ETHICAL HACK PREREQUISITE PROCEDURE

**Date:**

**Client:**

**Contact:**

**Project:**

This document is a prerequisite process which helps understand the scope and terms for the application ethical hacking that will be conducted by sapna security on the non production URL provided by the client. The client authorises sapna security to perform such testing under the following conditions:

# A. Environment details

| Client/Company Name |  |
| --- | --- |
| Application name and version |  |
| Short description of the application |  |
| Non production URL to be tested (including API) |  |
| Is the test server a shared environment where other customers live data may reside, or short disruption of service due to the test might cause issues |  |
| How much time does a session timeout take? |  |
| IP address of the application |  |
| Testing date range (24 hour time window for test each day) |  |
| Size of site based on the following: Small: (Dynamic: 0-5 Static 1-25)Medium (Dynamic: 6-10 Static 26-50)Large (Dynamic 21+ Static 51+) |  |
| List functionalities in the system (eg - user login, - change password, - see/update profile, add products to cart, payment system, view history. If you have a functional document which lists all user experience please pass that instead.). |  |
| List all user roles and give a short description |  |
| List the UserIDs the assessor will use to logon and access the application.Provide at least 3 accounts representative of each those roles (Do NOT include passwords, please send password using an encrypted method). |  |
| What OS and which version is the application hosted on (eg Debian 9) |  |
| What web server and which version is used by the application (eg Apache 2) |  |
| What programming language(s) is the application written (C, Java, .NET, etc)? |  |
| What database and which version is used by the application (eg MySQL) |  |
| Encryption / hashing technique used in the application |  |
| Is there a separate mobile URL, if so please send the test URL. |  |
| Details of mobile OS, version etc for which app is available (eg Android version, iOS version) |  |
| Details of what is required to get the app working on tester handset (UUID number needs to be sent by tester etc) |  |
| Name, email, and phone number of a support contact the assessor use to ask questions or resolve access issues |  |
| Name, email address, and phone number of the person(s) to receive final assessment report |  |

1. Testing will be conducted against the following non-production URLs mentioned above
2. Client will provide any document and app files like .apk or .ipa files for android / iOS.
3. Testing will be conducted during the period mentioned above. Any changes to this time window must be agreed to by both sapna security and Client.
4. Client will ensure that the following sapna security source IP addresses are whitelisted within Client’s Intrusion Detection System (IDS/IPS) during scan dates/times specified above:
176.9.38.84
138.201.129.35
88.99.99.234
162.55.235.245
5. Client will ensure that the test environment is stable and available during the agreed to testing time frame.
6. Client accepts responsibility for ensuring that all environments identified to sapna security for testing are non-production, containing only test data, and that the testing described in this document will not impact the production environment.
7. Client will provide sapna security with the test accounts (login IDs), credentials, and representative test data to be used during the assessment process. These accounts and data will be dedicated for use by sapna security throughout the testing period and will be sufficient to test all aspects of the identified systems.
8. Client will provide at least 3 test accounts for each user role supported by the application to sapna security. This to allow for verification of data access controls (horizontal authorization) and functional access controls (vertical authorization).

# B. Assessment process

1. sapna security will provide the source IP addresses to be used for testing prior to the start of the assessment. Client is responsible for distributing this information and the times of the assessment to their appropriate monitoring teams.
2. sapna security may request a demo of the system prior to the vulnerability testing.
3. sapna security will restrict its assessment activities to the Base URLs and network ranges identified in Section A.
4. The assessment process will include automated tools, public information gathering, and manual ethical hacking and analysis. Manual analysis is performed to confirm the automated findings as well as to perform more in-depth analysis.
5. Results of the Vulnerability Assessment will be shared with the Client once a final report is available.
6. sapna security and Client will identify primary technical points of contact for the purposes of issue notification and resolution. Examples of items include questions on application behaviour from the assessment team or verification from sapna security that anomalous activity is originating from the assessment activities.
7. The assessment process will not intentionally cause harm to the targeted systems.