Mobile Application Security and Penetration Testing Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The proliferation of mobile devices and the "mobile-first" approach across all industries have made Mobile Application Security a critical and high-demand domain. Mobile Application Security and Penetration Testing Training Course is designed to equip participants with the latest ethical hacking skills and methodologies to identify, exploit, and remediate vulnerabilities in modern Android and iOS applications. With advanced cyber threats like AI-driven malware, complex reverse engineering attacks, and insecure API endpoints constantly evolving, a proactive penetration testing approach is no longer optional but a business imperative for safeguarding sensitive user data and ensuring regulatory compliance

This intensive program covers the entire secure development lifecycle (SDLC) from a security perspective, emphasizing practical, hands-on techniques for both static and dynamic analysis. Participants will master industry-standard tools and frameworks like OWASP MASVS and the OWASP Mobile Top 10 to perform expert-level security assessments. By focusing on real-world zero-day vulnerabilities and advanced attack scenarios, this course prepares professionals to become highly skilled Mobile Security Analysts and Penetration Testers ready to tackle the complex challenges of securing the next generation of mobile applications.

Programme Curriculum

Mobile Application Security and Penetration Testing Training Course

Introduction

The proliferation of mobile devices and the "mobile-first" approach across all industries have made Mobile Application Security a critical and high-demand domain. Mobile Application Security and Penetration Testing Training Course is designed to equip participants with the latest ethical hacking skills and methodologies to identify, exploit, and remediate vulnerabilities in modern Android and iOS applications. With advanced cyber

threats like AI-driven malware, complex reverse engineering attacks, and insecure API endpoints constantly evolving, a proactive penetration testing approach is no longer optional but a business imperative for safeguarding sensitive user data and ensuring regulatory compliance

This intensive program covers the entire secure development lifecycle (SDLC) from a security perspective, emphasizing practical, hands-on techniques for both static and dynamic analysis. Participants will master industry-standard tools and frameworks like OWASP MASVS and the OWASP Mobile Top 10 to perform expert-level security assessments. By focusing on real-world zero-day vulnerabilities and advanced attack scenarios, this course prepares professionals to become highly skilled Mobile Security Analysts and Penetration Testers ready to tackle the complex challenges of securing the next generation of mobile applications.

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Master OWASP Mobile Top 10 risks and exploitation techniques.
2. Perform advanced Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) on Android and iOS apps.
3. Execute sophisticated Reverse Engineering and Code Obfuscation bypasses on mobile binaries.
4. Conduct comprehensive API Security Testing for mobile backend services and endpoints.
5. Implement and verify Runtime Application Self-Protection (RASP) mechanisms.
6. Identify and exploit flaws in Insecure Data Storage and Cryptographic Implementations.
7. Bypass advanced security controls like SSL Pinning and Root/Jailbreak Detection.
8. Understand and secure mobile apps within a DevSecOps pipeline.
9. Apply Zero Trust Architecture principles to the mobile application layer.
10. Analyze and mitigate Mobile Malware and advanced spyware threats.
11. Perform secure configuration analysis for both Android and iOS platform components.
12. Generate professional, actionable Penetration Testing Reports with detailed Remediation Strategies.
13. Ensure mobile app adherence to key Regulatory Compliance frameworks

Target Audience

1. Mobile App Developers
2. Penetration Testers and Ethical Hackers
3. Application Security Engineers
4. Security Consultants and Auditors
5. DevSecOps Engineers
6. Quality Assurance Testers with a focus on security
7. Cybersecurity Analysts and Researchers
8. IT Security Managers and Risk Officers.

Course Modules

Module 1: Mobile Security Fundamentals & Lab Setup

- Introduction to Android & iOS security architecture.
- Overview of the OWASP Mobile Top 10 and MASVS standards.

- Setting up a mobile penetration testing environment
- Essential tools: ADB, Xcode, Proxy configuration
- Case Study: The $2.5 Million Android SMS Stealer Malware.

Module 2: Static Analysis

- Decompilation and disassembly of APK and IPA files.
- Analyzing configuration files
- Identifying hardcoded secrets, keys, and credentials in the source code.
- Automated static analysis with tools like MobSF.
- Case Study: Hardcoded AWS Keys in a Fitness App Leading to Data Breach.

Module 3: Dynamic Analysis

- Intercepting and analyzing network traffic using proxy tools.
- Runtime manipulation and hooking using Frida and Objection.
- Monitoring file system, database, and logcat activities.
- Examining memory for sensitive data exposure.
- Case Study: Financial App Session Hijacking via Insecure Logging.

Module 4: Insecure Data Storage

- Identifying data stored in insecure locations
- Exploiting insecure local files and unencrypted backups.
- Keychain and Android Keystore analysis and extraction techniques.
- Remediation: Secure storage best practices and encrypted containers.
- Case Study: Health App Exposing Patient Records in Plaintext SQLite Database.

Module 5: Insecure Communication & Cryptography

- Attacks on data in transit: Man-in-the-Middle attacks.
- Bypassing and exploiting weak SSL/TLS implementations.
- Exploiting certificate and SSL Pinning implementation flaws.
- Identifying and exploiting weak or custom cryptographic algorithms.
- Case Study: Banking App SSL Pinning Bypass Leading to Credential Theft.

Module 6: Authentication & Authorization Flaws

- Testing for insecure user authentication, including weak password policies.
- Bypassing local and server-side authorization controls
- Exploiting session management vulnerabilities and insecure tokens.
- Testing for multi-factor authentication bypasses.
- Case Study: The 'Guessable Token' Flaw that Allowed Admin Access in a CRM App.

Module 7: Platform-Specific Security Issues

- Exploiting exposed Inter-Process Communication components
- Attacking Content Providers for information disclosure.
- Exploiting Deep Link vulnerabilities and URL Scheme attacks.
- Analysis of the Android Permission Model and its misuse.
- Case Study: Content Provider Leakage Exploited to Steal Contacts from a Utility App.

Module 8: Platform-Specific Security Issues

- Understanding the iOS security model, sandboxing, and code signing.
- Exploiting URL Schemes and Universal Links.
- Analyzing and manipulating the iOS Keychain.
- Jailbreak detection bypass and testing on non-jailbroken devices.
- Case Study: The "Side-Channel Data Leakage" via Pasteboard in a Popular iOS App.

Module 9: Reverse Engineering and Tampering

- Advanced techniques for decompiling and disassembling mobile binaries.
- Bypassing anti-reverse engineering controls and Obfuscation.
- Binary patching and code modification to alter app logic.
- Tools: Hopper Disassembler and IDA Pro.
- Case Study: Tampering with a Gaming App's Client Logic to Grant Unlimited Resources.

Module 10: Client-Side Injections

- Exploiting WebViews for Cross-Site Scripting and other injection attacks.
- Testing for SQLite/SQL Injection vulnerabilities in local storage.
- Injection via insecure keyboard input and third-party SDKs.
- Client-side validation bypass techniques.
- Case Study: Insecure WebView Implementation Leading to App-in-the-Middle Attack.

Module 11: Backend API Security for Mobile Apps

- Identifying and exploiting common API vulnerabilities
- Testing for weak Input Validation on all API parameters.
- Analyzing mobile-specific API issues
- Using Burp Suite for advanced mobile API testing.
- Case Study: Broken Object-Level Authorization in an E-commerce API.

Module 12: Advanced Platform Protection Bypass

- Techniques to bypass various Root Detection mechanisms.
- Methods to bypass various Jailbreak Detection mechanisms
- Deep dive into bypassing advanced SSL Pinning using tools like Frida.
- Evading Anti-Debugging and Anti-Tampering checks.
- Case Study: How a High-Security Payment App's Root Detection was Bypassed by a Custom Hook.

Module 13: Mobile Malware Analysis

- Identifying the characteristics and attack vectors of mobile malware.
- Tools and techniques for basic malware and spyware analysis.
- Understanding common mobile banking Trojans and ransomware.
- Case Study: Deep Analysis of the Joker Malware and its Subscription Fraud Technique.

Module 14: Mobile DevSecOps and Hardening

- Integrating security testing into the CI/CD pipeline.
- Implementing Secure Coding practices for Android and iOS.
- Application Hardening techniques

- Deploying and configuring Runtime Application Self-Protection
- Case Study: Implementing an Automated SAST Check to Prevent Secrets from Reaching Production.

Module 15: Reporting, Risk, and Compliance

- Developing professional, actionable penetration test reports.
- Vulnerability classification and Risk Scoring
- Remediation guidance and verification strategies.
- Mapping vulnerabilities to regulatory standards
- Case Study: Writing a Final Report for a FinTech App with High-Impact Regulatory Risks.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com