

Category	Checks	Tools
Data Storage	Testing Local data Storage <ul style="list-style-type: none"> - NSUserDefaults - Plist files - CoreData and SQLite files - Keychain - App database 	- SSH tools
	Testing for sensitive data in logs	- Console (Mac OS App)
	Testing Whether Sensitive Data Is Sent to Third Parties	
	Testing for Sensitive Data in the Keyboard Cache	
	Testing for Sensitive Data in the Clipboard	
	Testing for Sensitive Data Disclosure Through the User Interface	
	Testing whether Sensitive Data is exposed via IPC mechanisms	
	Testing for Sensitive Data in Backups	
	Testing For Sensitive Information in Auto-Generated Screenshots	
	URL Caching (HTTP Request and Response) on cache.db	- Any SFTP tool & DB Browser for SQLite
	Testing for Sensitive Data in Memory	- Objection (Memory Dump)
Cryptographic issues	Cryptographic Based Storage Strength	
	Random Number Generation	- MobSF
Local Authentication	Local Authentication Framework	
	Test for secure biometric implementation	- Objection
	Using Keychain Services for Local Authentication	
Network Testing	App Transport Security	- MobSF
	Analyzing the ATS Configuration	- MobSF
	Testing HTTPS – SSL/TLS Security Layer <ul style="list-style-type: none"> - Testing Custom Certificate Stores and Certificate Pinning - Weakness in SSL pinning - Weakness in TLS/SSL 	- MobSF
	Testing Custom URL Schemes	- Burp Suite
API testing	Test for API security issues <ul style="list-style-type: none"> - IDOR - Insecure authentication - Insecure JWT - Weak authorisation 	- Burp Suite
Code Quality and Build Settings	Verifying that the App is Properly Signed	- MobSF
	Testing for Debugging Symbols	
	Testing for Debugging Code and Verbose Error Logging	
	Testing Exception Handling	
	Testing for sensitive info inside application package/code	- Strings - Hopper - IDA Pro - Ghidra
	Verify That Free Security Features Are Activated	

Tampering and Reverse Engineering	Test for Anti-tampering	
iOS Anti-Reversing Defenses	File based checks for Jailbreak Detection	
	Checking File Permissions for jailbreak detection	
	Checking Protocol Handlers	
	Bypassing Jailbreak Detection	
	Device Binding	
App Features	Test for secure deeplink/universal links	
Webview Security	Test for WebView implementations and JavaScript support	
	Exposing External Java Interfaces in WebViews DOM	
Miscellaneous	Testing Open Source Codes or Third Party Libraries	
	Client side injection testing	
	Copy/Paste Buffer Caching	
	Test for sensitive info being saved inside user dictionary cache	
	Test for sensitive info in Heap Memory dump hex	
	Test for buffer overflow attacks	
	Stack/Heap Based Buffer Overflows	
	Object Lifetime Vulnerabilities (Use-after-free, double free's)	
Session Management	Format Strings Vulnerabilities	
	Test for logout functionality and session issues	
	Session sync between devices/applications	