Final Security Test Specification and Tools Report

Mobile Plataform	Web Application
Application domain type	m-Health
Authentication	Yes
Authentication schemes	Biometric-based authentication ; Factors-based authentication
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 ; PHP ; 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	Private Cloud
Hardware Specification	Yes
HW Authentication	Basic Authentication (user/pass)
HW Wireless Tech	3G ; 4G/LTE ; 5G ; Wi-Fi ; GPS
Data Center Phisical Access	Yes

In order to avoid or prevent *SQLi, XSS, Spoofing and CSRF attacks*, the following security tests should be performed.

Test Parameter	Testing Types	Testing Methods	Tools		
			Both	**Android**	**iOS**
Authentication and Authorization	Grey Box	Dinamic analysis via Vulnerability Scanner	OWASP WebScarab, OWASP Berretta, Nikto, Wikto, Paros Proxy, Spike Proxy, EOR, Pantera		
Access Control	Grey Box	Dinamic Analysis via Penetration Test	NMAP and Kali Linux		

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		
			Both	**Android**	**iOS**
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	WebScarab		
Database frangibility scanner	Grey Box	Dinamic Analisys via Vulnerability Scanner	Database Scanner of Internet Security Systems Co. and MetaCortex		
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(CCA)		
	White Box	Static Analysis via Binary code Scanner	BugScan of Logi- cLab Co. and Fx- Cop;BugScam		
Input validation of user SID	Grey Box	Manual Dinamic Analysis Checking input fields in GUI			
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 Browser	Slueth Kit+Autopsy	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	AndroGuard, Drozer, FindBugs, Andriller	
Content providers	White Box	Static Analysis via Forensic Mobile	Slueth Kit+Autopsy Browser	AndroGuard, 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-dump-z

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

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