Final Security Test Specification and Tools Report

Mobile Platform	Hybrid Application
Application domain type	m-Payment
Authentication	Yes
Authentication schemes	Biometric-based authentication ; Factors-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
User Registration	Yes
Type of Registration	The users will register themselves
Programming Languages	HTML5 ; 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	Community Cloud
Hardware Specification	Yes
HW Authentication	Basic Authentication (user/pass)
HW Wireless Tech	3G ; 4G/LTE ; 5G ; Bluetooth ; Wi-Fi ; GPS ; NFC
Data Center Phisical 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 *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 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	
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 Enginnering 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
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		Tools	
				Both	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		Tools	
				Both	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**		**Tools**	
				Both	**Android**	**iOS**
Dynamic binary analysis	Black Box	Dinamic Analysis	Penetration Testing		Introspy-Android	Introspy-iOS