# OWASP ZAP (ZED ATTACK PROXY) TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

## TRAINING AGENDA

## DAY 1

### Introduction to OWASP ZAP

- Overview of OWASP ZAP and its role in application security testing
- ZAP architecture and core components
- Use cases: developers, QA, AppSec, DevSecOps
- Comparison with other DAST tools

### Installing & Configuring OWASP ZAP

- Installation options (Windows, Linux, macOS, Docker)
- ZAP user interface overview
- Configuring browser proxy settings
- Understanding ZAP modes: Safe, Protected, and Standard

### Exploring Web Applications with ZAP

- Intercepting HTTP/HTTPS traffic

- Understanding requests, responses, and headers
- Using the Sites Tree and History tab
- Hands-on lab: browsing an application through ZAP

### Manual Testing & Passive Scanning

- Passive scanning concepts
- Identifying common vulnerabilities automatically
- Reviewing alerts and risk levels
- Hands-on lab: analyzing passive scan results

### Active Scanning Fundamentals

- Active scanning concepts and rules
- Scope definition and target selection
- Running active scans safely
- Interpreting active scan alerts

### Review & Q&A

- Summary of ZAP core features
- Review of hands-on exercises
- Q&A session

## DAY 2

### Spidering & Crawling Applications

- Traditional spider vs AJAX spider
- Crawling modern web applications

- Hands-on lab: mapping application attack surface

## Authentication & Session Handling in ZAP

- Handling login-based applications
- Configuring authentication in ZAP
- Managing sessions and tokens
- Testing authenticated areas

## ZAP Add-ons, Scripts & Automation

- Overview of ZAP add-ons
- Using scripts for custom testing
- Introduction to ZAP scripting languages
- Hands-on: creating simple scripts

## API Security Testing with ZAP

- Testing REST APIs using OpenAPI / Swagger definitions
- Importing API specifications into ZAP
- Common API vulnerabilities and detection
- Hands-on lab: API scanning

## CI/CD & DevSecOps Integration

- Automating ZAP scans in CI/CD pipelines
- ZAP baseline, full scan, and API scan modes
- Generating reports for DevSecOps
- Fail builds based on security thresholds

## Reporting, Risk Analysis & Best Practices

- Understanding ZAP reports and alert categories
- Prioritizing findings and reducing false positives
- Secure testing best practices
- ZAP limitations and safe usage guidelines

## Final Hands-On Lab & Assessment

- End-to-end security testing of a sample application
- Combining passive, active, and API scans
- Review findings and remediation guidance
- Final Q&A and course wrap-up