

Final Security Test Specification and Tools Report

Mobile Plataform	Web Application ; Hybrid Application
Application domain type	m-Health
Authentication	Yes
	Biometric-based authentication ; Channel-based authentication ; Factors-based authentication
Authentication schemes	Yes
Has DB	SQL
Type of data storage	MySQL
Which DB	Personal Information ; Confidential Data ; Critical Data
Type of data stored	Yes
User Registration	The users will register themselves
Type of Registration	HTML5 ; PHP
Programming Languages	Yes
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	5G ; 3G ; 4G/LTE ; Wi-Fi ; Bluetooth
Data Center Phisical Access	Yes
Mobile Plataform	Web Application ; Hybrid Application
Application domain type	m-Health
Authentication	Yes
	Biometric-based authentication ; Channel-based authentication ; Factors-based authentication
Authentication schemes	Yes
Has DB	SQL
Type of data storage	MySQL
Which DB	Personal Information ; Confidential Data ; Critical Data
Type of data stored	Yes
User Registration	The users will register themselves
Type of Registration	HTML5 ; PHP
Programming Languages	Yes
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	5G ; 3G ; 4G/LTE ; Wi-Fi ; Bluetooth
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		
			Both	Android	iOS
Add-ons	White Box	Static Analysis via Forensic Mobile		Addons Detector	
DoS, DDoS Attacks	Black Box	Dinamic Analysis via Penetration Test	NMAP, SlowBot Net, MetaSploit, 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		
			Both	Android	iOS
Mobile decryption, unpacking & conversion	White Box	Static Analysis via Test Penetration		Dex2jar	Clutch
Secure backup and logging	Grey Box	Dinamica Analysis via Proxies		adb	
Data leakage and Breach	Grey Box	Dinamic analysis via Proxies	Wireshark	tPacketCapturepro, AFWall+,	
	Grey Box	Dinamic Analysis via Penetration Testing	VASTO		

White Box

Dnamic Analysis via
Stressing Testing (fuzzing) Wfuzz

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	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 *Sniffing, Botnet, Phishing and Spoofing Attacks*, the following security tests should be performed.

Test Parameter	Testing Types	Testing Methods	Tools	
			Both	iOS
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 WebInspect	
	Grey Box	Dinamic Analysis via Penetration Test	TCPDump, Wireshak	idb tool
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	
			Both	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	Cycrypt

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	iOS
Input validation	Grey Box	Static Analysis via Forensic Mobile	Slueth Kit+Autopsy Browser	
			Android	
			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	iOS
Debug flag	White Box	Static Analysis via Forensic Mobile	BlackBag Blacklight, Encase forensics	
Content providers	White Box	Static Analysis via Forensic Mobile	Slueth Kit+Autopsy Browser	
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	Both	Tools	
Debug flag, Content providers, Code quality	White Box	Static Analysis via Forensic Mobile		Android AndroGuard, Drozer, FindBugs	iOS
Leak, Breach and data Loss	Black Box	Manual Dinamic Analysis Checking input fields from device and GUI			