OWASP TESTING GUIDE TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to OWASP Testing Guide

- Overview of OWASP Testing Guide (OTG) and its objectives
- Importance of structured web application security testing
- OWASP Top 10 vulnerabilities and testing relevance
- Security testing lifecycle and roles of testers

Information Gathering & Reconnaissance

- Understanding the target application and environment
- Passive and active information gathering techniques
- Footprinting, enumeration, and asset identification
- Hands-on exercises on reconnaissance

Configuration & Deployment Management Testing

- Testing for insecure configurations and misconfigurations

- Analyzing server, framework, and database setups
- Security headers, SSL/TLS validation, and deployment checks
- Practical exercises on misconfiguration detection

Identity Management & Authentication Testing

- Verifying authentication mechanisms and workflows
- Testing password policies, multi-factor authentication, and session management
- Identifying weaknesses in login flows and account recovery
- Hands-on testing scenarios

Session Management Testing

- Testing session token generation and management
- Session fixation, hijacking, and expiration checks
- Secure cookie and token handling
- Practical exercises and OWASP testing examples

Access Control & Authorization Testing

- Testing horizontal and vertical access controls
- Exploiting insecure direct object references (IDOR)
- Role-based access verification
- Hands-on access control testing

Wrap-Up & Q&A

- Summary of key concepts covered
- Q&A session with interactive discussion
- Lab exercises review

DAY 2

Input Validation & Injection Testing

- Testing for SQL, NoSQL, OS command, and LDAP injection
- Input validation weaknesses and attack simulation
- Secure coding implications for testing
- Hands-on injection exercises

Cross-Site Scripting (XSS) & Cross-Site Request Forgery (CSRF)

- Detecting and testing for XSS vulnerabilities
- Testing CSRF protections and token mechanisms
- Practical examples and lab exercises

Security Misconfigurations & Sensitive Data Exposure

- Identifying insecure storage, logging, and transport issues
- Testing encryption and TLS configurations
- Protecting sensitive information in transit and at rest
- Hands-on lab exercises

Business Logic & Application-Specific Vulnerabilities

- Testing business logic flaws in workflows and transactions
- Identifying race conditions, bypasses, and misuse scenarios
- Practical exercises and scenario-based testing

API & Web Services Security Testing

- Testing REST and SOAP APIs for common vulnerabilities

- Input validation, authentication, and authorization checks
- Hands-on API testing exercises using OWASP Testing Guide

Reporting, Metrics & Best Practices

- Documenting test findings and creating actionable reports
- Risk rating, prioritization, and remediation recommendations
- Best practices for structured security testing
- Mapping findings to OWASP Testing Guide controls

Final Review & Knowledge Assessment

- Recap of all testing modules
- Scenario-based knowledge check
- Hands-on lab review and Q&A
- Practical tips for applying OWASP Testing Guide in real projects