Faysal Aziz

ZAP DAST

Automating Security Testing in Modern CI/CD Pipelines in a day

FA-0459

Software Development · DevOps, Cloud & Infrastructure · Cybersecurity · Automation, RPA & Power Platform

---

Introduction

Security threats evolve as fast as software development itself. That's why OWASP ZAP (ZAP by Checkmarx) has become the go-to open-source security testing tool for developers who want to catch vulnerabilities in their web apps and APIs before attackers do.

Join us for an intensive, hands-on day learning how to harness ZAP's power. You'll master practical techniques for API testing, seamlessly integrate ZAP into your CI/CD pipelines with Jenkins and GitHub Actions, and learn to generate clear, actionable security reports.

Led by an industry veteran with three decades of experience, this workshop goes beyond theory to equip you with real-world security testing skills you can apply immediately. Whether you're new to application security or looking to level up your DevSecOps practices, you'll walk away ready to make security an integral part of your development workflow.

Learning outcomes

By the end of the course, participants will:

- Understand the core capabilities of OWASP ZAP for dynamic application security testing (DAST).
- Learn how to set up and use ZAP for automated security testing in CI/CD pipelines.
- Perform API security testing using ZAP and interpret scan results.
- Integrate ZAP with popular DevOps tools like Jenkins and GitHub Actions.
- Generate comprehensive reports for various stakeholders.
- Gain a foundational understanding of ZAP’s advanced features like scripting and extensions.

Prerequisites

- Familiarity with web application architecture (HTTP, APIs, etc.).
- Basic understanding of software development processes and CI/CD pipelines.
- Experience with version control systems like Git and tools like Jenkins or GitHub Actions (optional but helpful).
- A laptop with admin rights for installing ZAP and other tools.

Training outline

1. 1. Introduction to OWASP ZAP

- Overview of OWASP ZAP and its role in application security.
- Key differences between DAST, SAST, and other security testing methods.
- Installing and setting up ZAP.

  Understanding the ZAP interface:

  - Sites tree
  - Alerts tab
  - Scripts tab
  - Session management

2. 2. Setting Up and Configuring ZAP for Your Workflow

- Configuring ZAP for different environments (development, staging, production).
- Proxy setup and browser integration.
- Introduction to ZAP modes (Safe, Protected, Standard, Attack).
- Setting up contexts, authentication, and session management.

3. 3. Automated and Manual Security Testing with ZAP

Performing manual security testing:

- Identifying common vulnerabilities (SQL Injection, XSS, etc.).
- Using ZAP's spidering and active scan capabilities.

Automating scans:

- Setting scan policies for different use cases.
- Running automated scans with pre-defined configurations.

4. 4. API Security Testing

- Understanding the importance of API security in modern applications.
- Importing and testing OpenAPI/Swagger specifications in ZAP.
- Setting up and testing REST and SOAP APIs.
- Handling authentication and session tokens for API testing.
- Interpreting and analyzing API test results.

5. 5. Integrating ZAP into CI/CD Pipelines

- Why CI/CD integration is essential for DevSecOps.

  Integrating ZAP with:

  Jenkins:

  - Installing and configuring the ZAP plugin.
  - Automating scans as part of the build process.
  - Configuring post-build actions for security analysis.

  GitHub Actions:

  - Setting up ZAP in GitHub workflows.
  - Writing custom GitHub Actions for ZAP scans.
  - Configuring alerts and notifications for failed security checks.
- Leveraging Docker containers for ZAP integration.

6. 6. Custom Request from Client

- Conducting automated authenticated ZAP scans on applications that use Single Sign-On (SSO), OAuth, or complex authentication methods (like 2FA).
- Utilizing ZAP spidering and other scanning features through automation plans.
- Implementing automated ZAP scans on APIs by adjusting parameters or the request body to improve scanning efficiency.
- Measuring the scan coverage between ZAP manual scans and ZAP automated scans.

7. 7. Reporting and Analysis

- Understanding ZAP's reporting capabilities.
- Generating reports in different formats (HTML, XML, JSON).
- Customizing reports for technical teams and business stakeholders.
- Automating report generation and delivery in CI/CD pipelines.

This course offers a practical, hands-on approach tailored to modern development workflows. Participants will gain not just theoretical knowledge but actionable skills to integrate ZAP seamlessly into their DevSecOps practices.

© 2026 Faysal Aziz · Kuala Lumpur