DevOpsSchool

Course curriculum · November 2026

LEVEL 03 OF 04 · INTERMEDIATE

Skipfish Intermediate Training

Triage Skipfish findings, confirm real vulnerabilities manually and turn them into clear remediation tickets.

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	33 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/skipfish/skipfish-and-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 Skipfish course path, you will be able to:

1

Scan web applications safely

Run authorised Skipfish scans with the right scope, speed and authentication settings.

2

Turn findings into fixes

Validate results, remove false positives and give developers clear remediation steps.

3

Automate security testing

Combine Skipfish with modern scanners in repeatable CI-driven scanning workflows.

WHAT THE INTERMEDIATE LEVEL ADDS

Findings analysis, validation and remediation

Hands-on: Triage and validate scan findings. Classify the issues from a Juice Shop scan, confirm two real vulnerabilities by replaying requests in OWASP ZAP and write remediation tickets.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Essential level, or equivalent hands-on experience.
- You can already: Control Skipfish scope, speed and authentication so scans cover the right pages without harming the target.
- 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

Skipfish Intermediate Training agenda

33 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: Web scanning concepts and first Skipfish scan

Included from Foundation

1. Web application security basics: attack surface, HTTP requests and responses, cookies and sessions
2. What Skipfish is: an active web application reconnaissance scanner from Google, written in C
3. How Skipfish works: recursive crawling, dictionary-based probing and security checks on each response
4. Legal and ethical scanning: written authorisation, scope agreements and safe lab targets
5. Installation: Kali Linux package or building from source with libidn and OpenSSL dependencies
6. Project status: last upstream release 2.10b, what that means and why results need verification
7. Lab targets: OWASP Juice Shop, DVWA and bWAPP running in Docker containers
8. First scan: skipfish -o output_dir -W wordlist http://target and watching realtime statistics
9. Dictionaries: minimal.wl, medium.wl, complete.wl and extensions-only.wl and copying a working wordlist
10. Reading the report: index.html summary, issue types, risk levels and the crawled site map

DAY 2 — Essential: Scan control, scope and authentication

Included from Essential

11. Crawl scope options: -d depth, -c children per node, -x descendants per branch and -r total request limit
12. URL filtering: -I include, -X exclude, -K skip fuzzing named parameters and -D or -B for other domains
13. Safety switches: -O do not submit forms, -Z skip 5xx locations, -P do not parse new links
14. Performance settings: -g global connections, -m per-host connections, -l requests per second, -k scan duration
15. Timeouts and limits: -t request timeout, -w network I/O timeout, -i idle timeout and -s response size
16. HTTP authentication: -A user:pass for basic auth and custom headers with -H
17. Session cookies: -C name=value to reuse a logged-in session and -N to reject new cookies
18. Form authentication: --auth-form, --auth-user, --auth-pass and --auth-verify-url
19. Browser identity: -b to send MSIE, Firefox or iPhone style headers
20. Dictionary management: -W read-write wordlist, -S supplemental read-only list, -L and -Y learning controls
21. Reporting switches: -M mixed content warnings, -U external URLs and e-mails, -Q suppress duplicate nodes

DAY 3 — Intermediate: Findings analysis, validation and remediation

New at this level

22. Issue categories: high-risk findings such as SQL injection, XSS and shell injection versus medium and low risk
23. Information findings: directory listings, interesting files, server errors and MIME or charset mismatches
24. False positive triage: reproducing requests, checking responses and confirming impact
25. Manual validation: replaying requests with curl and Burp Suite Community or OWASP ZAP
26. Mapping to OWASP Top 10: injection, broken access control, security misconfiguration and more
27. Custom signatures: the signatures.conf format and adding checks for known content
28. Form auto-fill rules: -T name=value to drive deeper crawling through forms
29. Probabilistic crawling: -p crawl percentage and -q seed for repeatable partial scans
30. Configuration files: saving scan profiles with --config for repeatable runs

31. Comparing scans: re-scanning after fixes and tracking resolved and new issues
32. Remediation guidance: input validation, output encoding, parameterised queries and secure headers
33. Writing findings: evidence, risk rating, reproduction steps and fix recommendations

PRACTICE

Hands-on labs

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

FOUNDATION

First Skipfish scan in a lab

Run DVWA in Docker, install Skipfish and perform a first scan with a copied minimal dictionary, then walk through the generated HTML report.

ESSENTIAL

Authenticated, rate-limited scan

Scan the logged-in area of a lab application using session cookies, include and exclude rules and a request rate limit, then compare coverage with an anonymous scan.

INTERMEDIATE

Triage and validate scan findings

Classify the issues from a Juice Shop scan, confirm two real vulnerabilities by replaying requests in OWASP ZAP and write remediation tickets.

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 Skipfish 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 SKIPFISH 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/skipfish/

ENROL OR RESERVE A SEAT
Skipfish Intermediate Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com

Next step after this level: Skipfish Advanced Training - Combine Skipfish with modern scanners in automated pipelines and run a governed web scanning programme.