Mobile Penetration Testing

Unk9vvN

October
2021

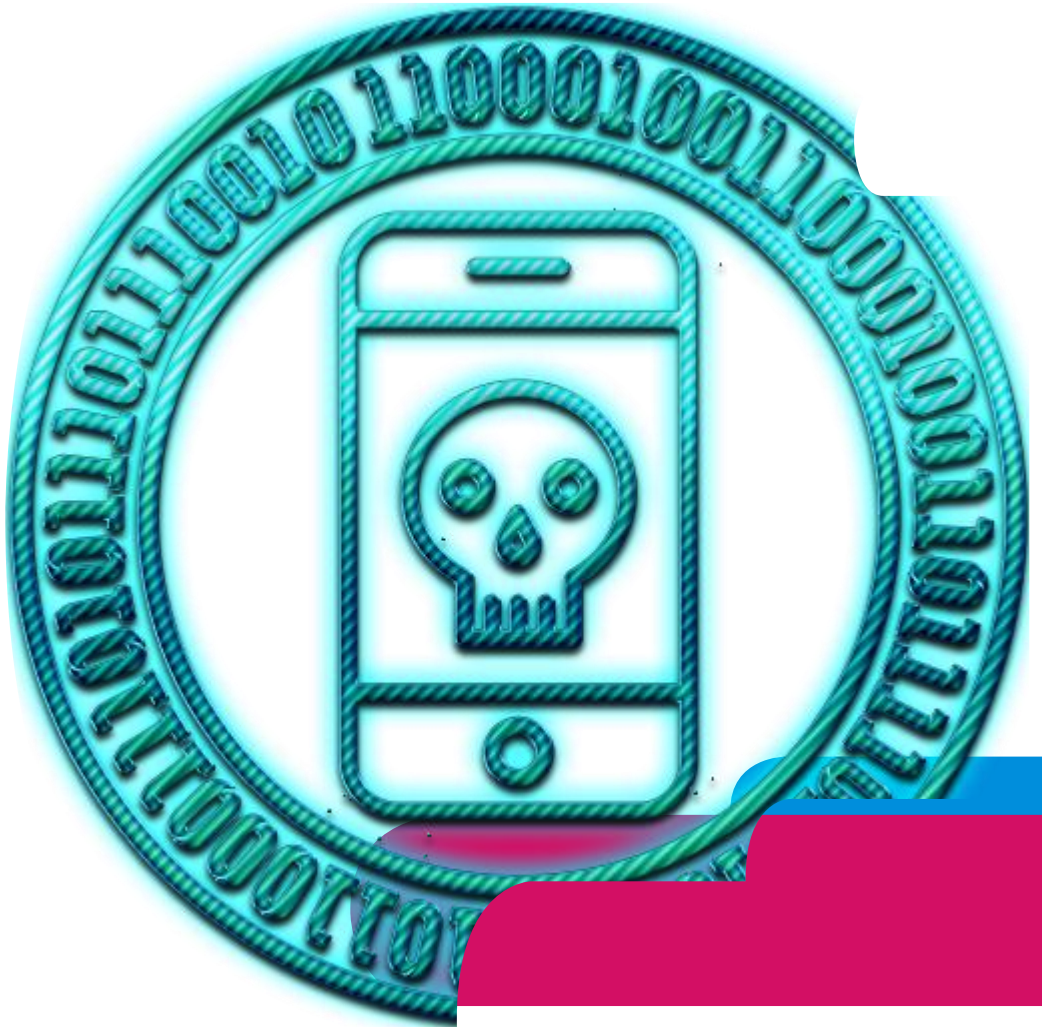
Introduction

0x01 Mobile App Taxonomy

- 1x01 Native App
- 1x02 Web App
- 1x03 Hybrid App
- 1x04 Progressive Web App

0x02 Mobile App Security Testing

- 2x01 Principles of Testing
- 2x02 Security Testing and the SDLC



General Vulnerabilities

0x01 Mobile App Authentication Architectures

- 1x01 General Guidelines on Testing Authentication
- 1x02 Verifying that Appropriate Authentication is in Place
- 1x03 Best Practices for Passwords
- 1x04 Stateful Session Management
- 1x05 Session Timeout
- 1x06 User Logout
- 1x07 Two-Factor Authentication
- 1x08 Stateless (Token-Based) Authentication
- 1x09 OAuth 2.0 Flows
- 1x10 Login Activity and Device Blocking

0x02 Testing Network Communication

- 2x01 Intercepting HTTP(S) Traffic
- 2x02 Burp plugins to Process Non-HTTP Traffic
- 2x03 Intercepting Traffic on the Network Layer
- 2x04 Verifying Data Encryption on the Network
- 2x05 Use Secure Communication Channels

0x03 Cryptography in Mobile Apps

- 3x01 Key Concepts
- 3x02 Identifying Insecure Cryptographic Algorithms
- 3x03 Common Configuration Issues
- 3x04 Cryptographic APIs on Android and iOS
- 3x05 Cryptographic policy

0x04 Testing Code Quality

- 4x01 Injection Flaws
- 4x02 Cross-Site Scripting Flaws
- 4x03 Memory Corruption Bugs

0x05 Tampering and Reverse Engineering

- 5x01 Reverse Engineering
- 5x02 Static Analysis
- 5x03 Dynamic Analysis
- 5x04 Tampering and Runtime Instrumentation
- 5x05 Customizing Android for Reverse Engineering

Android Vulnerabilities (One)

0x01 Platform Overview
- 1x01 Android Architecture
- 1x02 Android Security: Defense-in-Depth Approach
- 1x03 Android Application Structure
- 1x04 Android Application Publishing
- 1x05 Android Application Attack Surface

0x02 Android Basic Security Testing
- 2x01 Android Testing Setup
- 2x02 Basic Testing Operations
- 2x03 Setting up a Network Testing Environment

0x03 Data Storage on Android
- 3x01 Theory Overview
- 3x02 Data Storage Methods Overview
- 3x03 Local Storage for Sensitive Data
- 3x04 Local Storage for Input Validation
- 3x05 Logs for Sensitive Data
- 3x06 Sensitive Data is Sent to Third Parties
- 3x07 Keyboard Cache Is Disabled for Text Input Fields
- 3x08 Sensitive Stored Data Has Been Exposed via IPC Mechanisms
- 3x09 Sensitive Data Disclosure Through the User Interface
- 3x10 Backups for Sensitive Data
- 3x11 Sensitive Information in Auto-Generated Screenshots
- 3x12 Checking Memory for Sensitive Data
- 3x13 Device-Access-Security Policy

0x04 Android Cryptographic APIs
- 4x01 Recommendations
- 4x02 Symmetric Cryptography
- 4x03 Configuration of Cryptographic Standard Algorithms
- 4x04 Purposes of Keys
- 4x05 Random Number Generation

0x05 Local Authentication on Android
- 5x01 Confirm Credentials
- 5x02 Biometric Authentication

Android Vulnerabilities (Two)

0x06 Android Network APIs

- 6x01 Endpoint Identify Verification
- 6x02 Custom Certificate Stores and Certificate Pinning
- 6x03 Network Security Configuration Settings
- 6x04 Security Provider

0x07 Android Platform APIs

- 7x01 App Permissions
- 7x02 Injection Flaws
- 7x03 Fragment Injection
- 7x04 URL Loading in WebViews
- 7x05 Custom URL Schemes
- 7x06 Insecure Configuration of Instant Apps
- 7x07 Sensitive Functionality Exposure Through IPC
- 7x08 JavaScript Execution in WebViews
- 7x09 WebView Protocol Handlers
- 7x10 Java Objects Are Exposed Through WebViews

0x08 Code Quality and Build Settings for Android Apps

- 8x01 Making Sure That the App is Properly Signed
- 8x02 App is Debuggable
- 8x03 Debugging Symbols
- 8x04 Debugging Code and Verbose Error Logging
- 8x05 Weaknesses in Third Party Libraries
- 8x06 Exception Handling
- 8x07 Memory Corruption Bugs
- 8x08 Make Sure That Free Security Features Are Activated

0x09 Tampering and Reverse Engineering on Android

- 9x01 Reverse Engineering
- 9x02 Static Analysis
- 9x03 Dynamic Analysis
- 9x04 Tampering and Runtime Instrumentation
- 9x05 Customizing Android for Reverse Engineering

0x10 Android Anti-Reversing Defenses

- 10x01 Root Detection
- 10x02 Anti-Debugging Detection
- 10x03 File Integrity Checks
- 10x04 Reverse Engineering Tools Detection
- 10x05 Emulator Detection
- 10x06 Runtime Integrity Checks
- 10x07 Obfuscation
- 10x08 Device Binding

iOS Vulnerabilities (One)

0x01 Platform Overview
- 1x01 iOS Security Architecture
- 1x02 Software Development on iOS
- 1x03 Apps on iOS

0x02 iOS Basic Security Testing
- 2x01 iOS Testing Setup
- 2x02 Basic Testing Operations
- 2x03 Setting Up a Network Testing Environment

0x03 Data Storage on iOS
- 3x01 Local Data Storage
- 3x02 Logs for Sensitive Data
- 3x03 Sensitive Data Is Sent to Third Parties
- 3x04 Sensitive Data in the Keyboard Cache
- 3x05 Sensitive Data Is Exposed via IPC Mechanisms
- 3x06 Sensitive Data Disclosed Through the User Interface
- 3x07 Backups for Sensitive Data
- 3x08 Auto-Generated Screenshots for Sensitive Information
- 3x09 Memory for Sensitive Data

0x04 iOS Cryptographic APIs
- 4x01 Configuration of Cryptographic Standard Algorithms
- 4x02 Key Management
- 4x03 Random Number Generation

0x05 Local Authentication on iOS
- 5x01 Local Authentication
- 5x02 Note regarding temporariness of keys in the Keychain

0x06 iOS Network APIs
- 6x01 Network Framework
- 6x02 URLSession
- 6x03 App Transport Security
- 6x04 Custom Certificate Stores and Certificate Pinning

iOS Vulnerabilities (Two)

0x07 iOS Platform APIs
- 7x01 App Permissions
- 7x02 Sensitive Functionality Exposure Through IPC
- 7x03 Custom URL Schemes
- 7x04 iOS WebViews
- 7x05 WebView Protocol Handlers
- 7x06 Native Methods Are Exposed Through WebViews
- 7x07 Object Persistence
- 7x08 Enforced Updating

0x08 Code Quality and Build Settings for iOS Apps
- 8x01 Making Sure that the App Is Properly Signed
- 8x02 App is Debuggable
- 8x03 Debugging Symbols
- 8x04 Debugging Code and Verbose Error Logging
- 8x05 Weaknesses in Third Party Libraries
- 8x06 Exception Handling
- 8x07 Memory Corruption Bugs
- 8x08 Make Sure That Free Security Features Are Activated

0x09 Tampering and Reverse Engineering on iOS
- 9x01 Reverse Engineering
- 9x02 Static Analysis
- 9x03 Dynamic Analysis
- 9x04 Binary Analysis
- 9x05 Tampering and Runtime Instrumentation

0x10 iOS Anti-Reversing Defenses
- 10x01 Jailbreak Detection
- 10x02 Anti-Debugging Detection
- 10x03 File Integrity Checks
- 10x04 Reverse Engineering Tools Detection
- 10x05 Emulator Detection
- 10x06 Obfuscation
- 10x07 Device Binding

Unk9vvN

Phone:
026 368 06249

Email:
info@unk9vvn.com