



Accurate Detection. Real Time Response. Faster Recovery.

Planned list of Activities And Validation Process For Execution of VAPT

**STRYKER, INDIA**



April 11th, 2022



**Planned list of Activities and Validation Process for Execution of VAPT**

Warning: THIS DOCUMENT MAY CONTAIN INFORMATION THAT COULD SEVERELY DAMAGE OR IMPACT THE INTEGRITY AND SECURITY OF THE ORGANIZATION IF DISCLOSED PUBLICLY. THIS DOCUMENT SHOULD BE SAFEGUARDED AT ALL TIMES AND MAINTAINED IN A SECURE AREA WHEN NOT IN USE. G’ SECURE LABS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR THE SECURITY OF THIS DOCUMENT AFTER DELIVERY TO THE ORGANIZATION NAMED HEREIN. IT IS THE ORGANIZATION’S RESPONSIBILITY TO SAFEGUARD THIS MATERIAL AFTER DELIVERY.

THIS REPORT CONTAINS PROPRIETARY INFORMATION THAT IS NOT TO BE SHARED, COPIED, DISCLOSED OR OTHERWISE DIVULGED WITHOUT THE EXPRESS WRITTEN CONSENT OF G’ SECURE LABS OR THEIR DESIGNATED REPRESENTATIVE. USE OF THIS REPORTING FORMAT BY OTHER THAN G’ SECURE LABS OR ITS SUBSIDIARIES IS STRICTLY PROHIBITED AND MAY BE PROSECUTED TO THE FULLEST EXTENT OF THE LAW.

Disclaimer: THE RECOMMENDATIONS CONTAINED IN THIS REPORT ARE BASED ON INDUSTRY STANDARD “BEST PRACTICES”. BEST PRACTICES ARE, BY NECESSITY, GENERIC IN NATURE AND MAY NOT TAKE INTO ACCOUNT EXACERBATING OR MITIGATING CIRCUMSTANCES. THESE RECOMMENDATIONS, EVEN IF CORRECTLY APPLIED, MAY CAUSE CONFLICTS IN THE OPERATING SYSTEM OR INSTALLED APPLICATIONS. ANY RECOMMENDED CHANGES TO THE OPERATING SYSTEM OR INSTALLED APPLICATION SHOULD FIRST BE EVALUATED IN A NON-PRODUCTION ENVIRONMENT BEFORE BEING DEPLOYED IN THE PRODUCTION ENVIRONMENT.

**G’ Secure Labs**

WWW.GSECURELABS.COM



**Recipient:**

|  |  |
| --- | --- |
| Name/role | Company |
| Deepak | Stryker |

**Document Version:**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of the Author | Version | Title | Date |
| Arunesh Mishra | 1.0 | Planned list of Activities And Validation Process For Execution of VAPT | April 7th, 2022 |
| Arunesh Mishra | 2.0 | Planned list of Activities And Validation Process For Execution of VAPT | April 11th, 2022 |



Table of Contents

[1. Summary 5](#_Toc101206334)

[2. Planned List of Activities and Validation Process 5](#_Toc101206335)

**3. Requirements- Test Cases ……….………………………………………………………………………………………….……………..45**

# Summary

Stryker has assigned the task of carrying out vulnerability assessment and penetration testing of their SmartMedic Platform by G’Secure Labs team. This is planned list of activities and validation process for execution of VAPT task. The version 1.0 detailed planned list of activities described about each validation process task.

# Planned List of Activities and Validation Process

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat Event(s)** | **Vulnerabilities** | **Asset** | **TC No.** | **Planned list of Activities And Validation Process For Execution of VAPT** |
| Deliver undirected malware (CAPEC-185) | Unprotected external USB Port on the tablet/devices. | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | ST No.- 01 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Unprotected external USB Port on the tablet/devices. | Smart medic (Stryker device) System Component | TC No.- 02 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device. | Smart medic (Stryker device) System Component | TC No.- 03 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device. | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 04 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Legacy system identification if any | Smart medic (Stryker device) System Component | TC No.- 05 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Legacy system identification if any | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 06 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Ineffective patch management of firware, OS and applications thoughout the information system plan | Device Maintainence tool (Hardware/Software) | TC No.- 07 | NA |
| Deliver undirected malware (CAPEC-185) | Ineffective patch management of firware, OS and applications thoughout the information system plan | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 08 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Ineffective patch management of firware, OS and applications thoughout the information system plan | Smart medic (Stryker device) System Component | TC No.- 09 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Lack of plan for periodic Software Vulnerability Management | Device Maintainence tool (Hardware/Software) | TC No.- 10 | NA |
| Deliver undirected malware (CAPEC-185) | Lack of plan for periodic Software Vulnerability Management | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 11 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Lack of plan for periodic Software Vulnerability Management | Smart medic (Stryker device) System Component | TC No.- 12 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Unprotected network port(s) on network devices and connection points | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 13 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Unprotected network port(s) on network devices and connection points | Smart medic (Stryker device) System Component | TC No.- 14 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Unencrypted data at rest in all possible locations | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 15 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data at motion and MITM |
| Deliver undirected malware (CAPEC-185) | Unencrypted data in flight in all flowchannels | Smart medic (Stryker device) System Component | TC No.- 16 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Unencrypted data in flight in all flowchannels | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 17 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Outdated - Software/Hardware | Device Maintainence tool (Hardware/Software) | TC No.- 18 | NA |
| Deliver undirected malware (CAPEC-185) | Outdated - Software/Hardware | Smart medic (Stryker device) System Component | TC No.- 19 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver undirected malware (CAPEC-185) | Outdated - Software/Hardware | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 20 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers | Device Maintainence tool (Hardware/Software) | TC No.- 21 | NA |
| Deliver directed malware (CAPEC-185) | InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers | Smart medic (Stryker device) System Component | TC No.- 22 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 23 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | Unprotected external USB Port on the tablet/devices. | Wireless Network device | TC No.- 24 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering.  8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | Unprotected external USB Port on the tablet/devices. | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 25 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | Unprotected external USB Port on the tablet/devices. | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 26 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Deliver directed malware (CAPEC-185) | External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device. | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 27 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | Ineffective patch management of firware, OS and applications thoughout the information system plan | Device Maintainence tool (Hardware/Software) | TC No.- 28 | NA |
| Deliver directed malware (CAPEC-185) | Ineffective patch management of firware, OS and applications thoughout the information system plan | Smart medic (Stryker device) System Component | TC No.- 29 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | Ineffective patch management of firware, OS and applications thoughout the information system plan | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 30 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | Unprotected network port(s) on network devices and connection points | Smart medic (Stryker device) System Component | TC No.- 31 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | Unprotected network port(s) on network devices and connection points | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 32 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | Unprotected network port(s) on network devices and connection points | Wireless Network device | TC No.- 33 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering.  8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 34 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Deliver directed malware (CAPEC-185) | InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 35 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Deliver directed malware (CAPEC-185) | Unencrypted data at rest in all possible locations | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 36 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data at motion and MITM |
| Deliver directed malware (CAPEC-185) | Unencrypted data at rest in all possible locations | Tablet OS/network details & Tablet Application | TC No.- 37 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data at motion and MITM |
| Deliver directed malware (CAPEC-185) | Unencrypted data at rest in all possible locations | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 38 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Use sniffing tool to sniff the data at motion and MITM |
| Gaining Access ([S]TRID[E]) | Unprotected network port(s) on network devices and connection points | Tablet OS/network details & Tablet Application | TC No.- 39 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Gaining Access ([S]TRID[E]) | Unprotected network port(s) on network devices and connection points | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 40 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | Unprotected network port(s) on network devices and connection points | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 41 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Gaining Access ([S]TRID[E]) | Devices with default passwords needs to be checked for bruteforce attacks | Authenication/Authorisation data | TC No.- 42 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Gaining Access ([S]TRID[E]) | Devices with default passwords needs to be checked for bruteforce attacks | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 43 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | Devices with default passwords needs to be checked for bruteforce attacks | Interface/API Communication | TC No.- 44 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Authenication/Authorisation data | TC No.- 45 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Gaining Access ([S]TRID[E]) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 46 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Smart medic app (Azure Portal Administrator) | TC No.- 47 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | Checking authentication modes for possible hacks and bypasses | Authenication/Authorisation data | TC No.- 48 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Gaining Access ([S]TRID[E]) | Checking authentication modes for possible hacks and bypasses | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 49 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | Checking authentication modes for possible hacks and bypasses | Smart medic app (Azure Portal Administrator) | TC No.- 50 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | Controlled Use of Administrative Privileges over the network | Authenication/Authorisation data | TC No.- 51 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Gaining Access ([S]TRID[E]) | Controlled Use of Administrative Privileges over the network | Smart medic app (Azure Portal Administrator) | TC No.- 52 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | Unprotected external USB Port on the tablet/devices. | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 53 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Maintaining Access (TTP) | Devices with default passwords needs to be checked for bruteforce attacks | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 54 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Maintaining Access (TTP) | Devices with default passwords needs to be checked for bruteforce attacks | Smart medic app (Azure Portal Administrator) | TC No.- 55 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Maintaining Access (TTP) | Devices with default passwords needs to be checked for bruteforce attacks | Authenication/Authorisation data | TC No.- 56 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Maintaining Access (TTP) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 57 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Maintaining Access (TTP) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Smart medic app (Azure Portal Administrator) | TC No.- 58 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Maintaining Access (TTP) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Authenication/Authorisation data | TC No.- 59 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Maintaining Access (TTP) | Checking authentication modes for possible hacks and bypasses | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 60 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Maintaining Access (TTP) | Checking authentication modes for possible hacks and bypasses | Smart medic app (Azure Portal Administrator) | TC No.- 61 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Maintaining Access (TTP) | Controlled Use of Administrative Privileges over the network | Smart medic app (Azure Portal Administrator) | TC No.- 62 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Maintaining Access (TTP) | Controlled Use of Administrative Privileges over the network | Authenication/Authorisation data | TC No.- 63 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Clearing Track (TTP) | InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 64 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Clearing Track (TTP) | InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 65 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Clearing Track (TTP) | Outdated - Software/Hardware | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 66 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Clearing Track (TTP) | Lack of configuration controls for IT assets in the informaion system plan | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 67 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Clearing Track (TTP) | Lack of configuration controls for IT assets in the informaion system plan | Device Maintainence tool (Hardware/Software) | TC No.- 68 | NA |
| Clearing Track (TTP) | Ineffective patch management of firware, OS and applications thoughout the information system plan | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 69 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Clearing Track (TTP) | Ineffective patch management of firware, OS and applications thoughout the information system plan | Device Maintainence tool (Hardware/Software) | TC No.- 70 | NA |
| Clearing Track (TTP) | Ineffective patch management of firware, OS and applications thoughout the information system plan | Tablet OS/network details & Tablet Application | TC No.- 71 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Clearing Track (TTP) | The static connection digaram between devices and applications with provision for periodic updation as per changes | Device Maintainence tool (Hardware/Software) | TC No.- 72 | NA |
| Clearing Track (TTP) | The static connection digaram between devices and applications with provision for periodic updation as per changes | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 73 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Elevation of privilege (STRID[E]) | Controlled Use of Administrative Privileges over the network | Authenication/Authorisation data | TC No.- 74 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Elevation of privilege (STRID[E]) | Controlled Use of Administrative Privileges over the network | Smart medic app (Azure Portal Administrator) | TC No.- 75 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Denial of service (STRI(D)E) | Unprotected network port(s) on network devices and connection points | Wireless Network device | TC No.- 76 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering.  8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools. |
| Denial of service (STRI(D)E) | Unprotected network port(s) on network devices and connection points | Tablet OS/network details & Tablet Application | TC No.- 77 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Information disclosure (STR(I)DE) | Unencrypted data at rest in all possible locations | Data at Rest | TC No.- 78 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM 8) Use sniffing tool to sniff the data at motion and MITM |
| Information disclosure (STR(I)DE) | Unencrypted data in flight in all flowchannels | Data in Motion | TC No.- 79 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Information disclosure (STR(I)DE) | Weak Encryption Implementaion in data at rest and in motion tactical and design wise | Data at Rest | TC No.- 80 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Information disclosure (STR(I)DE) | Weak Encryption Implementaion in data at rest and in motion tactical and design wise | Data in Motion | TC No.- 81 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Information disclosure (STR(I)DE) | Weak Algorthim implementation with respect cipher key size | Data at Rest | TC No.- 82 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Information disclosure (STR(I)DE) | Weak Algorthim implementation with respect cipher key size | Data in Motion | TC No.- 83 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Information disclosure (STR(I)DE) | InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 84 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Information disclosure (STR(I)DE) | Unencrypted Network segment throught the information flow | Data in Motion | TC No.- 85 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Information disclosure (STR(I)DE) | Insecure communications in networks (hospital) | Data in Motion | TC No.- 86 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Data Access (STR[I]DE) | Unprotected network port(s) on network devices and connection points | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 87 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Data Access (STR[I]DE) | Unprotected network port(s) on network devices and connection points | Wireless Network device | TC No.- 88 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering.  8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools. |
| Data Access (STR[I]DE) | Unprotected network port(s) on network devices and connection points | Tablet OS/network details & Tablet Application | TC No.- 89 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Data Access (STR[I]DE) | Devices with default passwords needs to be checked for bruteforce attacks | Data at Rest | TC No.- 90 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Data Access (STR[I]DE) | Devices with default passwords needs to be checked for bruteforce attacks | Authenication/Authorisation data | TC No.- 91 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Data Access (STR[I]DE) | Devices with default passwords needs to be checked for bruteforce attacks | Data in Motion | TC No.- 92 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Data Access (STR[I]DE) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Data at Rest | TC No.- 93 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Data Access (STR[I]DE) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Smart medic app (Azure Portal Administrator) | TC No.- 94 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Data Access (STR[I]DE) | Controlled Use of Administrative Privileges over the network | Smart medic app (Azure Portal Administrator) | TC No.- 95 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Data Access (STR[I]DE) | Unprotected external USB Port on the tablet/devices. | Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) | TC No.- 96 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Open network port exploit (TTP) | Unprotected network port(s) on network devices and connection points | Tablet OS/network details & Tablet Application | TC No.- 97 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Open network port exploit (TTP) | Unprotected network port(s) on network devices and connection points | Wireless Network device | TC No.- 98 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering.  8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools. |
| Open network port exploit (TTP) | Unencrypted Network segment throught the information flow | Tablet OS/network details & Tablet Application | TC No.- 99 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Open network port exploit (TTP) | Unencrypted Network segment throught the information flow | Wireless Network device | TC No.- 100 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering.  8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools. |
| Open network port exploit (TTP) | Controlled Use of Administrative Privileges over the network | Smart medic app (Azure Portal Administrator) | TC No.- 101 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Open network port exploit (TTP) | Unencrypted data in flight in all flowchannels | Data in Motion | TC No.- 102 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Open network port exploit (TTP) | Insecure communications in networks (hospital) | Tablet OS/network details & Tablet Application | TC No.- 103 | 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability  5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.  7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. |
| Brute-force Attack (CAPEC-112) | Devices with default passwords needs to be checked for bruteforce attacks | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 104 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Brute-force Attack (CAPEC-112) | Devices with default passwords needs to be checked for bruteforce attacks | Smart medic app (Azure Portal Administrator) | TC No.- 105 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Brute-force Attack (CAPEC-112) | Devices with default passwords needs to be checked for bruteforce attacks | Azure Cloud DataBase | TC No.- 106 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Brute-force Attack (CAPEC-112) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 107 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Brute-force Attack (CAPEC-112) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Smart medic app (Azure Portal Administrator) | TC No.- 108 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Brute-force Attack (CAPEC-112) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Azure Cloud DataBase | TC No.- 109 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Brute-force Attack (CAPEC-112) | Checking authentication modes for possible hacks and bypasses | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 110 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Brute-force Attack (CAPEC-112) | Checking authentication modes for possible hacks and bypasses | Smart medic app (Azure Portal Administrator) | TC No.- 111 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Brute-force Attack (CAPEC-112) | Weak Encryption Implementaion in data at rest and in motion tactical and design wise | Data at Rest | TC No.- 112 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Brute-force Attack (CAPEC-112) | Weak Encryption Implementaion in data at rest and in motion tactical and design wise | Data in Motion | TC No.- 113 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM |
| Social Engineering (TTP) | InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 114 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Social Engineering (TTP) | Legacy system identification if any | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 115 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Social Engineering (TTP) | The password complexity or location vulnerability. Like weak passwords and hardcoded passwords. | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 116 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Social Engineering (TTP) | Checking authentication modes for possible hacks and bypasses | Interface/API Communication | TC No.- 117 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Social Engineering (TTP) | Checking authentication modes for possible hacks and bypasses | Smart medic app (Stryker Azure Cloud Web Application) | TC No.- 118 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Social Engineering (TTP) | Checking authentication modes for possible hacks and bypasses | Azure Cloud DataBase | TC No.- 119 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Social Engineering (TTP) | Checking authentication modes for possible hacks and bypasses | Smart medic app (Azure Portal Administrator) | TC No.- 120 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE) | Insufficient Logging information | Smart medic app (Azure Portal Administrator) | TC No.- 121 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE) | Insufficient Access permissions for accessing and modifying Log files | Smart medic app (Azure Portal Administrator) | TC No.- 122 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Unauthorized Alterations (S[T]RIDE) | InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers | Azure Cloud DataBase | TC No.- 123 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Unauthorized Alterations (S[T]RIDE) | Insufficient Access permissions for accessing and modifying Log files | Azure Cloud DataBase | TC No.- 124 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Gaining Access ([S]TRID[E]) | Error Info containing sensitive data for Failed Authentication attempts | Smart medic app (Azure Portal Administrator) | TC No.- 125 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | Error Info containing sensitive data for Failed Authentication attempts | Azure Cloud DataBase | TC No.- 126 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Gaining Access ([S]TRID[E]) | Absence of additional security factor along with user identification | Smart medic app (Azure Portal Administrator) | TC No.- 127 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | Absence of additional security factor along with user identification | Azure Cloud DataBase | TC No.- 128 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Gaining Access ([S]TRID[E]) | Having no limit on the login attempts | Smart medic app (Azure Portal Administrator) | TC No.- 129 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Gaining Access ([S]TRID[E]) | Having no limit on the login attempts | Azure Cloud DataBase | TC No.- 130 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Brute-force Attack (CAPEC-112) | Error Info containing sensitive data for Failed Authentication attempts | Smart medic app (Azure Portal Administrator) | TC No.- 131 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Brute-force Attack (CAPEC-112) | Error Info containing sensitive data for Failed Authentication attempts | Azure Cloud DataBase | TC No.- 132 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Brute-force Attack (CAPEC-112) | Absence of additional security factor along with user identification | Smart medic app (Azure Portal Administrator) | TC No.- 133 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Brute-force Attack (CAPEC-112) | Absence of additional security factor along with user identification | Azure Cloud DataBase | TC No.- 134 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |
| Brute-force Attack (CAPEC-112) | Having no limit on the login attempts | Smart medic app (Azure Portal Administrator) | TC No.- 135 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. |
| Brute-force Attack (CAPEC-112) | Having no limit on the login attempts | Azure Cloud DataBase | TC No.- 136 | 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port  6) Exploit related to Brute Force attempt for the authentication/authorization on the open port |

1. **Requirements- Test Cases**

|  |  |  |
| --- | --- | --- |
| **Test Case No.** | **Test Case Name** | **Asset** |
| REQ-STC-001 | The Application shall support the use of anti-malware mechanism | Tablet |
| REQ-STC-002 | The Application shall provide secure tunnel Communications channel | Tablet  SM Device  NSA |
| REQ-STC-003 | Only Stryker made/authenticated devices should be able to communicate with SM device and tablet. | Tablet  SM Device |
| REQ-STC-004 | The application shall be allowed to upgrade the tablet application. | Admin |
| REQ-STC-005 | Application shall have the User Management Screen to configure and manage the users as per the roles. | Admin |
| REQ-STC-006 | The Application shall be validated by using invisible captcha during login. | NSA |
| REQ-STC-007 | Invalid login creds, only 3 attempts left. | Admin  NSA |
| REQ-STC-008 | System shall store patient id in anonymized fashion. | Admin |
| REQ-STC-009 | Error msg: Something went wrong with API operation try again / contact API admin. | Admin  NSA |
| REQ-STC-010 | For sensitive data at rest, identification & proper encryption mechanism needs to be designed & implemented | Tablet  Cloud db |
| REQ-STC-011 | Secure sensitive data in the channel flow using strong encryption | Tablet  Admin |
| REQ-STC-012 | Weak algorithms such as DES, RC4, etc.. should be avoided and usage of strong algorithms such as AES, RSA, etc.. are recommended | Tablet  Cloud db |
| REQ-STC-013 | Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended. | Tablet  Cloud db |
| REQ-STC-014 | If database access using keys/certificates, their generation & storage should be done securely. | Tablet  Cloud db |
| REQ-STC-015 | Weight and patient data in the database shall be available upto 6 months. | NSA |
| REQ-STC-016 | User shall find the overall system flow in the User Manual document. | NSA |
| REQ-STC-017 | The application will be used by the Stryker Installation and service teams. | Admin |



\*\*\* End of the document



**THE NETHERLAND**Maria Montessorilaan 3,   
2719 DB Zoetermeer,   
The Netherlands

**www.gsecurelabs.com**

**Confidentiality Clause:**

This document and any files with it are for the sole use of the intended recipient(s) and may contain confidential and privileged information. If you are not the intended recipient, please destroy all copies of the document. Any unauthorized review, use, disclosure, dissemination, forwarding, printing or copying of this document or any action taken in reliance on this document is strictly prohibited and may be unlawful.

Copyright © Gateway Group

**INDIA**B/81, Corporate House,   
Judges Bungalow Road, Bodakdev,   
Ahmedabad - 380054. India