# Final Security Test Specification and Tools Report

| | |
|---|---|
| Mobile Platform | Hybrid Application |
| Application domain type | m-Health |
| Authentication | Yes |
| Authentication schemes | Biometric-based authentication ; ID-based authentication |
| Has DB | Yes |
| Type of database | SQL (Relational Database) |
| Which DB | MySQL |
| Type of information handled | Personal Information ; Confidential Data ; Critical Data |
| Storage Location | Both |
| User Registration | Yes |
| Type of Registration | The users will register themselves |
| Programming Languages | HTML5 + CSS + JavaScript |
| Input Forms | Yes |
| Upload Files | Yes |
| The system has logs | Yes |
| The system has regular updates | Yes |
| The system has third-party | Yes |
| System Cloud Environments | Public Cloud |
| HW Authentication | Basic Authentication (user/pass) |
| HW Wireless Tech | 3G ; 4G/LTE ; 5G ; Bluetooth ; Wi-Fi ; GPS ; NFC |
| Device or Data Center Physical Access | Yes |

In order to avoid or prevent *DoS Jamming, Wi-Fi Jamming, Orbital Jamming, GPS Jamming, Flooding* attacks, the following security tests should be performed.

| Test Parameter | Testing Types | Testing Analysis | Method | Tools | | |
|---|---|---|---|---|---|---|
| | | | | Both | Android | iOS |
| DoS and DDoS Attacks | Black Box | Dynamic Analysis | Penetration Testing | NMAP, SlowBot Net, MetaSploit, LOIC, Kali Linux | | |
| Web Server Authentication | Black Box | Dynamic Analysis | Proxies | Wireshark | tPacketCapturepro | |
| DoS and DDoS Attacks | Grey Box | Static Analysis | Penetration Testing | Cydia Substrate | | Cycript |

In order to avoid or prevent *Malicious Insider, Sniffing, MiTM, Eavesdropping* attacks, the following security tests should be performed.

| Test Parameter | Testing Types | Testing Analysis | Method | Tools | | |
|---|---|---|---|---|---|---|
| | | | | Both | Android | iOS |
| Data leakage and Breach | Grey Box | Dynamic analysis | Proxies | Wireshark | tPacketCapturepro, AFWall+ | |
| | Grey Box | Dynamic Analysis | Penetration Testing | VASTO | | |
| | White Box | Dynamic Analysis | Stressing Testing (fuzzing) | Webfuzz, Wfuzz | | |
| | Grey Box | Dynamic analysis | Vulnerability Scanner | Acunetix, W3af, Nikto, Fortify WebInspect | | |
| | Grey Box | Dynamic Analysis | Penetration Testing | TCPDump, Wireshark | | |
| Secure backup, logging and Insecure Data Storage | Black Box | Dynamic Analysis | Proxies | | adb | |

In order to avoid *MiTM, Eavesdropping, Side-Channel, VM Escape, Wi-Fi SSID Tracking, Rogue Access Point, Cellular Rogue Base Station, Sniffing, Cryptanalysis, Audit Log Manipulation Attacks, Byzantine, On-Off, Brute Force*, the following security tests should be perform.

| Test Parameter | Testing Types | Testing Analysis | Method | Tools | | |
|---|---|---|---|---|---|---|
| | | | | Both | Android | iOS |
| Proper SSL usage and Insecure TLS Protection, Use of encryption | White Box | Static analysis | Forensic Mobile | XRY, UFED Touch, OpenSSL | AndroGuard, MalloDroid, apktool, Amandroid | |
| Interception of network | Grey Box | Hybrid | Penetration Testing | Burp Suite, Wireshark, bettercap | | |
| Interception of network | Black Box | Dynamic Analysis | Proxy | mitm-relay, Kali Linux, Burp Suite | | |
| Poor use of certificate parameters | Black Box | Dynamic analysis | Proxies | NMAP, Nessus, Metasploit Framework | | |

| Test Parameter | Testing Types | Testing Analysis | Method | Both | Android | iOS |
|---|---|---|---|---|---|---|
| Data leakage | Grey Box | Dynamic analysis | Proxies | Wireshark | tPacketCapturepro, AFWall+ | |
| Secure backup, logging and Insecure Data Storage | Grey Box | Dynamic Analysis | Proxies, Penetration Testing | Frida | adb | PassFab iPhone Backup Unlocker |
| Secure backup, logging and Insecure Data Storage | White Box | Dynamic Analysis | Mobile Forensic | | Logcat | |
| Web Server connection | Black Box | Manual Dynamic Analysis | Proxies | OWASP WebScarab, OWASP ZAP, Paros | | |
| Web Server Authentication | Black Box | Dynamic Analysis | Proxies | Wireshark, CERT Tapioca | tPacketCapturepro | |
| Dynamic binary analysis | Black Box | Dinamic Analysis | Penetration Testing | | Introspy-Android | Introspy-iOS |

In order to avoid or prevent *SQLi, XSS, CSRF, SSRF, Command Injection, Code Injection* attacks, the following security tests should be performed.

| Test Parameter | Testing Types | Testing Analysis | Method | Tools Both | Android | iOS |
|---|---|---|---|---|---|---|
| Web Server connection | Black Box | Manual Dynamic Analysis | Proxies | OWASP WebScarab, OWASP ZAP, Paros | | |
| Input Validation | Grey Box | Static Analysis | Forensic Mobile | Bitdefender, Norton, McAfee, Kaspersky | SandDroid | |
| Dynamic binary analysis | Black Box | Dinamic Analysis | Penetration Testing | | Introspy-Android | Introspy-iOS |

In order to avoid *XSS, SQLi, CSRF, Session Fixation, Session Hijacking, Access Point Hijacking, Command Injection, Code Injection, Botnet, Malware as a Service, Spoofing, Pharming, Phishing, GPS Spoofing, Rogue Access Point, Cellular Rogue Base Station and SSRF Attacks*, the following security tests should be perform.

| Test Parameter | Testing Types | Testing Analysis | Method | Tools Both | Android | iOS |
|---|---|---|---|---|---|---|
| Authentication and Authorization | Grey Box | Dynamic analysis | Vulnerability Scanner | OWASP WebScarab, Nikto, Wikto, Paros Proxy, Spike Proxy, OWASP ZAP | | |
| Authentication and Authorization, Access Control | Grey Box | Dynamic Analysis | PenetrationTesting | NMAP, Kali Linux | | |
| Exploit Database Vulnerabilities | White Box | Manual Dynamic Analysis | Penetration Testing | SQLite browser | | Xcode, Xcode Command Line Tools |
| Proper SSL usage and Insecure TLS Protectio, Use of encryption, | Black Box | Dynamic Analysis | Proxies | OWASP WebScarab, OWASP ZAP | | |
| Use of encryption | Grey Box | Dynamic Analysis | Mobile Forensic | | API monitor | |
| Input Validation | Grey Box | Dynamic Analysis | Vulnerability Scanner | Rapid7 Nexpose, Vulnerability Manager Plus | | |
| Find Bugs | White Box | Static Analysis | Bytecode Scanner | bytecode-scanner, QARK | | |
| | White Box | Static Analysis | Source code analyser | PARASOFT C/C++ TEST, RATS, Clang Code Analyze, AndroBugs | Angr | |
| | White Box | Static Analysis | Binary code Scanner | BlackBerry Jarvis, CodeSonar for Binaries, BugScam, SAST | | |
| Input validation of user SID | Grey Box | Manual Dynamic Analysis | Checking input fields in GUI | | | |

In order to avoid or prevent *Malware as a Service, Malicious QR Code, Botnet, Spoofing and Eavesdroping, NFC Payment Replay, Bynzantine, Bluesnarfing, Bluejacking* attacks, the following security tests should be performed.

| Test Parameter | Testing Types | Testing Analysis | Method | Tools Both | Android | iOS |
|---|---|---|---|---|---|---|
| Malware and Privacy Scanners | Grey Box | Static Analysis | Forensic Mobile | Bitdefender, Norton, McAfee, Kaspersky | SandDroid | |

| | | | | Tools | | |
|---|---|---|---|---|---|---|
| | | | | **Both** | **Android** | **iOS** |
| Data Leakage | Black Box | Dinamic Analysis | Proxies | Wireshark | tPacketCapturepro | |
| Authentication and Authorization, Use of Encryption | Black Box | Dinamic Analysis | Proxies | | NFCSpy | |
| Encryption, Authentication and Authorization, Web Server Authentication, Access Control | Black Box | Dinamic Analysis | Penetration Testing | Kali Linux, hcitool | | |

In order to avoid or prevent *Bypassing Physical Security, Physical Theft and VM Migration attacks*, the following security tests should be performed.

| Test Parameter | Testing Types | Testing Analysis | Method | Tools | | |
|---|---|---|---|---|---|---|
| | | | | **Both** | **Android** | **iOS** |
| Data leakage and Breach | White Box | Static Analysis | Forensic Mobile | BlackBag Blacklight, Encase Forensics, Oxygen Forensic Suite | Androguard , Drozer, SpotBugs, Andriller | Elcomsoft iOS Forensic Toolkit |

In order to avoid or prevent *Malware as a Service, Malicious QR Code, Botnets, Spoofing, Eavesdroping, NFC Payment Replay, Bynzantine, Bluesnarfing, Bluejacking, Side-Channel, Flooding attacks*, the following security tests should be performed.

| Test Parameter | Testing Types | Testing Analysis | Method | Tools | | |
|---|---|---|---|---|---|---|
| | | | | **Both** | **Android** | **iOS** |
| Malware and Privacy Scanners | Grey Box | Static Analysis | Forensic Mobile | Bitdefender, Norton, McAfee, Kaspersky | SandDroid | |
| Data Leakage | Black Box | Dinamic Analysis | Proxies | Wireshark | tPacketCapturepro, AFWall+ | |
| Authentication and Authorization, Use of Encryption | Black Box | Dinamic Analysis | Proxies | | NFCSpy | |
| Encryption, Authentication and Authorization, Web Server Authentication, Access Control | Black Box | Dinamic Analysis | Penetration Testing | Kali Linux, hcitool | | |
| Use of encryption, Secure backup, logging and Insecure Data Storage | White Box | Static Analysis | Forensic Mobile | Slueth Kit + Autopsy Browser | AndroGuard, Drozer, apktool, Amandroid | |
| Dynamic binary analysis: debugging, tracing | White Box | Hybrid Analysis | Vulnerability Scanner | RMS | Drozer, Sieve | |
| Secure backup, logging and Insecure Data Storage | Grey Box | Static Analysis | Mobile Forensic | | | iOSbackup |

In order to avoid or prevent *Spoofing, Eavesdropping, Sniffing, Botnets, MiTM, Flooding, Reverse Engineering attacks*, the following security tests should be performed.

| Test Parameter | Testing Types | Testing Analysis | Method | Tools | | |
|---|---|---|---|---|---|---|
| | | | | **Both** | **Android** | **iOS** |
| Mobile decryption, unpacking & conversion | White Box | Static Analysis | Penetration Testing | Ghidra | Dex2jar, JD-GUI, Dextra | Clutch |
| Mobile decryption, unpacking & conversion | Black Box | Static Analysis | Penetration Testing | MobSF | APKEnum | Damn Vulnerable iOS App |
| Secure backup, logging and Insecure Data Storage | Grey Box | Dynamic Analysis | Proxies | | adb | |
| Static binary analysis: disassembly, decompilation | Grey Box | Static Analysis | Manual (Reversed) Code Review | r2ghidra-dec,r2frida, Radare2 | | Hooper |

In order to avoid or prevent *Malware as a Service, Side-Channel and Botnets* attacks, the following security tests should be performed.

| Test Parameter | Testing Types | Testing Analysis | Method | Tools | | |
|---|---|---|---|---|---|---|
| | | | | **Both** | **Android** | **iOS** |

| Test Parameter | Testing Types | Testing Analysis | Method | Both | Tools Android | iOS |
|---|---|---|---|---|---|---|
| Use of encryption, Secure backup, logging and Insecure Data Storage | White Box | Static Analysis | Forensic Mobile | Slueth Kit + Autopsy Browser | AndroGuard, Drozer, apktool, Amandroid | |

In order to avoid or prevent *Phishing, Botnet, Malware as a Service* attacks, the following security tests should be performed.

| Test Parameter | Testing Types | Testing Analysis | Method | Both | Tools Android | iOS |
|---|---|---|---|---|---|---|
| Add-ons | White Box | Static Analysis | Forensic Mobile | | Addons Detector | |

In order to avoid or prevent *Spoofing, Eavesdrooping, Botnets, Flooding* attacks, the following security tests should be performed.

| Test Parameter | Testing Types | Testing Analysis | Method | Both | Tools Android | iOS |
|---|---|---|---|---|---|---|
| Web Server Authentication | Black Box | Dynamic Analysis | Proxies | Wireshark | tPacketCapturepro | |
| DoS and DDoS Attacks | Grey Box | Static Analysis | Penetration Testing | Cydia Substrate | | Cycript |

In order to avoid *SQLi, Command Injection, Session Hijacking, Botnets, AP Hijacking, Brute Force, Phishing, Spoofing, MiTM, Buffer Overflow, Sniffing, CSRF, VM Migration* attacks, the following security tests should be perform.

| Test Parameter | Testing Types | Testing Analysis | Method | Both | Tools Android | iOS |
|---|---|---|---|---|---|---|
| Dynamic binary analysis | Black Box | Dinamic Analysis | Penetration Testing | | Introspy-Android | Introspy-iOS |