DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

OWASP ZAP Advanced Training

Scan complex modern applications at scale, extend ZAP with custom rules and run a governed DAST programme across teams.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **5 days · Days 1-5**	SELF-PACED VIDEO **1-year LMS access**
BATCH SIZE **Max 10 learners**	NEXT BATCHES **1st of every month · weekends: first Saturday**	CERTIFICATE **Verifiable certificate of completion**

Foundation	Essential	Intermediate	Advanced
1 day · Included	2 days · Included	3 days · Included	5 days · This curriculum

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	47 topics · Foundation to Advanced
Hands-on labs	4 labs
Formats and fees	Live, 1:1, self-paced, corporate
Trainer and reviews	Rajesh Kumar
Enrolment	Batches, payment, contacts

WHY DEVOPSSCHOOL

- Rated 4.6 on Google
- 1,500+ verifiable certificates issued in the public registry
- Trainer Rajesh Kumar: 20 years in industry
- Small batches: max 10 learners, every session recorded

Course page: www.devopsschool.com/courses/zap/zap-and-advance-training.html
Talk to us: WhatsApp +91 99057 40781 · +1 (469) 756-6329 · contact@DevOpsSchool.com · reply within 1 hour

OUTCOMES

What you will achieve

By the end of the OWASP ZAP course path, you will be able to:

1

Find web vulnerabilities

Use ZAP's proxy, spiders, passive and active scans and manual tools to find and confirm vulnerabilities.

2

Automate security testing

Run authenticated web and API scans automatically in CI/CD with clear quality gates.

3

Run a DAST programme

Scale, govern and report dynamic testing across many applications and teams.

WHAT THE ADVANCED LEVEL ADDS

Complex authentication, scale and DAST programme governance

Hands-on: Capstone: run a DAST programme. Scan three applications with tailored Automation Framework plans in containers, triage results in a tracker and present a remediation and metrics report.

WHO SHOULD ATTEND

- Experienced OWASP ZAP practitioners responsible for quality, security and scale.
- Senior engineers, architects and leads who design and troubleshoot OWASP ZAP solutions.
- Teams making OWASP ZAP an organisation-wide standard.

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Automate ZAP with the Automation Framework, scan APIs and run baseline and full scans as quality gates in CI/CD pipelines.
- Basic computer skills and a laptop with a stable internet connection for the live sessions and labs.
- This curriculum includes every earlier level, so it is complete on its own.

AGENDA · FOUNDATION TO ADVANCED

OWASP ZAP Advanced Training agenda

47 topics. Each level builds on the one before it, so this curriculum lists every earlier level in full. Days are for corporate (day-wise) delivery; live online batches cover the same agenda in max 8-10 hours.

DAY 1 — Foundation: DAST concepts, ZAP installation and first scan

Included from Foundation

1. Dynamic application security testing: how DAST differs from SAST and SCA and where it fits in the SDLC
2. ZAP overview: the open source web app scanner, its history from OWASP and current stewardship
3. Rules of engagement: scanning only authorised targets and using safe test applications such as OWASP Juice Shop
4. Installation: desktop installers for Windows, macOS and Linux, Java requirements and Docker images
5. Desktop UI tour: sites tree, history, alerts, output tabs and the request and response panes
6. Intercepting proxy: local proxy settings, the ZAP root CA certificate and launching a proxied browser
7. Manual explore: browsing an application through ZAP to populate the sites tree
8. Automated scan: Quick Start against a URL and what happens during the scan
9. Alerts: risk and confidence levels, evidence, CWE and WASC references and solutions
10. Common findings: missing security headers, cookie flags, XSS and SQL injection indicators
11. First report: generating an HTML report and reading it with developers

DAY 2 — Essential: Spidering, scan policies, authentication and manual testing

Included from Essential

12. Contexts and scope: defining in-scope URLs, technologies and excluding risky paths
13. ZAP modes: safe, protected, standard and attack modes and when to use each
14. Traditional spider: crawl settings, depth, parameters and limits
15. AJAX and client spiders: crawling JavaScript-heavy single page applications with a browser
16. Passive scanning: passive scan rules, tags and what they detect without attacking
17. Active scanning: scan policies, attack strength, alert threshold and technology filters
18. Authentication: form-based, JSON-based and browser-based authentication with verification strategies
19. Users and sessions: session management methods, tokens, cookies and logged-in indicators
20. Manual request editor and resend: crafting and replaying requests
21. Breakpoints: intercepting and modifying requests and responses on the fly
22. Fuzzer: payload lists, processors and spotting anomalies in responses
23. False positives: alert filters, marking findings and keeping scan results trustworthy

DAY 3 — Intermediate: Automation, APIs and CI/CD integration

Included from Intermediate

24. Automation Framework: YAML plans, jobs, environments and running plans from the command line
25. Packaged scans: baseline, full and API scans in Docker and their configuration files
26. API scanning: importing OpenAPI, GraphQL and SOAP definitions and scanning endpoints
27. Daemon mode and the ZAP API: API keys, endpoints and controlling scans remotely
28. Client libraries: driving ZAP from Python and Java scripts
29. GitHub Actions: baseline, full scan and API scan actions with rules files
30. GitLab CI and Jenkins: running ZAP stages and failing builds on new high-risk alerts

31. Scripting: authentication, HTTP sender and active rule scripts in JavaScript and Zest
32. Add-ons: the marketplace, alpha, beta and release status and keeping add-ons updated
33. Reports: modern HTML, JSON, XML and SARIF reports for tools and dashboards
34. Vulnerability management: importing results into DefectDojo and tracking fixes
35. Tuning: scan duration, threads, rule selection and handling unstable targets

DAYS 4-5 **Advanced: Complex authentication, scale and DAST programme governance** **New at this level**

36. Complex authentication: OAuth 2.0 and OIDC flows, token refresh scripts and multi-step logins
37. Modern apps: single page applications, WebSockets, gRPC limitations and API gateways
38. Custom scan rules: writing passive and active rules for application-specific risks
39. Extending ZAP: building add-ons and sharing scripts and plans across teams
40. Scaling scans: parallel containers, Kubernetes jobs and scheduling large scan estates
41. Environment strategy: ephemeral test environments, test data and avoiding production impact
42. Combining tools: correlating DAST with SAST, SCA and penetration testing results
43. Risk-based policies: scan depth by application tier and release cadence
44. Triage workflow: severity mapping to OWASP Top 10, ownership, SLAs and exceptions
45. Metrics: coverage, time to remediate, recurring issues and programme reporting
46. Compliance evidence: using DAST results for PCI DSS, ISO 27001 and customer audits
47. Capstone: a DAST programme with automated scans, triage and reporting for several applications

PRACTICE

Hands-on labs

You build these yourself during the course, guided by the trainer.

FOUNDATION **Run a first scan on Juice Shop**
Run OWASP Juice Shop in Docker, explore it through the ZAP proxy, run an automated scan and produce an HTML report of the findings.

ESSENTIAL **Run an authenticated scan of an app**
Create a context with browser-based authentication for a test application, spider it with the AJAX spider and run an active scan as a logged-in user.

INTERMEDIATE **Gate a pipeline with ZAP scans**
Add a ZAP baseline scan and an OpenAPI scan to a CI pipeline using an Automation Framework plan, publish reports and fail the build on new high alerts.

ADVANCED **Capstone: run a DAST programme**
Scan three applications with tailored Automation Framework plans in containers, triage results in a tracker and present a remediation and metrics report.

HOW YOU CAN LEARN

Formats and fees

The same agenda in four formats. Fees are in Indian rupees as of November 2026; the course page shows them in your currency.

FORMAT	DURATION	WHAT YOU GET	FEE
Live & interactive (online)	Max 8-10 hours	Instructor-led public batch of max 10 learners with demos, labs, Q&A and assignment review. Weekday batches start on the 1st of every month, weekend batches on the first Saturday of every month.	**INR 34,999**
1:1 live training (online)	Max 8-10 hours, one-to-one	The same agenda, taught one-to-one by the trainer. Starts immediately, without waiting for the next batch; sessions planned around your working hours, at your pace.	**INR 99,999**
Self-paced video	1-year LMS access	All four OWASP ZAP levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	5 days for this level	A private batch for your team, on demand. Foundation 1 day, Essential 2, Intermediate 3, Advanced 5 (cumulative).	**Quote on request**

ASSESSMENT AND CERTIFICATE

Your progress is checked through hands-on labs and assignments at every level. On completion you receive a DevOpsSchool certificate of completion with a unique credential ID that anyone can verify at devopsschool.com/certificates.

INCLUDED WITH EVERY LIVE BATCH

- Every live session is recorded and stays in your LMS for a year.
- Can't attend your batch? Move to next month's batch.
- Free demo class before you pay.
- Free 10-15 minute call with an advisor or the trainer to check the course fits you.

YOUR TRAINER

Learn from Rajesh Kumar

Principal Architect, trainer and mentor in DevOps, SRE, DevSecOps and platform engineering, with 20 years across 8+ software MNCs, including Staff DevOps/SRE Engineer for a leading Japanese mobile-payment platform and Principal DevOps Architect and Manager in Europe.

Profile: www.rajeshkumar.xyz · Videos: youtube.com/@TheDevOpsSchool

20 years in industry	**200+** corporate trainings
10,000+ engineers mentored	**70+** organisations coached

REVIEWS

What learners say

Rated 4.6 on Google · more reviews at devopsschool.com/testimonials and in our video testimonials.

> “Rajesh is very good trainer. Rajesh was able to resolve our queries and question effectively. We really liked the hands-on examples covered during this training program.”
>
> Indrayani, India

> “The training was very useful and interactive. Rajesh helped develop the confidence of all.”
>
> Abhinav Gupta, Pune

START YOUR OWASP ZAP TRAINING

Join the next batch

Weekday batches start on the 1st of every month and weekend batches on the first Saturday of every month, with max 10 learners each. 1:1 training can start immediately; corporate batches run on demand. We reply within 1 hour.

Pay by UPI, credit and debit cards, net banking or PayPal. Before you pay, read our refund policy. All levels of this course: www.devopsschool.com/courses/zap/

ENROL OR RESERVE A SEAT
OWASP ZAP Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com