODC

Installing & Configuring Dependency-Check

- CLI installation and setup

- Updating the NVD database
- Configuration files and command-line options
- Proxy, offline, and enterprise configurations

Scanning Different Project Types

- Java (Maven, Gradle) projects
- JavaScript / Node.js projects
- Python, .NET, and other ecosystems
- Handling multi-module applications

Running Scans & Understanding Reports

- Scan execution modes
- Report formats: HTML, JSON, XML, SARIF
- CVSS scores and severity interpretation
- Hands-on: Run a scan and analyze results

DAY 2

Reducing False Positives & Improving Accuracy

- Dependency suppression files
- Evidence confidence tuning
- Known issues and exclusions
- Best practices for clean reports

Policy Enforcement & Build Failures

- Defining severity thresholds
- Failing builds on critical vulnerabilities
- Managing technical debt

- Risk-based vulnerability acceptance

Integrating Dependency-Check into CI/CD Pipelines

- Jenkins integration
- GitHub Actions / GitLab CI
- Azure DevOps pipelines
- Shift-left security workflows

Dependency-Check with Containers & Microservices

- Scanning container builds
- Monorepos and microservices architectures
- Pipeline optimization strategies
- Performance considerations

Reporting, Compliance & Audits

- Using reports for audits and compliance
- Mapping results to OWASP Top 10
- Evidence for ISO, SOC 2, PCI DSS
- Vulnerability tracking and remediation workflow

Dependency-Check vs Other SCA Tools

- Comparison with Snyk, Black Duck, Trivy, Grype
- Strengths and limitations of Dependency-Check
- When to combine tools
- Open-source vs commercial trade-offs

Real-World Implementation & Best Practices

- Enterprise adoption strategy

- Common pitfalls and solutions
- Scaling Dependency-Check across teams
- Roadmap and future considerations