

# MOBILE APP SECURITY RESOURCE KIT

This list has been compiled by Jason Haddix, and is a living document based on current resources & tools for the most secure mobile app development and testing.

## GENERAL RESOURCES

### [OWASP MOBILE TOP 10 RISKS](#)

Results from industry poll on new vulnerability statistics in the field of mobile applications. Representation of the mobile application threat landscape.

### [THE SSL CONSERVATORY](#)

Sample SSL client code for correct endpoint validation.

### [SSL CHECKLIST](#)

List of various SSL/TLS checks that can be performed manually with OpenSSL or a browser.

### [OWASP PROACTIVE CONTROLS](#)

The most important control and control categories that every architect and developer should absolutely, 100% include in every project.

### [OWASP XSECURITY PROJECT](#)

The OWASP XSecurity Project aims to provide the best free security tool integrated with the IDE to assist iOS developers to develop secure iOS apps.

### [OWASP REVERSE ENGINEERING AND CODE MODIFICATION PREVENTION PROJECT](#)

This umbrella project will help you understand the risks of reverse engineering and how to ensure that code cannot be reverse engineered or modified.

### [TUTORIAL: USING CHARLES PROXY WITH YOUR IOS DEVELOPMENT AND HTTP DEBUGGING](#)

Tutorial on how With Charles, you're able to peek into the network requests and responses that your app is making/receiving.

## TOOLS

### [SQLCIPHER](#)

SQLCipher is an open source extension to SQLite that provides transparent 256-bit AES encryption of database files.

### FOR THE IOS DEVELOPER

#### [IOS DEVELOPER CHEAT SHEET](#)

This document is written for iOS app developers and is intended to provide a set of basic pointers to vital aspects of developing secure apps for Apple's iOS operating system following the Owasp Mobile Top Ten List.

#### [APP PROGRAMMING GUIDE FOR IOS](#)

This document highlights the core behaviors that make your app work well on iOS. You might not implement every feature described in this document but you should consider these features for every project you create.

#### [IOS ENCRYPTED CORE DATA GUIDE](#)

Provides a Core Data store that encrypts all data that is persisted. Besides the initial setup, the usage is exactly the same as Core Data and can be used in existing projects that use Core Data.

#### [SECURE CODING PRACTICES FOR IOS DEVELOPMENT](#)

This document concentrates on security vulnerabilities and programming practices of special interest to developers using OS X or iOS.

### FOR THE IOS TESTER

#### [IDB IOS ASSESSMENT TOOL](#)

idb is a tool to simplify some common tasks for iOS pentesting and research.

### [OWASP IOS TESTING CHEAT SHEET](#)

This cheat sheet provides a checklist of tasks to be performed when testing an iOS application taking into account: client software, the communication channel and the server side infrastructure.

### FOR THE ANDROID DEVELOPER

#### [ANDROID: CERT SECURE CODING PRACTICES FOR ANDROID](#)

The following rules and guidelines are specific only to the Android platform that Does not apply to the development of Java or C programs for non-Android platforms.

#### [JSSEC.ORG SECURE ANDROID CODING MANUAL](#)

A collection of tips concerning the know-how of secure designs and secure coding for Android application developers.

#### [ANDROID SECURITY GUIDE](#)

Describe the security features of the Android platform including the security components and considerations of the various levels of the Android software stack.

### FOR THE ANDROID TESTER

#### [ANDROID DEBUG BRIDGE \(ADB\)](#)

How to enable and use ADB, a versatile command line tool that lets you communicate with an emulator instance or connected Android-powered device.

#### [DROZER ANDROID TOOLKIT](#)

The Leading security audit and attack framework for Android.

## SOURCES

