Mobile Application Security Testing

[OWASP | SANS | PCI DSS | ISO27001]

android

Tests **Techniques** **Tools** **Apps**

Android Tests

- MASVS-STORAGE
- MASVS-CRYPTO
- MASVS-AUTH
- MASVS-NETWORK
- MASVS-PLATFORM
- MASVS-CODE
- MASVS-RESILIENCE

Generic Techniques

- ✓ Binary Analysis
- ✓ Tampering and Runtime Instrumentation
- ✓ Static Analysis
- ✓ Reverse Engineering
- ✓ Dynamic Analysis

STORAGE

- Testing the Device-Access-Security Policy
- Testing Local Storage for Sensitive Data
- Determining Whether Sensitive Data Is Shared with Third Parties via Embedded Services
- Testing Logs for Sensitive Data
- Determining Whether the Keyboard Cache Is Disabled for Text Input Fields
- Determining Whether Sensitive Data Is Shared with Third Parties via Notifications
- Testing Memory for Sensitive Data
- Testing Backups for Sensitive Data

CRYPTO

- Testing Random Number Generation
- Testing the Configuration of Cryptographic Standard Algorithms
- Testing Symmetric Cryptography
- Testing the Purposes of Keys

AUTH

- Testing Confirm Credentials
- Testing Biometric Authentication

NETWORK

- Testing Endpoint Identify Verification
- Testing the TLS Settings
- Testing the Security Provider
- Testing Data Encryption on the Network
- Testing Custom Certificate Stores and Certificate Pinning

PLATFORM

- Determining Whether Sensitive Stored Data Has Been Exposed via IPC Mechanisms
- Testing for App Permissions
- Testing for Vulnerable Implementation of PendingIntent
- Testing Deep Links
- Testing for Sensitive Functionality Exposure Through IPC

- Testing JavaScript Execution in WebViews
- Testing for Java Objects Exposed Through WebViews
- Testing WebView Protocol Handlers
- Testing WebViews Cleanup
- Testing for Overlay Attacks
- Checking for Sensitive Data Disclosure Through the User Interface
- Finding Sensitive Information in Auto-Generated Screenshots

CODE

- Testing Enforced Updating
- Checking for Weaknesses in Third Party Libraries
- Make Sure That Free Security Features Are Activated
- Testing for URL Loading in WebViews
- Testing Implicit Intents
- Testing for Injection Flaws
- Testing Local Storage for Input Validation
- Memory Corruption Bugs
- Testing Object Persistence

RESILIENCE

- Testing Emulator Detection
- Testing Root Detection
- Making Sure that the App is Properly Signed
- Testing File Integrity Checks
- Testing Runtime Integrity Checks
- Testing for Debugging Symbols
- Testing for Debugging Code and Verbose Error Logging
- Testing Obfuscation
- Testing whether the App is Debuggable
- Testing Reverse Engineering Tools Detection
- Testing Anti-Debugging Detection

Android Security Testing Techniques

- Reverse Engineering Android Apps
- Setting Up an Interception Proxy
- Process Exploration
- Runtime Reverse Engineering
- Disassembling Native Code
- Listing Installed Apps
- Automated Static Analysis
- Host-Device Data Transfer
- Symbolic Execution
- Basic Network Monitoring/Sniffing
- Repackaging & Re-Signing
- Information Gathering - Network Communication
- Dynamic Analysis on Non-Rooted Devices
- Reviewing Disassembled Native Code
- Reviewing Decompiled Java Code
- Installing Apps
- Patching
- Sandbox Inspection
- Get Open Files
- Monitoring System Logs
- Get Open Connections
- Disassembling Code to Smali
- Dynamic Analysis on Android
- Emulation-based Analysis
- Decompiling Java Code
- Repackaging Apps
- JNI Tracing
- Static Analysis on Android
- Taint Analysis
- Execution Tracing
- Getting Loaded Classes and Methods Dynamically
- Information Gathering - API Usage
- Library Injection
- Accessing the Device Shell
- Debugging
- Retrieving Strings
- Bypassing Certificate Pinning
- Waiting for the Debugger
- Accessing App Data Directories
- Get Loaded Native Libraries
- Native Code Tracing

- Method Hooking
- Retrieving Cross References
- Method Tracing
- Obtaining and Extracting Apps
- Exploring the App Package
- Root Detection
- Emulator Detection
- Insecure Data Storage – Shared Prefs - 1
- Insecure Data Storage - Shared Prefs - 2
- Insecure Data Storage - SQLite
- Insecure Data Storage – Temp Files
- Insecure Data Storage – SD Card
- Keyboard Cache
- Insecure Logging
- Input Validations – XSS
- Input Validations – SQLi
- Input Validations – WebView
- Unprotected Android Components – Activity
- Unprotected Android Components –Service
- Unprotected Android Components – Broadcast Receivers
- Unprotected Android Components – Content Providers (Coming Soon)
- Hard coding issues
- Network intercepting – HTTP
- Network intercepting – HTTPS
- Network intercepting – Certificate Pinning
- Misconfigured Network_Security_Config.xml
- Android Debuggable
- Android allowBackup
- Custom URL Scheme
- Broken Cryptography
- QR Code Scanning (Coming Soon)
- Fingerprint Authentication (Coming Soon)

Testing Tools

To perform static analysis, dynamic analysis, dynamic instrumentation, etc. These tools are meant to help you conduct your assessments, rather than provide a conclusive result on an application's security status. It's essential to carefully review the tools' output, as it can contain both false positives and false negatives.

we prioritize including tools that meet the following criteria:

- Open-source
- Free to use
- Capable of analyzing recent Android applications
- Regularly updated
- Strong community support

Note: The functionality of the tools can also be affected by whether you're using a rooted or jailbroken device, the specific version of the rooting or jailbreaking method, and/or the tool version itself.

Generic Tools

- r2frida
- Ghidra
- Frida
- LIEF
- Iaito
- MobSF
- RMS Runtime Mobile Security
- Objection
- Frida CodeShare

Android Tools

- Magisk
- Busybox.
- Bytecode Viewer
- Scrcpy
- APKiD
- Android SDK
- Termux
- MobSF for Android
- Jdb
- Apkx
- Apktool
- FlowDroid
- nm - Android

- RootCloak Plus
- JustTrustMe
- Adb
- Xposed
- Android NDK
- Drozer
- Android Studio
- Angr
- Android-SSL-TrustKiller
- radare2 for Android
- Frida for Android
- gplaycli
- jadx
- objection for Android
- SSLUnpinning
- House
- Proguard
- APKLab

Network Tools

- Wireshark
- MITM Relay
- OWASP ZAP
- Burp Suite
- bettercap
- Android tcpdump
- tcpdump