DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

Mobile Security Advanced Training

Run full mobile penetration tests, exploit weaknesses safely and harden apps and enterprise fleets against real attacks.

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	46 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/mobile/mobile-security-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 Mobile Security course path, you will be able to:

1

Understand mobile platform security

Explain Android and iOS security architecture and where real mobile apps go wrong.

2

Test mobile apps thoroughly

Perform static, dynamic and runtime testing of Android and iOS apps against OWASP MASVS.

3

Harden apps and fleets

Recommend and verify app hardening, secure backends and enterprise mobile controls.

WHAT THE ADVANCED LEVEL ADDS

Exploitation, app hardening and enterprise mobile security

Hands-on: Full mobile penetration test. Test an Android and iOS banking-style app end to end, exploit chained flaws, then verify the developer fixes and hardening.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Analyse and manipulate running mobile apps with Frida, objection and debuggers, bypass client-side controls and report findings.
- 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

Mobile Security Advanced Training agenda

46 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: Android and iOS security architecture, lab setup

Included from Foundation

1. Mobile threat landscape: OWASP Mobile Top 10 (2024), OWASP MASVS and the MASTG testing guide
2. Introduction to Android: Android security architecture, Linux kernel, app sandbox, SELinux, permissions and verified boot
3. Android application components: activities, services, broadcast receivers, content providers, intents and the manifest
4. What is ADB: connecting devices, installing apps, shell, logcat and pulling files
5. Setting up an Android pentesting environment: Genymotion or Android Studio emulator, a rooted test device and tools
6. Setting up a Burp proxy: device proxy settings and installing the Burp CA certificate
7. iOS application security basics: MVC and event-driven architecture and the ARM (arm64) processor
8. iOS security mechanisms: security architecture, secure boot chain and loading trusted applications with code signing
9. iOS isolation and protection: application isolation (sandbox), data encryption with data protection classes and Secure Enclave
10. iOS network security: App Transport Security and system TLS behaviour
11. First look at an app: APK and IPA structure, AndroidManifest.xml and Info.plist

DAY 2 — Essential: Static analysis, data storage and traffic testing

Included from Essential

12. Static analysis on Android: apktool, jadx and MobSF scans of an APK
13. Insecure data storage on Android: SharedPreferences, SQLite databases, external storage and logs
14. Testing exported components: activities, services, receivers and content providers with adb and drozer
15. WebView risks: JavaScript interfaces, file access and loading untrusted content
16. Network testing: intercepting HTTPS, network security configuration and certificate pinning concepts
17. Authentication and session flaws: token storage, session expiry and insecure API calls from apps
18. Jailbreaking: what it changes on iOS, current jailbreak options and rooting Android with Magisk
19. Creating an iOS pentest platform: Cydia or Sileo, logging into your jailbroken device over SSH and tools to install
20. iOS data storage: SQLite databases, plist files, NSUserDefaults and the Keychain
21. Class-dump-z and class-dump: extracting Objective-C class information from iOS binaries
22. Mapping findings to MASVS: storage, network, platform and authentication controls

DAY 3 — Intermediate: Runtime analysis, instrumentation and reverse engineering

Included from Intermediate

23. Runtime analysis concepts: hooking, method tracing and modifying app behaviour in memory
24. Runtime analysis with Cycript: inspecting live Objective-C objects and combining Cycript with class-dump-z
25. Lifecycle of an application: iOS app states and where sensitive data is exposed
26. Decrypting applications: App Store encryption, Clutch and modern tools such as frida-ios-dump
27. Runtime analysis with GDB and LLDB: breakpoints, registers and memory inspection

28. Dynamic instrumentation: Frida scripts and objection commands on Android and iOS
29. Certificate pinning bypass: Frida and objection techniques and what they reveal
30. Root and jailbreak detection bypass: why client-side checks are not enough
31. Reverse engineering native code: ARM binaries and shared libraries in Ghidra
32. Repackaging Android apps: smali editing, rebuilding and re-signing with apksigner
33. Secrets and cryptography flaws: hardcoded keys, weak algorithms and insecure random numbers
34. Deep links and universal links: hijacking risks and validation

DAYS 4-5 **Advanced: Exploitation, app hardening and enterprise mobile security** — New at this level

35. Exploiting iOS apps: chaining runtime and storage flaws into working attacks
36. Porting exploits to Metasploit: module structure and Android payloads with msfvenom
37. App hardening: R8 or ProGuard obfuscation, anti-tampering, anti-debugging and runtime protection
38. Platform attestation: Play Integrity API and Apple App Attest for genuine app and device checks
39. Secure mobile backends: OAuth 2.0 with PKCE, token binding and API rate limiting
40. Third-party SDK and supply chain risk: SDK inventory, Android data safety and iOS privacy manifests
41. Enterprise mobility: MDM and app protection policies with Microsoft Intune and BYOD controls
42. Mobile threat defence: detecting malicious apps, phishing and network attacks on devices
43. DevSecOps for mobile: SAST, DAST and SCA in mobile CI pipelines with MobSF
44. Compliance and privacy: GDPR, India's DPDP Act and PCI DSS considerations for mobile apps
45. Reporting: risk rating, reproducible evidence and developer-ready remediation guidance
46. Capstone: an end-to-end Android and iOS penetration test with exploitation and a remediation report

PRACTICE

Hands-on labs

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

FOUNDATION **Build your mobile testing lab**
Set up an Android emulator with ADB and Burp interception, install a deliberately vulnerable app and map its components and traffic.

ESSENTIAL **Data storage and traffic assessment**
Assess a vulnerable Android and iOS app for insecure storage, exported components and weak network security, and record MASVS-mapped findings.

INTERMEDIATE **Runtime manipulation of a mobile app**
Use Frida and objection to bypass pinning and jailbreak detection, decrypt an iOS app and extract secrets from native code.

ADVANCED **Full mobile penetration test**
Test an Android and iOS banking-style app end to end, exploit chained flaws, then verify the developer fixes and hardening.

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 Mobile Security 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 MOBILE SECURITY 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/mobile/

ENROL OR RESERVE A SEAT
Mobile Security Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com