Final Security Test Specification and Tools Report

Mobile Plataform Web Application; Hybrid Application

m-Health Application domain type Yes Authentication

Biometric-based authentication; Channel-based authentication; Factors-based Authentication schemes

Has DB Yes Type of data storage SQL Which DB MySQL

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

User Registration

Type of Registration The users will register themselves

HTML5; PHP **Programming Languages**

Input Forms Yes Upload Files Yes The system has logs Yes The system has regular updates Yes The system has third-party Yes Public Cloud System Cloud Environments Hardware Specification Yes

HW Authentication Basic Authentication (user/pass) **HW Wireless Tech** 5G; 3G; 4G/LTE; Wi-Fi; Bluetooth

Data Center Phisical Access

Mobile Plataform Web Application; Hybrid Application

Application domain type m-Health Authentication Yes

Biometric-based authentication; Channel-based authentication; Factors-based Authentication schemes

authentication

Has DB Yes Type of data storage SQL Which DB MySQL

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

User Registration

Type of Registration The users will register themselves

Programming Languages HTML5; PHP

Input Forms Yes Upload Files Yes The system has logs Yes The system has regular updates Yes The system has third-party Yes Public Cloud System Cloud Environments Hardware Specification

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 | | |
|-------------------|---------------|--|---|-----------------|-----|
| | resting types | | 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 | Teeting Types | Testing Methods | | Tools | | |
|---|---------------|---|-----------|--------------------------------|--------|--|
| | Testing Types | Testing Methods | 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 Webfuzz, SPI Fuzzer, 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 | Android | iOS |
| | | | OWASP WebScarab, | | |
| Authentication and Authorization | Grey Box | Dinamic analysis via | inamic analysis via OWASP Berretta, Nikto, | | |
| | | Vulnerability Scanner | Wikto, Paros Proxy, Spik | e | |
| | | | Proxy, EOR, Pantera | | |
| Access Control | Cray Bay | Dinamic Analysis via | NMAP and Kali Linux | | |
| | Grey Box | Penetration Test | NIVIAP and Kall Linux | | |

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

| Test Parameter | Tooting Types | Teeting Methods | | Tools | |
|-------------------------|----------------------|--|--------------------------|---------|----------|
| | Testing Types | Testing Methods | Both | Android | iOS |
| Use of encryption | White Box | Static Analysis via Forensic Mobile | OpenSSL | | |
| | | | Acunetix, Web3af, Nikto, | | |
| Poor use of certificate | ertificate Grey Box | Dinamic analysis via | IBM Security AppScan | | |
| parameters | | Vulnerability Scanner Standard and HP | | | |
| | | | WebInspect | | |
| | Crov Boy | Dinamic Analysis via | TODD: Wins als als | | idb tool |
| | Grey Box | Penetration Test | TCPDump, Wireshak | | 1001 |
| Secure backup and | Black Box | Dinamic Analysis via | is via | | |
| logging | | 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 | | |
|--|---------------|--|--|---------|---------|
| rest rarameter | resting Types | | 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 | | |
|------------------|---------------|--|-------------------------------|--|-----|--|
| | resulig Types | resuing Methods | Both An | 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 | BlackBag Blacklight, | AndroGuard, Drozer, | |
| Debug liag | | Forensic Mobile | Encase forensics | FindBugs, Andriller | |
| Content providers | White Box | Static Analysis via | Slueth Kit+Autopsy | AndroGuard, Drozer, | |
| Content providers | | Forensic Mobile | Browser | apktool | |
| Code quality | 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 | | |
| | white Box | code Analyser | Analyzer(CCA) | | |

White Box

Static Analysis via source BugScan of LogicLab Co. code Analyser and Fx- Cop, BugScam

class-dump-z

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

| | Tost Mothod | | Tools | | |
|---------------|----------------------------|--|--|--|--|
| Test Approach | rest Method | Both | Android | iOS | |
| White Poy | Static Analysis via | | AndroGuard, Drozer, | | |
| white Box | Forensic Mobile | | FindBugs | | |
| | Manual Dinamic Analysis | | | | |
| Black Box | Checking input fields from | | | | |
| | device and GUI | | | | |
| | White Box | White Box Static Analysis via Forensic Mobile Manual Dinamic Analysis Black Box Checking input fields from | Test Approach White Box Static Analysis via Forensic Mobile Manual Dinamic Analysis Black Box Checking input fields from | Test Approach White Box Static Analysis via Forensic Mobile Manual Dinamic Analysis Black Box Test Method Both Android AndroGuard, Drozer, FindBugs FindBugs Checking input fields from | |