DevOpsSchool

Course curriculum · November 2026

LEVEL 03 OF 04 · INTERMEDIATE

Owasp Intermediate Training

Verify applications against ASVS, secure APIs using the API Security Top 10 and automate OWASP tools in CI/CD pipelines.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **3 days · Days 1-3**	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 · This curriculum	5 days · Next step

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	35 topics · Foundation to Intermediate
Hands-on labs	3 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/owasp/owasp-intermediate-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 course path, you will be able to:

1

Recognise web application risks

Identify, exploit in a lab and explain the OWASP Top 10 and API Top 10 risks.

2

Build secure software

Apply ASVS, Cheat Sheets and OWASP tools to design, code and test secure applications.

3

Run application security

Use SAMM to measure and improve application security across an organisation.

WHAT THE INTERMEDIATE LEVEL ADDS

ASVS, API security, DevSecOps automation

Hands-on: Build a DevSecOps pipeline with OWASP tools. Add ZAP, Dependency-Check and SBOM generation to a CI pipeline for a vulnerable API, fail the build on high risks and fix them.

WHO SHOULD ATTEND

- Regular Owasp users who want to automate, integrate and manage it at a deeper level.
- Specialists who support Owasp for colleagues or customers.
- Leads preparing Owasp for wider use across projects.

BEFORE YOU START

- The Essential level, or equivalent hands-on experience.
- You can already: Exploit and fix each Top 10 risk in a lab, test applications with ZAP and apply OWASP Cheat Sheets to secure your code.
- 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 INTERMEDIATE

Owasp Intermediate Training agenda

35 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: OWASP projects, Top 10 risks and secure basics

Included from Foundation

1. OWASP overview: the open community, flagship projects and how to use them in a security programme
2. Web application basics: HTTP requests and responses, cookies, sessions, headers and same-origin policy
3. OWASP Top 10 introduction: how the list is built and the 2021 and 2025 editions compared
4. Broken access control: IDOR, missing function-level checks and path traversal
5. Injection: SQL injection, command injection and cross-site scripting (XSS) basics
6. Cryptographic failures: plaintext data, weak algorithms and missing TLS
7. Security misconfiguration: default credentials, verbose errors and missing security headers
8. Software supply chain failures: vulnerable and unmaintained components and untrusted packages
9. Authentication failures: weak passwords, credential stuffing and session fixation
10. Practice lab setup: OWASP Juice Shop and WebGoat running locally in Docker
11. Tooling intro: browser developer tools and ZAP as an intercepting proxy

DAY 2 — Essential: Top 10 in depth, testing and secure coding

Included from Essential

12. Insecure design: threat modelling basics with STRIDE and OWASP Threat Dragon
13. Software and data integrity failures: insecure deserialization, unsigned updates and CI/CD integrity
14. Logging and alerting failures: what to log, log injection and detecting attacks
15. Server-side request forgery and exceptional conditions: SSRF, unsafe error handling and fail-open logic
16. Fixing injection: parameterised queries, ORM pitfalls, output encoding and Content Security Policy
17. Fixing access control: deny by default, server-side authorization and object ownership checks
18. Authentication done right: MFA, password storage with Argon2 or bcrypt and session management
19. OWASP Cheat Sheet Series: applying cheat sheets for authentication, XSS prevention and secrets
20. ZAP in practice: spidering, passive and active scans, authenticated scanning and reports
21. Dependency checks: OWASP Dependency-Check and CycloneDX SBOMs for component risk
22. OWASP Proactive Controls: the developer-focused top controls mapped to code
23. Team workflow: security user stories, code review checklists and triaging scan findings

DAY 3 — Intermediate: ASVS, API security, DevSecOps automation

New at this level

24. OWASP ASVS: verification levels 1 to 3, chapters and using ASVS as security requirements
25. OWASP API Security Top 10: broken object level authorization, mass assignment and resource consumption
26. API testing: testing REST and GraphQL APIs with ZAP and OpenAPI definitions
27. JWT and OAuth security: token validation, algorithm confusion, scopes and token storage
28. DevSecOps pipelines: ZAP baseline and full scans, Dependency-Check and SAST in CI
29. Dependency-Track: continuous component analysis from CycloneDX SBOMs
30. Web application firewall: ModSecurity or Coraza with the OWASP Core Rule Set and tuning false positives

31. Security headers and browser defences: CSP, HSTS, SameSite cookies and CORS configuration
32. Secrets management: avoiding hard-coded secrets and scanning repositories for leaks
33. Mobile security: OWASP MASVS and MASTG basics for Android and iOS apps
34. Security testing guide: OWASP Web Security Testing Guide (WSTG) methodology
35. Troubleshooting findings: false positives, risk rating and remediation guidance

PRACTICE

Hands-on labs

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

FOUNDATION

Find your first Top 10 flaws

Run OWASP Juice Shop locally and use the browser and ZAP to find and explain an access control flaw, an injection and a misconfiguration.

ESSENTIAL

Exploit and fix Top 10 issues

Exploit SQL injection, XSS and broken access control in WebGoat, then fix each in code and confirm the fix with a ZAP scan.

INTERMEDIATE

Build a DevSecOps pipeline with OWASP tools

Add ZAP, Dependency-Check and SBOM generation to a CI pipeline for a vulnerable API, fail the build on high risks and fix them.

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 levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	3 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 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/owasp/

ENROL OR RESERVE A SEAT **Owasp Intermediate Training**	WHATSAPP · INDIA **+91 99057 40781**
WHATSAPP · USA **+1 (469) 756-6329**	EMAIL **contact@DevOpsSchool.com**

Next step after this level: Owasp Advanced Training - Build an application security programme with OWASP SAMM, secure AI and LLM applications and govern AppSec across many teams.