

Mobile AppSec: OWASP Top 10, iOS & Android

Learn to assess and secure iOS and Android apps against OWASP Mobile Top 10 risks, from reverse engineering to API security testing.

5 Days

DURATION

38

TOPICS

11

HANDS-ON ACTIVITIES

COURSE OVERVIEW

This course examines mobile security fundamentals, including mobile architecture, threats, and the OWASP Mobile Top 10. It covers iOS and Android architecture, data storage, jailbreaking and rooting, application interaction, and malware threats on both platforms. Learners then work through static application analysis and reverse engineering of obfuscated applications, followed by mobile penetration testing using the Mobile Application Security Verification Standard, including jailbreak detection, certificate pinning, and keychain and keystore recommendations. The course concludes with API security audit testing and API security tools and best practices, alongside techniques for protecting mobile devices with antivirus and security tools.

WHO THIS COURSE IS FOR

Penetration Testers

Mobile Security Analysts

Application Security Engineers

Security Auditors

Reverse Engineers

LEARNING OBJECTIVES

- Explain mobile architecture, threats and the OWASP Mobile Top 10
- Describe iOS and Android architecture and data storage mechanisms
- Identify weaknesses from jailbreaking, rooting and malware threats
- Analyse mobile applications through static analysis and reverse engineering
- Apply the Mobile Application Security Verification Standard to app testing
- Assess certificate pinning, jailbreak detection and application integrity
- Evaluate API security risks and test APIs for common vulnerabilities
- Compare API security tools and best practices for securing mobile devices

38 Topics

DAY 1 Introduction to Mobile Security

TOPICS

- Introduction to Mobile Security
- Mobile Problems and Opportunities
- Challenges and Opportunities for Secure Mobile Phone Deployments
- Weaknesses in Mobile Devices
- OWASP Mobile Top 10
- Mobile Architecture & Threats

DAY 2 iOS & Android Security Fundamentals

TOPICS

- iOS Architecture
- Jailbreaking iOS Devices
- iOS Data Storage and File System Architecture
- iOS Application Interaction
- iOS Malware Threats
- Android Architecture
- Rooting Android Devices
- Android Data Storage and File System Architecture
- Android Application Interaction
- Android Malware Threats
- Android Platform Analysis

DAY 3 Static Analysis & Reverse Engineering

Static Application Analysis

3 Hands-On Labs

TOPICS

- Retrieving iOS and Android Apps for Reverse Engineering Analysis
- Decompiling Android Applications
- Circumventing iOS App Encryption
- Header Analysis and Objective-C Disassembly

Reverse-Engineering Obfuscated Applications

TOPICS

Identifying Obfuscation Techniques · Decompiling Obfuscated Applications

MOBILE APPLICATION SECURITY VERIFICATION STANDARD

2 Activities

3 Hands-On Labs

- Step-by-Step Recommendations for Application Analysis
- Taking a Methodical Approach to Application Security Verification
- Common Pitfalls While Assessing Applications
- Detailed Recommendations for Jailbreak Detection, Certificate Pinning, and Application Integrity Verification
- **Android and iOS Critical Data Storage:** Keychain and Keystore Recommendations

API Security Audit Testing

3 Hands-On Labs

TOPICS

- Introduction to API Security
- Basics of API Fundamentals
- Common Vulnerabilities and Attack Vectors in APIs (OWASP Top 10 API Security Risks)
- API Authentication, Authorization, and Data Integrity
- Tools and Methodologies for API Security Testing
- Assessing the Resilience of APIs to Various Types of Attacks
- Penetration Testing Techniques for APIs

API Security Tools & Best Practices

TOPICS

Real-World Case Studies · API Security Tools Overview · Securing APIs – Best Practices

Practise What You Learn

MODULE	ACTIVITY
Static Analysis & Reverse Engineering	HANDS-ON LAB
	■ Mobile Device Footprinting & Scanning: Gathering Information on Mobile Devices (OS, Apps, Network)
	■ Mobile Device Footprinting & Scanning: Identifying Open Ports & Services Running on a Mobile Device
	■ Mobile Device Footprinting & Scanning: Using Reconnaissance Tools to Map Mobile Attack Surface
	PENETRATION TESTING WITH LAB
	■ Intercepting TLS Traffic
Mobile Penetration Testing	■ Man-in-the-Middle Troubleshooting
	HANDS-ON LAB
	■ Exploiting Android ADB with PhoneSploit: Understanding Android Debug Bridge (ADB) and Its Security Risks
	■ Exploiting Android ADB with PhoneSploit: Exploiting ADB Misconfigurations with PhoneSploit
	■ Exploiting Android ADB with PhoneSploit: Identifying Weaknesses and Securing ADB Against Attacks
API Security & Mobile Device Protection	HANDS-ON LAB
	■ Securing Mobile Devices with Antivirus & Security Tools: Overview of Mobile Security Solutions
	■ Securing Mobile Devices with Antivirus & Security Tools: Scanning and Detecting Malware on Mobile Devices
	■ Securing Mobile Devices with Antivirus & Security Tools: Best Practices for Securing Android and iOS Devices

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com