



Mobile Penetration Testing 🕒 9 hours of content | 30 hours of practice | Final Project

1. Introduction to Mobile Penetration Testing

- Introduction to Android App Development
- Familiarization with the Operating System
- Types of Applications:
- Web App
- Hybrid App
- Native App
- Setting Up a Research and Development Environment:
- Android Studio
- Genymotion
- Structure of a Web App

2. Analysis of Native Applications

- Structure of Native Applications
- Android Building Blocks:
- Manifest File
- Activity
- Views
- Fragments
- Intent
- Content Provider
- Broadcast Receiver

3. Analysis of Hybrid Applications

- Installing Plugin in Cordova
- Creating a Cordova Application
- Setting Up a Development Environment in Cordova
- Structure of Hybrid Apps
- Developing an Application with:
- HTML, CSS, JS
- Native Storage
- SQLite
- Local Notifications
- Submission Project

4. Security Flaws in Development

- Android App Sandbox
- Processes in Android
- File and Path Structure
- Working with ADB
- Importer Platform Usage
- Exposed Application Interface
- LogCat
- Drozer

5. Security Vulnerabilities in Communication and Storage

- Insecure Data Storage
- Attacking Shared Preferences
- Attacking SQLite Database
- Attacking Data On Sdcard
- Insecure Communication
- Sniffing Android Traffic
- Using BurpSuite
- HTTPS And BurpSuite
- Bypass SSL Pinning

6. Vulnerabilities in Authentication and Authorization Mechanisms

- Insecure Authentication
- Using BurpSuite Repeater
- Using BurpSuite Intruder
- Insufficient Cryptography
- Attacking Custom Encryption
- App Reverse Engineering - Jadx
- Insecure Authorization Bypass
- Insecure Permission Bypass
- Facebook Messenger cast study
- Demo Of Mobile PT Report

7. Static and Dynamic Code Analysis

- Client Code Quality
- Google Maps Case Study
- Pro Guard
- Code Temparing
- Frida Dynamic Instrumentation
- Repackaging

8. Code Analysis and Finding Vulnerabilities

- App Reverse Engineering
- Dji Drone Hacking Case Study
- Root Detection
- LG Gome Hack Case Study
- Extraneous Funcionality
- Debug Enabled Apps
- Hack Apps Via Backup
- Course Summary