Sensitive and Confidential Information – For Official Use Only

Information Security Testing and Evaluation Plan

**Prepared for: Unblock Health**

As performed by Security Testing Team

**ST&E Plan Document v1.0**

**07-22-2022**

**Table of Contents**

[Executive Summary 1](#_bookmark0)

1. [Introduction 2](#_bookmark0)
   1. [Purpose 2](#_bookmark2)
2. [Scope 3](#_bookmark3)
   1. [System or Application Name 3](#_bookmark4)
   2. [IP Addresses Slated for Testing 3](#_bookmark7)
   3. [Roles Slated for Testing 4](#_bookmark9)
   4. [Web Applications Slated for Testing 4](#_bookmark11)
   5. [Infrastructure and Network Slated for Testing 5](#_bookmark13)
   6. [Assumptions / Limitations 5](#_bookmark19)
3. [Methodology 6](#_bookmark20)
4. [Test Scheduled Tasks 8](#_bookmark26)
5. [Rules of Engagement 9](#_bookmark28)
   1. [Disclosures 9](#_bookmark29)
   2. [Security Testing Scenarios 9](#_bookmark30)
   3. [Test Inclusions 9](#_bookmark31)
   4. [Test Exclusions 1](#_bookmark32)0
   5. [End of Testing 1](#_bookmark33)0
   6. [Communication of Test Results 1](#_bookmark34)0

**List of Tables**

[Table 1. Information System Name and Description 3](#_bookmark5)

[Table 2. IP Addresses Slated for Testing 3](#_bookmark8)

[Table 3. Roles Slated for Testing 4](#_bookmark10)

[Table 4. Web Applications Slated for Testing 4](#_bookmark12)

[Table 5. Infrastructure and Network Components Slated for Testing 5](#_bookmark14)

[Table 6. Kali Linux Toolkit Sample ..7](#_bookmark25)

[Table 7. Test Scheduled Tasks ..8](#_bookmark27)

**Executive Summary**

An information security *testing and* *assessment* is the process of determining how effectively an entity being assessed (e.g., host, system, network, procedure, person—known as the assessment *object*) meets specific security objectives. Three types of assessment methods can be used to accomplish this—testing, examination, and interviewing. *Testing* is the process of exercising one or more assessment objects under specified conditions to compare actual and expected behaviors. *Examination* is the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. *Interviewing* is the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence. Assessment results are used to support the determination of security control effectiveness over time.

This document contains the technical aspects of the things done while conducting information security assessments. It presents technical testing and examination methods and techniques that an organization might use as part of an assessment, and offers insights to assessors on their execution and the potential impact they may have on systems and networks. For an assessment to be successful and have a positive impact on the security posture of a system, elements beyond the execution of testing and examination must support the technical process. Suggestions for these activities including a robust planning process, root cause analysis, and tailored reporting are also presented in this guide.

The processes and technical guidance presented in this document enable organizations to:

* Develop information security testing/assessment methodology, and individual roles and responsibilities related to the technical aspects of assessment
* Accurately plan for a technical information security assessment by providing guidance on determining which systems to assess and the approach for assessment, addressing logistical considerations, developing an assessment plan, and ensuring legal and policy considerations are addressed
* Safely and effectively execute a technical information security assessment using the presented methods and techniques, and respond to any incidents that may occur during the assessment
* Conduct analysis and reporting to translate technical findings into risk mitigation actions that will improve the organization’s security posture

1. **Introduction**

The Unblock Health will be tested and assessed by the Security Testing Team, and the use of an independent assessment team reduces the potential for conflicts of interest that could occur in verifying the implementation status and effectiveness of the security of the system. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk* states:

Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision.

The Security Testing Team/Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the system and the determination of security effectiveness. Their role is to provide an independent assessment of the application and the system and to maintain the integrity of the whole process. The team is required to attest to their independence and objectivity in completing the audit, and that neither the NEE nor the Auditor took any actions that might impair the objectivity of the findings in the audit

## Purpose

This *Security Test & Evaluation Plan* documents all testing to be conducted during the testing/assessment to validate the security for the application and server. It will be done by the Security Team for the benefit of Unblock Health.

1. **Scope**

## System or Application Name

Table 1 describes the information system(s) and/or application(s) scheduled for testing.

#### Table 1. Information System Name and Description

|  |  |
| --- | --- |
| **Information System Name** | **Information System Description** |
| Unblock Health(Devl) | The application is running in a devl environment so that active/aggressive tests can be done. |
| Unblock Health(Demo) | The application is running in a demo environment so network security tests are done in this environment. |

## IP Addresses Slated for Testing

Table 2 identifies the IP addresses and network range of the system that will be tested.

#### Table 2. IP Addresses Slated for Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **IP Address(s) or Range** | **Hostname** | **Software and Version** | **Function** |
| 1 | 192.241.165.153 | co.medigy.com | N/A | Unblock Health Demo Environment |
| 2 | 162.243.60.189 | www.medigy.com | N/A | Medigy Server |
| 3 | 138.88.145.229 | devl.co.medigy.com | N/A | Unblock Health Devl Environment |

## Roles Slated for Testing

For this assessment, a set of usernames have been used which are associated with the specific roles and corresponding responsibilities.

Table 3 identifies the roles slated for testing.

#### Table 3. Roles Slated for Testing

|  |  |  |  |
| --- | --- | --- | --- |
| **Role**  **Name** | **Test User ID/Credential** | **Account Username** | **Username Associated Responsibilities** |
| Hospital Admin(MRA) | prithvimra@gmail.com | Prithvi | View the requests assigned by the PPA user and also change the request status. |
| PPA | ellieppa@gmail.com | Ellie | Create request and assigned to MRAs and view patients details |
|  |  |  |  |

## Web Applications Slated for Testing

The Auditor must test for the most current Open Web Application Security Project (OWASP) Top Ten Most Critical Web Application Security Risks. Provided are the web application URL and components that will be in scope for this assessment.

Table 4 identifies the web applications slated for testing.

#### Table 4. Web Applications Slated for Testing

|  |  |  |
| --- | --- | --- |
| **Login URL for the Application** | **Web Application Name** | **Function / Description** |
| https://devl.co.medigy.com/login | Unblock Health | This application manages patient records especially medical record and billing insurance. |

1 The OWASP Top Ten Most Critical Web Application Security Risks are located at: https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project

## Infrastructure and Network Slated for Testing

Table 5 identifies the infrastructure and/or network components of the system that will be tested.

#### Table 5. Infrastructure and Network Components Slated for Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Unique ID** | **rDNS Recod Name** | **IP Address** | **OS Name and Version** | **Asset Type** |
| 1 | docker.nyc2.netspective.com | 162.243.60.189 | Ubuntu 18 | Web Server |
| 2 | docker2.nyc2.netspective.com | 192.241.165.153 | Ubuntu 18 | Web Server |

## Assumptions / Limitations

1. Unblock Health resources, including documentation and individuals with knowledge of the Unblock Health systems, applications, and infrastructure and associated contact information, will be available to Security Testing Team during the scheduled assessment timeframe and testing activities in order to complete the assessment.
2. The Unblock Health will provide login account information/credentials necessary for Security Testing Team to use with its testing devices to perform authenticated scans of devices and applications.
3. The Unblock Health will permit Security Testing Team to connect testing laptops to the Unblock Health networks defined within the scope of this assessment.
4. The Unblock Health will permit communication from the Auditor testing appliances to an internet-hosted vulnerability management service to permit the analysis of vulnerability data.

Significant upgrades or changes to the infrastructure and components of the system undergoing testing will not be performed during the security assessment period.

1. **Methodology**

Security Testing Team will perform the security testing/assessment of Unblock Health s using the methodology mentioned in OWASP & PTES. Security Testing Team will use test procedures to evaluate the security of server and the application.

Data gathering activities will consist of the following:

* Request required documentation
* Request any follow-up documentation, files, or information needed that is not provided in required documentation
* Obtain information using security testing tools

Security testing/assessment will be verified using one or more of the following assessment methods:

* **Planning**. Critical to a successful security assessment, the planning phase is used to gather information needed for assessment execution—such as the assets to be assessed, the threats of interest against the assets, and the security controls to be used to mitigate those threats—and to develop the assessment approach. A security assessment should be treated as any other project, with a project management plan to address goals and objectives, scope, requirements, team roles and responsibilities, limitations, success factors, assumptions, resources, timeline, and deliverables.
* **Execution**. Primary goals for the execution phase are to identify vulnerabilities and validate them when appropriate. This phase should address activities associated with the intended assessment method and technique. Although specific activities for this phase differ by assessment type, upon completion of this phase assessors will have identified system, network, and organizational process vulnerabilities.
* **Post-Execution**. The post-execution phase focuses on analyzing identified vulnerabilities to determine root causes, establish mitigation recommendations, and develop a final report.

All testing will be done using Kali Linux which is widely used OS for penetration testing and security assessment activities. The Kali linux OS will contain all the industry standard open-source tools needed for the security testing.

Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools targeted towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Kali Linux is a multi platform solution, accessible and freely available to information security professionals and hobbyists.

Table 7 identifies the tools and frameworks that will be used while performing the testing.

#### Table 6. Kali Linux Toolkit Sample

|  |  |
| --- | --- |
| **Security Testing Technique** | **Security Testing Tool** |
| **Review** | |
| Network Sniffing | Dsniff, Ettercap, Kismet, Mailsnarf, Msgsnarf, Ntop, Phoss, SinFP, SMB Sniffer, and Wireshark |
| File Integrity Checking | Autopsy, Foremost, RootkitHunter, and Sleuthkit |
| **Target Identification and Analysis** | |
| Application Security Testing | CIRT Fuzzer, Fuzzer 1.2, NetSed, Paros Proxy, and Peach |
| Network Discovery | Autonomous System Scanner, Ettercap, Firewalk, Netdiscover, Netenum, Netmask, Nmap, P0f, Tctrace, and Umit |
| Network Port and Service Identification | Amap, AutoScan, Netdiscover, Nmap, P0f, Umit, and UnicornScan |
| Vulnerability Scanning | Firewalk, GFI LANguard, Hydra, Metasploit, Nmap, Paros Proxy, Snort, and SuperScan |
| Wireless Scanning | Airsnarf, Airsnort, BdAddr, Bluesnarfer, Btscanner, FakeAP, GFI LANguard, Kismet, and WifiTAP |
| **Target Vulnerability Validation** | |
| Password Cracking | Hydra, John the Ripper, RainbowCrack, Rcrack, SIPcrack, SIPdump, TFTP-Brute, THC PPTP, VNCrack, and WebCrack |
| Remote Access Testing | IKEProbe, IKE-Scan, PSK-Crack, and VNC\_bypauth |
| Penetration Testing | Driftnet, Dsniff, Ettercap, Kismet, Metasploit, Nmap, Ntop, SinFP, SMB Sniffer, and Wireshark |

# **Test Scheduled Tasks**

Table 8 presents the assessment testing related tasks. All parties must agree on the tasks and durations.

#### Table 7. Test Schedule

|  |  |
| --- | --- |
| **No** | **Task Name** |
| 1 | Hold Kickoff Meeting |
| 2 | Develop Draft ST&EP |
| 3 | Hold Meeting to Review ST&EP |
| 4 | Finalize ST&EP |
| 5 | Conduct Interviews of Unblock Health Staff |
| 6 | Perform Testing |
| 7 | Develop Draft SAR/STR |
| 8 | Report Issues to Bug Tracking Platform |
| 9 | Hold Issue Resolution Meeting |
| 10 | Finalize SAR/STR |
| 11 | Send Final Version of SAR/STR to Unblock Health |

# **Rules of Engagement**

## 

## 5.1 Disclosures

Any testing will be performed according to terms and conditions designed to minimize risk exposure that could occur during security testing. All scans will originate from the following IP address(es):115.246.243.186

## 5.2 Security Testing Scenarios

The following Vulnerabilities and Testing scenarios are provided by CMS and their testing is required:

Test specifically for the following security vulnerabilities in addition to the security controls provided:

* + 1. Injection
    2. Broken Authentication
    3. Sensitive Data Exposure
    4. XML External Entity (XXE)
    5. Broken Access Control
    6. Security Misconfiguration
    7. Cross-Site Scripting (XSS)
    8. Insecure Deserialization
    9. Using Components with Known Vulnerabilities
    10. Insufficient Logging & Monitoring

For additional information, consult the OWASP Top Ten Most Critical Web Application Security Risks.

## 5.3 Test Inclusions

Security testing may include the following activities:

* Port scans and other network service interaction and queries
* Network sniffing, traffic monitoring, traffic analysis, and host discovery
* Attempted logins or other use of systems, with any account name/password
* Attempted structured query language (SQL) injection and other forms of input parameter testing
* Use of exploit code for leveraging discovered vulnerabilities
* Password cracking via capture and scanning of authentication databases
* Spoofing or deceiving servers regarding network traffic
* Altering running system configuration except where denial of service would result
* Adding user accounts

## 5.4 Test Exclusions

Security testing will not include any of the following activities:

* Changes to assigned user passwords(on live/demo/production servers)
* Modification of user files or system files(on live/demo/production servers)
* Intentional viewing of Unblock Health staff email, Internet caches, and/or personnel cookie files
* Denial of service attacks
* Exploits that will introduce new weaknesses to the system
* Intentional introduction of malicious code (viruses, Trojans, worms, etc.)

## 5.5 End of Testing

The Security Testing Team will notify Unblock Health people when security testing has been completed.

## 5.6 Communication of Test Results

All communications and reports on all security testing will be done according to Unblock Health requirements. Security testing results will be sent and disclosed to the individuals