Mobile Security Testing Techniques

## **Generic Techniques**

| **ID** | **Name** | **Platform** |
| --- | --- | --- |
| [MASTG-TECH-0050](https://mas.owasp.org/MASTG/techniques/generic/MASTG-TECH-0050) | Binary Analysis | generic |
| [MASTG-TECH-0051](https://mas.owasp.org/MASTG/techniques/generic/MASTG-TECH-0051) | Tampering and Runtime Instrumentation | generic |
| [MASTG-TECH-0048](https://mas.owasp.org/MASTG/techniques/generic/MASTG-TECH-0048) | Static Analysis | generic |
| [MASTG-TECH-0047](https://mas.owasp.org/MASTG/techniques/generic/MASTG-TECH-0047) | Reverse Engineering | generic |
| [MASTG-TECH-0049](https://mas.owasp.org/MASTG/techniques/generic/MASTG-TECH-0049) | Dynamic Analysis | generic |

## **Android Techniques**

| **ID** | **Name** | **Platform** |
| --- | --- | --- |
| [MASTG-TECH-0013](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0013) | Reverse Engineering Android Apps | android |
| [MASTG-TECH-0011](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0011) | Setting Up an Interception Proxy | android |
| [MASTG-TECH-0044](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0044) | Process Exploration | android |
| [MASTG-TECH-0045](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0045) | Runtime Reverse Engineering | android |
| [MASTG-TECH-0018](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0018) | Disassembling Native Code | android |
| [MASTG-TECH-0006](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0006) | Listing Installed Apps | android |
| [MASTG-TECH-0025](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0025) | Automated Static Analysis | android |
| [MASTG-TECH-0002](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0002) | Host-Device Data Transfer | android |
| [MASTG-TECH-0037](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0037) | Symbolic Execution | android |
| [MASTG-TECH-0010](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0010) | Basic Network Monitoring/Sniffing | android |
| [MASTG-TECH-0039](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0039) | Repackaging & Re-Signing | android |
| [MASTG-TECH-0022](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0022) | Information Gathering - Network Communication | android |
| [MASTG-TECH-0026](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0026) | Dynamic Analysis on Non-Rooted Devices | android |
| [MASTG-TECH-0024](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0024) | Reviewing Disassembled Native Code | android |
| [MASTG-TECH-0023](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0023) | Reviewing Decompiled Java Code | android |
| [MASTG-TECH-0005](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0005) | Installing Apps | android |
| [MASTG-TECH-0038](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0038) | Patching | android |
| [MASTG-TECH-0030](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0030) | Sandbox Inspection | android |
| [MASTG-TECH-0027](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0027) | Get Open Files | android |
| [MASTG-TECH-0009](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0009) | Monitoring System Logs | android |
| [MASTG-TECH-0028](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0028) | Get Open Connections | android |
| [MASTG-TECH-0016](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0016) | Disassembling Code to Smali | android |
| [MASTG-TECH-0015](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0015) | Dynamic Analysis on Android | android |
| [MASTG-TECH-0036](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0036) | Emulation-based Analysis | android |
| [MASTG-TECH-0017](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0017) | Decompiling Java Code | android |
| [MASTG-TECH-0004](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0004) | Repackaging Apps | android |
| [MASTG-TECH-0035](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0035) | JNI Tracing | android |
| [MASTG-TECH-0014](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0014) | Static Analysis on Android | android |
| [MASTG-TECH-0108](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0108) | Taint Analysis | android |
| [MASTG-TECH-0032](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0032) | Execution Tracing | android |
| [MASTG-TECH-0042](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0042) | Getting Loaded Classes and Methods Dynamically | android |
| [MASTG-TECH-0021](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0021) | Information Gathering - API Usage | android |
| [MASTG-TECH-0041](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0041) | Library Injection | android |
| [MASTG-TECH-0001](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0001) | Accessing the Device Shell | android |
| [MASTG-TECH-0031](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0031) | Debugging | android |
| [MASTG-TECH-0019](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0019) | Retrieving Strings | android |
| [MASTG-TECH-0012](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0012) | Bypassing Certificate Pinning | android |
| [MASTG-TECH-0040](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0040) | Waiting for the Debugger | android |
| [MASTG-TECH-0008](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0008) | Accessing App Data Directories | android |
| [MASTG-TECH-0029](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0029) | Get Loaded Native Libraries | android |
| [MASTG-TECH-0034](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0034) | Native Code Tracing | android |
| [MASTG-TECH-0043](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0043) | Method Hooking | android |
| [MASTG-TECH-0020](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0020) | Retrieving Cross References | android |
| [MASTG-TECH-0033](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0033) | Method Tracing | android |
| [MASTG-TECH-0003](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0003) | Obtaining and Extracting Apps | android |
| [MASTG-TECH-0007](https://mas.owasp.org/MASTG/techniques/android/MASTG-TECH-0007) | Exploring the App Package | android |

## **Ios Techniques**

| **ID** | **Name** | **Platform** |
| --- | --- | --- |
| [MASTG-TECH-0056](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0056) | Installing Apps | ios |
| [MASTG-TECH-0059](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0059) | Accessing App Data Directories | ios |
| [MASTG-TECH-0095](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0095) | Method Hooking | ios |
| [MASTG-TECH-0093](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0093) | Waiting for the debugger | ios |
| [MASTG-TECH-0082](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0082) | Get Loaded Native Libraries | ios |
| [MASTG-TECH-0090](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0090) | Patching | ios |
| [MASTG-TECH-0067](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0067) | Dynamic Analysis on iOS | ios |
| [MASTG-TECH-0065](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0065) | Reverse Engineering iOS Apps | ios |
| [MASTG-TECH-0088](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0088) | Emulation-based Analysis | ios |
| [MASTG-TECH-0086](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0086) | Method Tracing | ios |
| [MASTG-TECH-0096](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0096) | Process Exploration | ios |
| [MASTG-TECH-0062](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0062) | Basic Network Monitoring/Sniffing | ios |
| [MASTG-TECH-0075](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0075) | Reviewing Decompiled Objective-C and Swift Code | ios |
| [MASTG-TECH-0083](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0083) | Sandbox Inspection | ios |
| [MASTG-TECH-0064](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0064) | Bypassing Certificate Pinning | ios |
| [MASTG-TECH-0073](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0073) | Information Gathering - API Usage | ios |
| [MASTG-TECH-0085](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0085) | Execution Tracing | ios |
| [MASTG-TECH-0094](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0094) | Getting Loaded Classes and Methods dynamically | ios |
| [MASTG-TECH-0078](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0078) | Automated Static Analysis | ios |
| [MASTG-TECH-0081](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0081) | Get Open Connections | ios |
| [MASTG-TECH-0097](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0097) | Runtime Reverse Engineering | ios |
| [MASTG-TECH-0053](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0053) | Host-Device Data Transfer | ios |
| [MASTG-TECH-0057](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0057) | Listing Installed Apps | ios |
| [MASTG-TECH-0092](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0092) | Repackaging and Re-Signing | ios |
| [MASTG-TECH-0091](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0091) | Library Injection | ios |
| [MASTG-TECH-0061](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0061) | Dumping KeyChain Data | ios |
| [MASTG-TECH-0080](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0080) | Get Open Files | ios |
| [MASTG-TECH-0089](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0089) | Symbolic Execution | ios |
| [MASTG-TECH-0070](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0070) | Extracting Information from the Application Binary | ios |
| [MASTG-TECH-0054](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0054) | Obtaining and Extracting Apps | ios |
| [MASTG-TECH-0087](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0087) | Native Code Tracing | ios |
| [MASTG-TECH-0066](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0066) | Static Analysis on iOS | ios |
| [MASTG-TECH-0079](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0079) | Dynamic Analysis on Non-Jailbroken Devices | ios |
| [MASTG-TECH-0060](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0060) | Monitoring System Logs | ios |
| [MASTG-TECH-0052](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0052) | Accessing the Device Shell | ios |
| [MASTG-TECH-0071](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0071) | Retrieving Strings | ios |
| [MASTG-TECH-0068](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0068) | Disassembling Native Code | ios |
| [MASTG-TECH-0084](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0084) | Debugging | ios |
| [MASTG-TECH-0072](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0072) | Retrieving Cross References | ios |
| [MASTG-TECH-0098](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0098) | Patching React Native Apps | ios |
| [MASTG-TECH-0055](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0055) | Repackaging Apps | ios |
| [MASTG-TECH-0077](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0077) | Reviewing Disassembled Native Code | ios |
| [MASTG-TECH-0076](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0076) | Reviewing Disassembled Objective-C and Swift Code | ios |
| [MASTG-TECH-0074](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0074) | Information Gathering - Network Communication | ios |
| [MASTG-TECH-0058](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0058) | Exploring the App Package | ios |
| [MASTG-TECH-0063](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0063) | Setting up an Interception Proxy | ios |
| [MASTG-TECH-0069](https://mas.owasp.org/MASTG/techniques/ios/MASTG-TECH-0069) | Decompiling Native Code | ios |
|  | | |

# OWASP MAS Checklist

The OWASP Mobile Application Security Checklist contains links to the MASTG test cases for each MASVS control.

* **Security Assessments / Pentests**: ensure you're at least covering the standard attack surface and start exploring.
* **Standard Compliance**: includes MASVS and MASTG versions and commit IDs.
* **Learn & practice** your mobile security skills.
* **Bug Bounties**: go step by step covering the mobile attack surface.

URL: <https://github.com/OWASP/owasp-mastg/releases/latest/download/OWASP_MAS_Checklist.xlsx>

****url