

## Final Security Test Specification and Tools Report

Mobile Platform	Web Application
Application domain type	m-Health
Authentication	Yes
Authentication schemes	Biometric-based authentication ; Channel-based authentication ; Factors-based authentication
Has DB	Yes
Type of data storage	Local Storage (Centralized Database)
Which DB	
Type of data stored	Confidential Data ; Critical Data
User Registration	Yes
Type of Registration	The users will register themselves
Programming Languages	Java ; HTML5
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
Hardware Specification	Yes
HW Authentication	Basic Authentication (user/pass)
HW Wireless Tech	3G ; 4G/LTE ; 5G ; Bluetooth ; Wi-Fi ; GPS ; NFC
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	Both	Tools Android	iOS
DoS and DDoS Attacks	Black Box	Dynamic Analysis	Penetration Testing	<a href="#">NMAP</a> , <a href="#">SlowBot Net</a> , <a href="#">MetaSploit</a> , <a href="#">LOIC</a> , <a href="#">Kali Linux</a>		
Web Server Authentication	Black Box	Dynamic Analysis	Proxies	<a href="#">Wireshark</a>	<a href="#">tPacketCapturepro</a>	
DoS and DDoS Attacks	Grey Box	Static Analysis	Penetration Testing	<a href="#">Cydia Substrate</a>		<a href="#">Cycrypt</a>

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	Both	Tools Android	iOS
Data leakage and Breach	Grey Box	Dynamic analysis	Proxies	<a href="#">Wireshark</a>	<a href="#">tPacketCapturepro</a> , <a href="#">AFWall+</a>	
	Grey Box	Dynamic Analysis	Penetration Testing	<a href="#">VASTO</a>		
	White Box	Dynamic Analysis	Stressing Testing (fuzzing)	<a href="#">Webfuzz</a> , <a href="#">Wfuzz</a>		
	Grey Box	Dynamic analysis	Vulnerability Scanner	<a href="#">Acunetix</a> , <a href="#">W3af</a> , <a href="#">Nikto</a> , <a href="#">Fortify</a>		
	Grey Box	Dynamic Analysis	Penetration Testing	<a href="#">WebInspect</a> , <a href="#">TCPDump</a> , <a href="#">Wireshark</a>		
Secure backup, logging and Insecure Data Storage	Black Box	Dynamic Analysis	Proxies		<a href="#">adb</a>	

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 performed.

Test Parameter	Testing Types	Testing Analysis	Method	Both	Tools Android	iOS
Proper SSL usage and Insecure TLS Protection, Use of encryption	White Box	Static analysis	Forensic Mobile	<a href="#">XRY</a> , <a href="#">UFED Touch</a> , <a href="#">OpenSSL</a>	<a href="#">AndroGuard</a> , <a href="#">MalloDroid</a> , <a href="#">apktool</a> , <a href="#">Amandroid</a>	
Interception of network	Grey Box	Hybrid	Penetration Testing	<a href="#">Burp Suite</a> , <a href="#">Wireshark</a> , <a href="#">bettercap</a>		
Interception of network	Black Box	Dynamic Analysis	Proxy	<a href="#">mitm-relay</a> , <a href="#">Kali Linux</a> , <a href="#">Burp Suite</a>		

Poor use of certificate parameters	Black Box	Dynamic analysis	Proxies	<a href="#">NMAP</a> , <a href="#">Nessus</a> , <a href="#">Metasploit Framework</a>		
Data leakage	Grey Box	Dynamic analysis	Proxies	<a href="#">Wireshark</a>	<a href="#">tPacketCapturepro</a> , <a href="#">AFWall+</a>	
Secure backup, logging and Insecure Data Storage	Grey Box	Dynamic Analysis	Proxies, Penetration Testing	<a href="#">Frida</a>	<a href="#">adb</a>	<a href="#">PassFab iPhone Backup Unlocker</a>
Secure backup, logging and Insecure Data Storage	White Box	Dynamic Analysis	Mobile Forensic		<a href="#">Logcat</a>	
Web Server connection	Black Box	Manual Dynamic Analysis	Proxies	<a href="#">OWASP WebScarab</a> , <a href="#">OWASP ZAP</a> , <a href="#">Paros</a>		
Web Server Authentication	Black Box	Dynamic Analysis	Proxies	<a href="#">Wireshark</a> , <a href="#">CERT</a> <a href="#">Tapioca</a>	<a href="#">tPacketCapturepro</a>	
Dynamic binary analysis	Black Box	Dinamic Analysis	Penetration Testing		<a href="#">Introspy-Android</a>	<a href="#">Introspy-iOS</a>

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

Test Parameter	Testing Types	Testing Analysis	Method	Both	Tools Android	iOS
Malware and Privacy Scanners	Grey Box	Static Analysis	Forensic Mobile	<a href="#">Bitdefender</a> , <a href="#">Norton</a> , <a href="#">McAfee</a> , <a href="#">Kaspersky</a>	<a href="#">SandDroid</a>	
Data Leakage	Black Box	Dinamic Analysis	Proxies	<a href="#">Wireshark</a>	<a href="#">tPacketCapturepro</a>	
Authentication and Authorization, Use of Encryption	Black Box	Dinamic Analysis	Proxies		<a href="#">NFCSpy</a>	
Encryption, Authentication and Authorization, Web Server Authentication, Access Control	Black Box	Dinamic Analysis	Penetration Testing	<a href="#">Kali Linux</a> , <a href="#">hctool</a>		

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	Both	Tools Android	iOS
Data leakage and Breach	White Box	Static Analysis	Forensic Mobile	<a href="#">BlackBag Blacklight</a> , <a href="#">Encase Forensics</a> , <a href="#">Oxygen Forensic Suite</a>	<a href="#">Androguard</a> , <a href="#">Drozer</a> , <a href="#">SpotBugs</a> , <a href="#">Andriller</a>	<a href="#">Elcomsoft iOS Forensic Toolkit</a>

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

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

Secure backup, logging and Insecure Data Storage	Grey Box	Static Analysis	Mobile Forensic			<a href="#">iOSbackup</a>
--	----------	-----------------	-----------------	--	--	---------------------------

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

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	Both	Tools Android	iOS
Use of encryption, Secure backup, logging and Insecure Data Storage	White Box	Static Analysis	Forensic Mobile	<a href="#">Slueth Kit + Autopsy Browser</a>	<a href="#">AndroGuard</a> , <a href="#">Drozer</a> , <a href="#">apktool</a> , <a href="#">Amandroid</a>	

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		<a href="#">Addons Detector</a>	

In order to avoid or prevent *Spoofing, Eavesdropping, 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	<a href="#">Wireshark</a>	<a href="#">tPacketCapturepro</a>	
DoS and DDoS Attacks	Grey Box	Static Analysis	Penetration Testing	<a href="#">Cydia Substrate</a>		<a href="#">Cycrypt</a>

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		<a href="#">Introspy-Android</a>	<a href="#">Introspy-iOS</a>