Final Security Test Specification and Tools Report

Architeture	Web Application
Application domain type	m-Payment
Authentication	Username and Password
Has DB	Yes
Type of data storage	SQL
Which DB	MySQL
Type of data stored	Personal Information ; Confidential Data ; Critical Data
User Registration	Yes
Type of Registration	The users will register themselves
Programming Languages	HTML5 ; Javascript ; PHP
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 Phisical Access	Yes

In order to avoid or prevent *Botnet, DoS and DDoS Attacks*, the following security tests should be performed.

Test Parameter	Testing Types	Testing Methods	Tools
Add-ons	White Box	Static Analysis via Forensic Mobile	Addons Detecto
DoS, DDoS Attacks	Black Box	Dinamic Analysis via Penetration Test	NMAP, SlowBot Net, MetaSploi LOIC and Kali Linux

In order to avoid or prevent *Botnet, DoS, DDoS, Phishing, MITM, Spoofing and Sniffing Attacks*, the following security tests should be performed.

Test Parameter	Testing Types	Testing Methods	Tools

Mobile decryption, unpacking & conversion	White Box	Static Analysis via Test Penetration	Dex2jar	Ex2jar
Secure backup and logging	Grey Box	Dinamica Analysis via Proxies	adb	
Data leakage and Breach	Grey Box	Dinamic analysis via Proxies	tPacket Wireshar AFWall+	
	Grey Box	Dinamic Analysis via Penetration Testing	VASTO	
	White Box	Dnamic Analysis via Stressing Testing (fuzzing)	Webfuzz, SPI Fuzzer, Wfuzz	

In order to avoid or prevent *Sniffing, Botnet, Phishing and Spoofing Attacks*, the following security tests should be performed.

Test Parameter	Testing Types	Testing Methods	Tools	
			Ba	**Bo**
Use of encryption	White Box	Static Analysis via Forensic Mobile	OpenSSL	

Poor use of certificate parameters	Grey Box	Dinamic analysis via Vulnerability Scanner	Acunetix, Web3af, Nikto, IBM Security AppScan Standard and HP WebInsp
	Grey Box	Dinamic Analysis via Penetration Test	TCPdu Wiresh tcpdum
Secure backup and logging	Black Box	Dinamic Analysis via Proxies	adb

In order to avoid or prevent *Botnet, Spoofing and Sniffing attacks*, the following security tests should be performed.

Test Parameter	Testing Types	Testing Methods	Tools		
Exploit Database Vulnerabilities	White Box	Manual Dinamic Analysis via Penetration Test	SQLite browser	Xcode	
Proper SSL usage and Use of encryption	Black Box	Dinamic Analysis via Proxies	WebScar		

Database framework scanner	Grey Box	Dinamic Analisys via Vulnerability Scanner	Database Scanner of Internet Security Systems Co. and MetaCort
Find Bugs	White Box	Static Analysis via Bytecode Scanner	FindBugs BugScan of LogicLab Co.
	White Box	Static Analysis via source code Analyser	C++Test, RATS, C Code Analyzer(
	White Box	Static Analysis via Binary code Scanner	BugScan of Logi-cLab Co. and Fx-Cop;Bug
Input validation of user SID	Grey Box	Manual Dinamic Analysis Checking input fields in GUI	

Test Parameter	Testing Types	Testing Methods	Tools		
			Both		Android

Runtime manipulation: code injection, patching	Grey Box	Static Analysis via Test Penetration	Cydia Substrate		Cycript

In order to avoid or prevent *Malicious Insider and VM-Migration attacks*, the following security tests should be performed.

Test Parameter	**Testing Types**	**Testing Methods**	**Tools**		
			Both	**Android**	**iOS**
Input validation	Grey Box	Static Analysis via Forensic Mobile	Slueth Kit+Autopsy Browser	AndroGuard, Drozer, apktool, Amandroid	

In order to avoid or prevent *Malware injection and Side-channel Attacks*, the following security tests should be performed.

Test Parameter	**Testing Types**	**Testing Methods**	**Tools**	
			Both	**Android** **iOS**
Debug flag	White Box	Static Analysis via Forensic Mobile	BlackBag Blacklight, Encase forensics	AndroG Drozer, FindBug Andrille
Content providers	White Box	Static Analysis via Forensic Mobile	Slueth Kit+Autopsy Browser	AndroG Drozer, apktool
Code quality	White Box	Static Analysis via Byte- code Scanner	FindBugs, BugScan of LogicLab Co.	
	White Box	Static Analysis via source code Analyser	C++Test, RATS, C Code Analyzer(CCA)	
	White Box	Static Analysis via source code Analyser	BugScan of LogicLab Co. and Fx- Cop, BugScam	class-

In order to avoid or prevent *physical attacks*, the following security tests should be performed.

Test Parameter	**Test Approach**	Test Method	Tools		
			Bel	iOS	Android
Debug flag, Content providers, Code quality	White Box	Static Analysis via Forensic Mobile			AndroG Drozer, FindBug
Leak, Breach and data Loss	Black Box	Manual Dinamic Analysis Checking input fields from device and GUI			