## Mobile Application Penetration Testing Cheat Sheet

The Mobile App Pentest cheat sheet was created to provide concise collection of high value information on specific mobile application penetration testing topics and checklist, which is mapped OWASP Mobile Risk Top 10 for conducting pentest.

### Mobile Application Security Testing Distributions

- Appie - A portable software package for Android Pentesting and an awesome alternative to existing Virtual machines.
- Android Tamer - Android Tamer is a Virtual / Live Platform for Android Security professionals.
- Androl4b - A Virtual Machine For Assessing Android applications, Reverse Engineering and Malware Analysis
- Vezir Project - Mobile Application Pentesting and Malware Analysis Environment.
- Mobexler - Mobexler is a customised virtual machine, designed to help in penetration testing of Android & iOS applications.

### All-in-One Mobile Security Frameworks

- Mobile Security Framework - MobSF - Mobile Security Framework is an intelligent, all-in-one open source mobile application (Android/iOS) automated pen-testing framework capable of performing static and dynamic analysis.
  - `python manage.py runserver 127.0.0.1:1337`

- Needle - Needle is an open source, modular framework to streamline the process of conducting security assessments of iOS apps including Binary Analysis, Static Code Analysis, Runtime Manipulation using Cycript and Frida hooking, and so on.
- Objection - Objection is a runtime mobile exploration toolkit, powered by Frida. It was built with the aim of helping assess mobile applications and their security posture without the need for a jailbroken or rooted mobile device.
- RMS-Runtime-Mobile-Security - Runtime Mobile Security (RMS), powered by FRIDA, is a powerful web interface that helps you to manipulate Android and iOS Apps at Runtime.

### Android Application Penetration Testing

### Reverse Engineering and Static Analysis

- APKTool - A tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modifications.
  - Disassembling Android apk file

    -
      ```
      apktool d <apk file>
      ```
  - Rebuilding decoded resources back to binary APK/JAR with certificate signing

    -
      ```
      apktool b <modified folder>
      ```

    -
      ```
      keytool -genkey -v -keystore keys/test.keystore
      -alias Test -keyalg RSA -keysize 1024 -sigalg SHA1withRSA
      -validity 10000
      ```

    -
      ```
      jarsigner -keystore keys/test.keystore dist/test.apk
      -sigalg SHA1withRSA -digestalg SHA1 Test
      ```
- Bytecode Viewer - Bytecode Viewer is an Advanced Lightweight Java Bytecode Viewer, It's written completely in Java, and it's open sourced.
- Jadx - Dex to Java decompiler: Command line and GUI tools for produce Java source code from Android Dex and Apk files.
- APK Studio - Open-source, cross platform Qt based IDE for reverse-engineering Android application packages.
- Oat2dex - A tool for converting .oat file to .dex files.
  - Deoptimize boot classes (The output will be in "odex" and "dex" folders)

    -
      ```
      java -jar oat2dex.jar boot <boot.oat file>
      ```
  - Deoptimize application

    -
      ```
      java -jar oat2dex.jar <app.odex> <boot-class-folder
      output from above>
      ```
  - Get odex from oat

    -
      ```
      java -jar oat2dex.jar odex <oat file>
      ```
  - Get odex smali (with optimized opcode) from oat/odex

    -
      ```
      java -jar oat2dex.jar smali <oat/odex file>
      ```

- Spotbugs - SpotBugs is FindBugs' successor. A tool for static analysis to look for bugs in Java code.
- Qark - This tool is designed to look for several security related Android application vulnerabilities, either in source code or packaged APKs.
- SUPER - SUPER is a command-line application that can be used in Windows, MacOS X and Linux, that analyzes .apk files in search for vulnerabilities. It does this by decompressing APKs and applying a series of rules to detect those vulnerabilities.
- AndroBugs - AndroBugs Framework is an efficient Android vulnerability scanner that helps developers or hackers find potential security vulnerabilities in Android applications. No need to install on Windows.
- Simplify - A tool for de-obfuscating android package into Classes.dex which can be use Dex2jar and JD-GUI to extract contents of dex file.

  -
    ```
    simplify.jar -i "input smali files or folder" -o <output
    dex file>
    ```
- ClassNameDeobfuscator - Simple script to parse through the .smali files produced by apktool and extract the .source annotation lines.
- Android backup extractor - Utility to extract and repack Android backups created with adb backup (ICS+). Largely based on BackupManagerService.java from AOSP. Tip !! "adb backup" command can also be used for extracting application package with the following command:

  -
    ```
    adb backup <package name>
    ```

  -
    ```
    dd if=backup.ab bs=1 skip=24 | python -c "import zlib,sys;sys.stdout.write(zlib.dec
    > backup.tar
    ```
- GDA(GJoy Dex Analysizer) - GDA, a new Dalvik bytecode decompiler, is implemented in C++, which has the advantages of faster analysis and lower memory&disk consumption and an stronger ability to decompiling the APK, DEX, ODEX, OAT files(supports JAR, CLASS and AAR files since 3.79)

### Dynamic and Runtime Analysis

- Cydia Substrate - Cydia Substrate for Android enables developers to make changes to existing software with Substrate extensions that are injected in to the target process's memory.
- Xposed Framework - Xposed framework enables you to modify the system or application aspect and behaviour at runtime, without modifying any Android application package(APK) or re-flashing.
- PID Cat - An update to Jeff Sharkey's excellent logcat color script which only shows log entries for processes from a specific application package.
- Inspeckage - Inspeckage is a tool developed to offer dynamic analysis of Android applications. By applying hooks to functions of the Android API, Inspeckage will help you understand what an Android application is doing at runtime.
- Frida - The toolkit works using a client-server model and lets you inject in to running processes not just on Android, but also on iOS, Windows

and Mac.

- Diff-GUI - A Web framework to start instrumenting with the avaliable modules, hooking on native, inject JavaScript using Frida.
- Fridump - Fridump is using the Frida framework to dump accessible memory addresses from any platform supported. It can be used from a Windows, Linux or Mac OS X system to dump the memory of an iOS, Android or Windows application.
- House - A runtime mobile application analysis toolkit with a Web GUI, powered by Frida, is designed for helping assess mobile applications by implementing dynamic function hooking and intercepting and intended to make Frida script writing as simple as possible.
- AndBug - AndBug is a debugger targeting the Android platform's Dalvik virtual machine intended for reverse engineers and developers.
  - Identifying application process using adb shell
    - `adb shell ps | grep -i "App keyword"`
  - Accessing the application using AndBug in order to identify loaded classes
    - `andbug shell -p <process number>`
  - Tracing specific class
    - `ct <package name>`
  - Debugging with jdb
    - `adb forward tcp:<port> jdwp:<port>`
    - `jdb -attach localhost:<port>`
- Cydia Substrate: Introspy-Android - Blackbox tool to help understand what an Android application is doing at runtime and assist in the identification of potential security issues.
- Drozer - Drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.
  - Starting a session
    - `adb forward tcp:31415 tcp:31415`
    - `drozer console connect`
  - Retrieving package information
    - `run app.package.list -f <app name>`
    - `run app.package.info -a <package name>`
  - Identifying the attack surface
    - `run app.package.attacksurface <package name>`
  - Exploiting Activities
    - `run app.activity.info -a <package name> -u`
    - `run app.activity.start --component <package name> <component name>`
  - Exploiting Content Provider
    - `run app.provider.info -a <package name>`
    - `run scanner.provider.finduris -a <package name>`
    - `run app.provider.query <uri>`
    - `run app.provider.update <uri> --selection <conditions>`

        `<selection arg> <column> <data>`
        - `run scanner.provider.sqltables -a <package name>`
        - `run scanner.provider.injection -a <package name>`
        - `run scanner.provider.traversal -a <package name>`
    - Exploiting Broadcast Receivers
        - `run app.broadcast.info -a <package name>`
        - `run app.broadcast.send --component <package name> <component name> --extra <type> <key> <value>`
        - `run app.broadcast.sniff --action <action>`
    - Exploiting Service
        - `run app.service.info -a <package name>`
        - `run app.service.start --action <action> --component <package name> <component name>`
        - `run app.service.send <package name> <component name> --msg <what> <arg1> <arg2> --extra <type> <key> <value> --bundle-as-obj`

### Network Analysis and Server Side Testing

- Tcpdump - A command line packet capture utility.
- Wireshark - An open-source packet analyzer.
    - Live packet captures in real time
        - `adb shell "tcpdump -s 0 -w - | nc -l -p 4444"`
        - `adb forward tcp:4444 tcp:4444`
        - `nc localhost 4444 | sudo wireshark -k -S -i -`
- Mallory - A Man in The Middle Tool (MiTM) that use to monitor and manipulate traffic on mobile devices and applications.
- Burp Suite - Burp Suite is an integrated platform for performing security testing of applications.
    - Installing trusted CA at the Android OS level (Root device/Emulator) for Android N+ as the following:
        - `openssl x509 -inform PEM -subject_hash -in BurpCA.pem | head -1`
        - `cat BurpCA.pem > 9a5ba580.0`
        - `openssl x509 -inform PEM -text -in BurpCA.pem -out /dev/null >> 9a5ba580.0`
        - `adb root`
        - `abd remount`
        - `adb push 9a5ba580.0 /system/etc/security/cacerts/`
        - `adb shell "chmod 644 /system/etc/security/cacerts/9a5ba580.0"`
        - `adb shell "reboot"`
        - Check Settings > Security > Trusted Credentials > SYSTEM to confirm your newly added CA is listed.
- Burp Suite Mobile Assistant - Burp Suite Mobile Assistant is a tool to facilitate testing of iOS apps with Burp Suite; It can modify the system-wide proxy settings of iOS devices so that HTTP(S) traffic can be easily

redirected to a running instance of Burp, It can attempt to circumvent SSL certificate pinning in selected apps, allowing Burp Suite to break their HTTPS connections and intercept, inspect and modify all traffic.
- OWASP ZAP - OWASP Zed Attack Proxy Project is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.
- Proxydroid - Global Proxy App for Android System.
- mitmproxy - is an interactive, SSL/TLS-capable intercepting proxy with a console interface for HTTP/1, HTTP/2, and WebSockets.

### Bypassing Root Detection and SSL Pinning

- Magisk - Magisk suites provide root access to your device, capability to modify read-only partitions by installing modules and hide Magisk from root detections/system integrity checks.
- Xposed Module: Just Trust Me - Xposed Module to bypass SSL certificate pinning.
- Xposed Module: SSLUnpinning - Android Xposed Module to bypass SSL certificate validation (Certificate Pinning).
- Cydia Substrate Module: Android SSL Trust Killer - Blackbox tool to bypass SSL certificate pinning for most applications running on a device.
- Cydia Substrate Module: RootCoak Plus - Patch root checking for commonly known indications of root.
- Android-ssl-bypass - an Android debugging tool that can be used for bypassing SSL, even when certificate pinning is implemented, as well as other debugging tasks. The tool runs as an interactive console.
- Apk-mitm - A CLI application that automatically prepares Android APK files for HTTPS inspection
- Frida CodeShare - The Frida CodeShare project is comprised of developers from around the world working together with one goal - push Frida to its limits in new and innovative ways.
  - Bypassing Root Detection
    - `frida --codeshare dzonerzy/fridantiroot -f YOUR_BINARY`
  - Bypassing SSL Pinning
    - `frida --codeshare pcipolloni/universal-android-ssl-pinning-bypass-with-frida -f YOUR_BINARY`

### Security Libraries

- PublicKey Pinning - Pinning in Android can be accomplished through a custom X509TrustManager. X509TrustManager should perform the customary X509 checks in addition to performing the pinning configuration.
- Android Pinning - A standalone library project for certificate pinning on Android.
- Java AES Crypto - A simple Android class for encrypting & decrypting strings, aiming to avoid the classic mistakes that most such classes suffer

from.

- Proguard - ProGuard is a free Java class file shrinker, optimizer, obfuscator, and preverifier. It detects and removes unused classes, fields, methods, and attributes.
- SQL Cipher - SQLCipher is an open source extension to SQLite that provides transparent 256-bit AES encryption of database files.
- Secure Preferences - Android Shared preference wrapper than encrypts the keys and values of Shared Preferences.
- Trusted Intents - Library for flexible trusted interactions between Android apps.
- RootBeer - A tasty root checker library and sample app.
- End-to-end encryption - Capillary is a library to simplify the sending of end-to-end encrypted push messages from Java-based application servers to Android clients.

### iOS Application Penetration Testing

### Access Filesystem on iDevice

- FileZilla - It supports FTP, SFTP, and FTPS (FTP over SSL/TLS).
- Cyberduck - Libre FTP, SFTP, WebDAV, S3, Azure & OpenStack Swift browser for Mac and Windows.
- itunnel - Use to forward SSH via USB.
- iProxy - Let's you connect your laptop to the iPhone to surf the web.
- iFunbox - The File and App Management Tool for iPhone, iPad & iPod Touch.

### Reverse Engineering and Static Analysis

- otool - The otool command displays specified parts of object files or libraries.
- Clutch - Decrypted the application and dump specified bundleID into binary or .ipa file.
- Dumpdecrypted - Dumps decrypted mach-o files from encrypted iPhone applications from memory to disk. This tool is necessary for security researchers to be able to look under the hood of encryption.

  -
    ```
    iPod:~ root# DYLD_INSERT_LIBRARIES=dumpdecrypted.dylib
    /var/mobile/Applications/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/Scan.app/Scan
    ```
- class-dump - A command-line utility for examining the Objective-C runtime information stored in Mach-O files.
- dsdump - An improved nm + objc/swift class-dump.
- Weak Classdump - A Cycript script that generates a header file for the class passed to the function. Most useful when you cannot classdump or dumpdecrypted , when binaries are encrypted etc.

  -
    ```
    iPod:~ root# cycript -p Skype weak_classdump.cy; cycript
    -p Skype
    ```

  -
    ```
    #cy weak_classdump_bundle([NSBundle mainBundle],"/tmp/Skype")
    ```

- Fridpa - An automated wrapper script for patching iOS applications (IPA files) and work on non-jailbroken device.
- Frida-iOS-Dump - Pull a decrypted IPA from a jailbroken device.
- bagbak - Yet another frida based iOS dumpdecrypted, supports decrypting app extensions and no SSH required.
- bfinject - bfinject loads arbitrary dylibs into running App Store apps. It has built-in support for decrypting App Store apps, and comes bundled with iSpy and Cycript.
  - A Simple Test
    - `bash bfinject -P Reddit -L test`
  - Decrypt App Store apps
    - `bash bfinject -P Reddit -L decrypt`
  - Cycript
    - `bash bfinject -P Reddit -L cycript`
- HopperApp - Hopper is a reverse engineering tool for OS X and Linux, that lets you disassemble, decompile and debug your 32/64bits Intel Mac, Linux, Windows and iOS executables.
- hopperscripts - Hopperscripts can be used to demangle the Swift function name in HopperApp.
- Radare2 - Radare2 is a unix-like reverse engineering framework and commandline tools.
- XReSign - XReSign allows you to sign or resign unencrypted ipa-files with certificate for which you hold the corresponding private key. Checked for developer, ad-hoc and enterprise distribution.

### Dynamic and Runtime Analysis

- cycript - Cycript allows developers to explore and modify running applications on either iOS or Mac OS X using a hybrid of Objective-C++ and JavaScript syntax through an interactive console that features syntax highlighting and tab completion.
  - Show currently visible view controller
    - `cy# UIApp.keyWindow.rootViewController.visibleViewController`
  - Show view controller at the top of the navigation stack
    - `cy# UIApp.keyWindow.rootViewController.topViewController`
  - Get an array of existing objects of a certain class
    - `cy# choose(UIViewController)`
  - UI Dump,cuts off lots of descriptions of UIViews
    - `cy# [[UIApp keyWindow] _autolayoutTrace].toString()`
  - Skip UIViews and nextResponders to get ViewControllers directly
    - `cy# [[[UIApp keyWindow] rootViewController] _printHierarchy].toString()`
  - List method at runtime
    - `cy# classname.messages` or `cy# function printMethods(className, isa) { var count = new new Type("I"); var classObj = (isa != undefined) ? objc_getClass(className)->isa : objc_getClass(className); var methods = class_copyMethodList(classObj,`

    `count); var methodsArray = []; for(var i = 0; i < *count; i++) { var method = methods[i]; methodsArray.push({selector:method_getN implementation:method_getImplementation(method)}); } free(methods); return methodsArray; }`

  - - `cy# printMethods("<classname>")`
  - Prints out all the instance variables
    - `cy# a=#0x15d0db80`
    - `cy# *a` or
    - `cy# function tryPrintIvars(a){ var x={}; for(i in *a){ try{ x[i] = (*a)[i]; } catch(e){} } return x; }`
    - `cy# a=#0x15d0db80`
    - `cy# tryPrintIvars(a)`
  - Manipulating through property
    - `cy# [a pinCode]`
    - `cy# [a setPinCode: @"1234"]` or `cy# a.setPinCode= @"1234"`
  - Method Swizzling for Instance Method
    - `cy# [a isValidPin]`
    - `cy# <classname>.prototype.isValidPin = function(){return 1;}`
  - Method Swizzling for Class Method
    - `cy# [Pin isValidPin]`
    - `cy# Pin.contructor.prototype.['isValidPin'] = function(){return 1;}`
- iNalyzer - AppSec Labs iNalyzer is a framework for manipulating iOS applications, tampering with parameters and method.
- Grapefruit - Runtime Application Instruments for iOS, previously Passionfruit .
- Introspy-iOS - Blackbox tool to help understand what an iOS application is doing at runtime and assist in the identification of potential security issues.
- Apple configurator 2 - A utility which can be used to view live system log on iDevice.
- keychaindumper - A tool to check which keychain items are available to an attacker once an iOS device has been jailbroken.
- BinaryCookieReader - A tool to dump all the cookies from the binary Cookies.binarycookies file.

### Network Analysis and Server Side Testing

- Mallory - A Man in The Middle Tool (MiTM) that use to monitor and manipulate traffic on mobile devices and applications.
- Burp Suite - Burp Suite is an integrated platform for performing security testing of applications.
- OWASP ZAP - OWASP Zed Attack Proxy Project is an open-source web application security scanner. It is intended to be used by both those new

to application security as well as professional penetration testers.
- Charles Proxy - HTTP proxy / HTTP monitor / Reverse Proxy that enables a developer to view all of the HTTP and SSL / HTTPS traffic between their machine and the Internet.

### Bypassing Root Detection and SSL Pinning

- SSL Kill Switch 2 - Blackbox tool to disable SSL certificate validation - including certificate pinning - within iOS and OS X Apps.
- iOS TrustMe - Disable certificate trust checks on iOS devices.
- tsProtector - Another tool for bypassing Jailbreak detection.
- JailProtect - Apart from bypassing jailbreak detection, it also allows you to spoof your iOS firmware version easily.
- Shadow - Shadow is a tweak to bypass jailbreak detection that defeats basic detection methods used by many App Store apps.
- Frida CodeShare - The Frida CodeShare project is comprised of developers from around the world working together with one goal - push Frida to its limits in new and innovative ways.
  - Bypassing SSL Pinning
    - `frida --codeshare lichao890427/ios-ssl-bypass -f YOUR_BINARY`
    - `frida --codeshare dki/ios10-ssl-bypass -f YOUR_BINARY`

### Security Libraries

- PublicKey Pinning - iOS pinning is performed through a NSURLConnectionDelegate. The delegate must implement connection:canAuthenticateAgainstProtectionSpace: and connection:didReceiveAuthenticationChallenge:. Within connection:didReceiveAuthenticationChallenge:, the delegate must call SecTrustEvaluate to perform customary X509 checks.
- Swiftshield - SwiftShield is a tool that generates irreversible, encrypted names for your iOS project's objects (including your Pods and Storyboards) in order to protect your app from tools that reverse engineer iOS apps, like class-dump and Cycript.
- IOSSecuritySuite - iOS Security Suite is an advanced and easy-to-use platform security & anti-tampering library written in pure Swift! If you are developing for iOS and you want to protect your app according to the OWASP MASVS standard, chapter v8, then this library could save you a lot of time.
- OWASP iMAS - iMAS is a collaborative research project from the MITRE Corporation focused on open source iOS security controls.

### Mobile Penetration Testing Lab

- WaTF Bank - What-a-Terrible-Failure Mobile Banking Application (WaTF-Bank), written in Java, Swift 4, Objective-C and Python (Flask framework) as a backend server, is designed to simulate a "real-world" web services-enabled mobile banking application that contains over 30 vulnerabilities based on OWASP Mobile Top 10 Risks.

- InsecureBankv2 - WThis vulnerable Android application is named “InsecureBankv2” and is made for security enthusiasts and developers to learn the Android insecurities by testing this vulnerable application. Its back-end server component is written in python.
- DVIA-v2 - Damn Vulnerable iOS App (DVIA) is an iOS application that is damn vulnerable. Its main goal is to provide a platform to mobile security enthusiasts/professionals or students to test their iOS penetration testing skills in a legal environment.
- DIVA Android - DIVA (Damn insecure and vulnerable App) is an App intentionally designed to be insecure.The aim of the App is to teach developers/QA/security professionals, flaws that are generally present in the Apps due poor or insecure coding practices.
- DVHMA - Damn Vulnerable Hybrid Mobile App (DVHMA) is an hybrid mobile app (for Android) that intentionally contains vulnerabilities. Its purpose is to enable security professionals to test their tools and techniques legally, help developers better understand the common pitfalls in developing hybrid mobile apps securely.
- MSTG Hacking Playground - This is a collection of iOS and Android mobile apps, that are intentionally build insecure. These apps are used as examples to demonstrate different vulnerabilities explained in the the OWASP Mobile Security Testing Guide.
- UnCrackable Mobile Apps - UnCrackable Apps for Android and iOS, a collection of mobile reverse engineering challenges. These challenges are used as examples throughout the Mobile Security Testing Guide.
- OWASP iGoat - Goat is a learning tool for iOS developers (iPhone, iPad, etc.) and mobile app pentesters. It was inspired by the WebGoat project, and has a similar conceptual flow to it.

### Contribution

Your contributions and suggestions are welcome.

### License