

Mobile Security: OWASP Mobile Top 10 & ADB Exploits

3 Days

DURATION

9

MODULES

37

TOPICS

LEARNING OBJECTIVES

- Explain the importance and challenges of mobile security testing
- Describe mobile app architecture and OS security models
- Identify OWASP Mobile Top 10 risks such as insecure storage
- Apply reconnaissance tools to map the mobile attack surface
- Analyse security misconfigurations and real-world incidents
- Exploit ADB misconfigurations using PhoneSploit
- Assess mobile devices using antivirus and security tools
- Plan secure coding and continuous testing for mobile apps

9 Modules, 37 Topics

01

Introduction to Mobile Security Testing

TOPICS

- Importance of Mobile Application Security Testing
- Differences Between Web and Mobile Application Security
- Security Challenges in Mobile Applications
- Attack Surface in Mobile Applications

02

Mobile Application Architecture & Security Considerations

TOPICS

- Understanding Mobile App Components (Frontend, Backend, APIs)
- Mobile OS Security Models (Android vs. iOS)
- Security Implications of Mobile App Permissions
- Secure Data Storage and Communication in Mobile Apps

03

Overview of OWASP Mobile Top 10 Security Risks

TOPICS

- | | |
|-----------------------------|------------------------------|
| ■ Improper Platform Usage | ■ Insecure Authorization |
| ■ Insecure Data Storage | ■ Client Code Quality Issues |
| ■ Insecure Communication | ■ Code Tampering |
| ■ Insecure Authentication | ■ Reverse Engineering |
| ■ Insufficient Cryptography | ■ Extraneous Functionality |

04

Mobile Device Footprinting & Scanning (Practical)

TOPICS

- Gathering Information on Mobile Devices (OS, Apps, Network)
- Identifying Open Ports & Services Running on a Mobile Device
- Using Reconnaissance Tools to Map Mobile Attack Surface

05

Mobile Application Security Testing Process

TOPICS

- Pre-Engagement Activities and Scoping
- Understanding Threat Models for Mobile Applications
- Identifying and Mapping Attack Vectors

06

Mobile Application Vulnerability Identification

TOPICS

- Identifying Risks in Mobile Apps Based on OWASP Guidelines
- Analyzing Security Misconfigurations in Mobile Apps
- Reviewing Real-World Mobile Security Incidents

07

Exploiting Android ADB with PhoneSploit (Practical)

TOPICS

- Understanding Android Debug Bridge (ADB) and its Security Risks
- Exploiting ADB Misconfigurations with PhoneSploit
- Identifying Weaknesses and Securing ADB Against Attacks

08

Securing Mobile Devices with Antivirus & Security Tools (Practical)

TOPICS

- Overview of Mobile Security Solutions
- Scanning and Detecting Malware on Mobile Devices
- Best Practices for Securing Android and iOS Devices

09

Best Practices for Secure Mobile Application Development & Testing

TOPICS

- Security in the Mobile App Development Lifecycle
- Secure Coding & Testing Strategies for Developers and Testers
- Security Considerations for iOS and Android Apps
- Guidelines for Continuous Security Testing in Mobile Development

WHAT IS INCLUDED

Everything You Need to Succeed

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