Final Security Test Specification and Tools Report

Architecture Hybrid Application
Application domain type m-Health

Authentication Username and Password

Has DBYesType of data storageSQLWhich DBMySQL

Type of data stored Personal Information; Confidential Data; Critical Data

User Registration Y

Type of Registration The users will register themselves
Programming Languages HTML5 ; Javascript ; PHP

Input FormsYesUpload FilesYesThe system has logsYesThe system has regular updatesYesThe system has third-partyYesSystem Cloud EnvironmentsPublic Cloud

Hardware Specification Yes

HW Authentication Basic Authentication (user/pass)
HW Wireless Tech 3G : 4G/LTE : 5G : Bluetooth : W

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		
	Testing Types	Both	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 Kal Linux	i		

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,	White Box	Static Analysis via Test		Dex2jar	Clutch
unpacking & conversion	Willie DOX	Penetration		Dexzjai	Oluton
Secure backup and	Grey Box	Dinamica Analysis via	adb	adh	
logging	Gley Box	Proxies		aub	
Data leakage and Breach	Grov Pov	Dinamic analysis via	Wireshark	tPacketCapturepro,	
Data leakage and breach	Gley Box	Proxies	Wileshark	AFWall+,	
	Grey Box Dinamic Analysis via VASTO	VASTO			
ŕ	Gley Box	Penetration Testing	VASTO		
	White Box	Dnamic Analysis via	Webfuzz, SPI Fuzzer,		
		Stressing Testing (fuzzing	g) Wfuzz		

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

Test Parameter	Tooting Types	Teeting Methods				
	Testing Types	Testing Methods	Both	Android	iOS	
			OWASP WebScara	ab,		
Authentication and	Cray Day	Dinamic analysis via	OWASP Berretta, I	Nikto,		
Authorization	Grey Box	Vulnerability Scanner	Scanner Wikto, Paros Proxy, Spike			
			Proxy, EOR, Pante	era		
Access Control	Crov Boy	Dinamic Analysis via	NIMAD and Kali Lin			
Access Control	Grey Box	Penetration Test	NMAP and Kali Lin	ux		

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	
rest Farameter	resuing Types	resuling Methods	Both	Android	iOS
Use of encryption	White Box	Static Analysis via Forensic Mobile	OpenSSL		
			Acunetix, Web3af, Nikto,		
Poor use of certificate	Grev Box	Dinamic analysis via	IBM Security AppScan		
parameters	Gley box	Vulnerability Scanner	Standard and HP		
			WebInspect		

	Grev Box	Dinamic Analysis via	TCPDump, Wireshak	idb tool
	Gley Box	Penetration Test	repump, wheshak	lub tool
Secure backup and	Plack Pay	Dinamic Analysis via	adb	
logging	Black Box	Provine	aub	

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				
rest Farailletei	resuing rypes	resting wethous	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	Tooting Types	Testing Methods		Tools	
	Testing Types	resumg weutous	Both	Android	iOS
Input validation	Grev Box	Static Analysis via	Slueth Kit+Autopsy	AndroGuard, Drozer,	
	Gley box	Forensic Mobile	Browser	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	BlackBag Blacklight,	AndroGuard, Drozer,		
		Forensic Mobile	Encase forensics	FindBugs, Andriller		
Content providers	White Box	Static Analysis via	Slueth Kit+Autopsy	AndroGuard, Drozer,		
		Forensic Mobile	Browser	apktool		
Code suglitu	White Box	Static Analysis via Byte-	FindBugs, BugScan of			
Code quality		code Scanner	LogicLab Co.			
	White Box	Static Analysis via source	C++Test, RATS, C Code			
		code Analyser	Analyzer(CCA)			
White	Mile it - Day	Static Analysis via source	BugScan of LogicLab Co.		-1	
	White Box code Analyser	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 Method		Tools		
	Test Approach		Both	Android	iOS
Debug flag, Content	White Box	Static Analysis via		AndroGuard, Drozer,	
providers, Code quality	Write Box	Forensic Mobile		FindBugs	
Leak, Breach and data		Manual Dinamic Analysis	;		
Loss	Black Box	Checking input fields fror	n		
		device and GUI			