

**Security Services Scoping Questionnaire**

EnSec Solution has developed this scoping questionnaire to assist organizations in communicating project scope, size and requirements. Submit the completed questionnaire to:

|  |  |
| --- | --- |
| Business Development: | info@ensecsolution.com |
| Bhagyashree Paghdal | bhagyashree@ensecsolution.com |

Should any questions arise regarding the enclosed document, please do not hesitate to contact us. EnSec Solution will promptly respond with any follow-up inquiries and provide a detailed quotation. Your comprehensive responses to this Penetration Testing Questionnaire are greatly appreciated, as they enable us to gain a thorough understanding of your testing requirements and accurately estimate the project timeline.

**Table of Contents**

[**Section 1: Web Application Vulnerability Assessment and Penetration Testing** 3](#_Toc176476783)

[**Section 2: API Vulnerability Assessment and Penetration Testing** 6](#_Toc176476784)

[**Section 3: Mobile Vulnerability Assessment and Penetration Testing** 7](#_Toc176476785)

[**Section 4: Network Vulnerability Assessment and Penetration Testing** 8](#_Toc176476786)

[**Section 5: Device Configuration Audit** 10](#_Toc176476787)

[**Section 6: Secure Code Review** 11](#_Toc176476788)

[**Section 7: Cloud Security Assessment** 12](#_Toc176476789)

[**Appendix A: Application Architecture Diagrams** 13](#_Toc176476790)

[**Appendix B: Environment for Testing** 13](#_Toc176476791)

[**Appendix C: Access to the Application** 13](#_Toc176476792)

# **Section 1: Web Application Vulnerability Assessment and Penetration Testing**

When completing this scoping questionnaire, please keep in mind that this document is intended as an initial starting point, do not worry if you don’t have all the information to hand at this stage, as we will work with you to ensure all relevant information is captured before we put forward a proposal of work.

The objective of this document is to:

* Provide steering for our consultants to ask the right follow-up questions, building a full picture of your requirements.
* Gain advanced notice of any factors that may affect timely delivery of the work.
* Enable us to confidently arrive at a realistic expectation around the number of days to deliver the scoped requirement.

Please answer the following questions for EACH application that needs to be tested. *Copy and paste the tables for more applications, as necessary*.

|  |  |
| --- | --- |
| **Application / WebApp #1** | *Application Name* |
| **What is the primary reason for the test?**  **For example:**  - Regulatory (Bank/PCI/CHECK/ISO)  - Project/Product Security Assurance  - Client Requirement etc. | *General, Regulatory, Client requirement*  *Click here to provide details.* |
| **Are there any specific security concerns with regards to the application?** | *Click here to provide details.* |
| **Has the application been developed?** | Internally  Externally |
| **Is this test part of a development cycle?**  (Before a go live date/Audit Date) | Yes  No  *Click here to provide details.* |
| **Are any internal authorizations required before testing begins?** | Yes  No |
| **Has this application been tested before?** | Yes  No  *If yes, please provide details here.* |
| **Is the authorization of an external / third party required before testing?**  **For example:**  - Hosting partners  - Third-party developers etc. | Yes  No  *If yes, please provide details here.* |
| **Is this a multi-tenant application?** | Yes  No  *If yes, please provide details here.* |
| **Can testing be performed remotely?** | On-site at client’s location  Remote testing  Remote testing with client provided VM using VPN access |
| **Testing Style** | Black Box - Without Credentials, no access source code  Gray Box – with Credentials, full access to documentation, no access source code  White Box – with Credentials, full access to documentation, access to source code |
| **Application URL** | *Application URL to be tested* |
| **What sort of environment will the test be conducted on?** | Production Live Environment  UAT (User Acceptance Testing)  Development Environment |
| **How many static pages?**  (A static webpage is a page that has fixed content which remains constant) | *Click here to provide details.* |
| **How many unique dynamic pages?**  **Less than 10, 20, 50, 100?**  (A dynamic webpage is a page that has frequently changing information which is being generated in real-time) | *Click here to provide details.* |
| **What language is the Web Application written in? e.g.** C#, Java, PHP, .NET, Perl | *Click here to provide details.* |
| **What is the level of overlap that exists between the main web application and the API?** | *Types of API involved in the application ex. RESTful APIs, SOAP APIs, Graph QL APIs or Microservices APIs.* |
| **What is the main functionality and purpose of the application?**  ex. Online Banking, E-Commerce etc. | *Click here to provide details.* |
| **What type of data is processed and stored by the application?**  **For example:**  - Personal, Financial, Medical etc. | *Click here to provide details.* |
| **Is supporting documentation or an application walkthrough available?** | Yes  No |
| **Are there any IPS/IDS or WAF in place?**  - (IPS = Intrusion Prevention System)  - (IDS = Intrusion Detection System)  - (WAF = Web Application Firewall) | *Click here to provide details.* |
| **Please list any application or functionality that are explicitly out of scope for testing.** | *Click here to provide details.* |
| **We normally ask our customers to disable IPS/IDS/WAFs for application tests given that they can slow down the test and consequently limit its coverage. Is this acceptable?** | Yes  No |
| **If disabling WAF/IDS/IPS is not acceptable, should part of the test be used to determine their strength and whether they can be bypassed?** | Yes  No |
| **Is this site hosted with a third-party?**  **For example:**  - AWS  - Azure  - GCP | Yes  No  *If yes, please provide details here.* |
| **How many application users?** | *Click here to provide details.* |
| **What authentication mechanism(s) does the application employ?**  - Basic password-based Auth  - API Key Authentication  - OAuth  - OpenID connect | *Click here to provide details.* |
| **Does the application have different types of users?**  **For example:**  - Administrator  - Power User  - Regular User | Yes  No  *If yes, please provide details here.* |
| **How are sessions persisted across the application?**  **For example:**  - Session Cookies  - JWT Tokens  - OAUTH Tokens | *Click here to provide details.* |
| **Is the source code available for the consultant during testing?**  (Provision of the source code provides for better coverage, as the consultant can confirm findings) | Yes  No |
| **Are there any restrictions in the hours when testing can be performed?**  Our typical testing is conducted between 10:00 - 19:00 IST. | Yes  No  *If yes, please provide details here.* |
| **Do you have any specific timelines / deadlines by which testing has to be completed?** | Yes  No  *If yes, please provide details here.* |

# **Section 2: API Vulnerability Assessment and Penetration Testing**

|  |  |
| --- | --- |
| **API / Product #1** | *Product Name* |
| **What is the primary reason for the test?**  **For example:**  - Regulatory (Bank/PCI/CHECK/ISO)  - Project/Product Security Assurance  - Client Requirement etc. | *General, Regulatory, Client requirement*  *Click here to provide details.* |
| **Are there any specific security concerns with regards to the application?** | *Click here to provide details.* |
| **Has the application been developed?** | Internally  Externally |
| **Is this test part of a development cycle?**  (Before a go live date/Audit Date) | Yes  No  *Click here to provide details.* |
| **Are any internal authorizations required before testing begins?** | Yes  No |
| **Has this application been tested before?** | Yes  No  *If yes, please provide details here.* |
| **Is the source code available for the consultant during testing?**  (Provision of the source code provides for better coverage, as the consultant can confirm findings) | Yes  No |
| **Are there any restrictions in the hours when testing can be performed?**  Our typical testing is conducted between 10:00 - 19:00 IST. | Yes  No  *If yes, please provide details here.* |
| **Do you have any specific timelines / deadlines by which testing has to be completed?** | Yes  No  *If yes, please provide details here.* |
| **What sort of environment will the test be conducted on?** | Production Live Environment  UAT (User Acceptance Testing)  Development Environment |
| **Can testing be performed remotely?** | On-site at client’s location  Remote testing  Remote testing with client provided VM using VPN access |
| **Testing Style** | Black Box - Without Credentials, no access source code  Gray Box - Credentials, full access to documentation, no access source code  White Box - Credentials, full access to documentation, access to source code |
| **Is supporting API documentation or an walkthrough available?**  Ex. Swagger, Postman etc. | Yes  No  *If yes, please provide details here.* |
| **API calling sequence present in API document?** | Yes  No  *If no, Share the flow diagram, if not already mentioned in the API document.* |
| **Is any demo application / script available for calling API?** | *e.g. Need a demo app or script that calls the specific API to understand the parameters, values passed to the API* |

# **Section 3: Mobile Vulnerability Assessment and Penetration Testing**

|  |  |
| --- | --- |
| **Application #1** | *Application Name* |
| **What is the primary reason for the test?**  **For example:**  - Regulatory (Bank/PCI/CHECK/ISO)  - Project/Product Security Assurance  - Client Requirement etc. | *General, Regulatory, Client requirement*  *Click here to provide details.* |
| **Are there any specific security concerns with regards to the application?** | *Click here to provide details.* |
| **Has the application been developed?** | Internally  Externally |
| **Is this test part of a development cycle?**  (Before a go live date/Audit Date) | Yes  No  *Click here to provide details.* |
| **Are any internal authorizations required before testing begins?** | Yes  No |
| **Has this application been tested before?** | Yes  No  *If yes, please provide details here.* |
| **Is the source code available for the consultant during testing?**  (Provision of the source code provides for better coverage, as the consultant can confirm findings) | Yes  No |
| **Are there any restrictions in the hours when testing can be performed?**  Our typical testing is conducted between 10:00 - 19:00 IST. | Yes  No  *If yes, please provide details here.* |
| **Do you have any specific timelines / deadlines by which testing has to be completed?** | Yes  No  *If yes, please provide details here.* |
| **What sort of environment will the test be conducted on?** | Production Live Environment  UAT (User Acceptance Testing)  Development Environment |
| **Can testing be performed remotely?** | On-site at client’s location  Remote testing  Remote testing with client provided VM using VPN access |
| **Testing Style** | Black Box - Without Credentials, no access source code  Gray Box - Credentials, full access to documentation, no access source code  White Box - Credentials, full access to documentation, access to source code |
| **What communication protocol does it use to exchange data with servers?** | http/https  Other  *If other, please provide details here.* |
| **Application Platform** | Android  iOS  Windows  Other  *If other, please provide details here.* |
| **How many unique screens?**  **Less than 10, 20, 50, 100?**  (Number of screens based on modules available in the application) | *Click here to provide details.* |
| **Does the application have different types of users?**  **For example:**  - Administrator, Power User, Regular User | Yes  No  *If yes, please provide details here.* |

# **Section 4: Network Vulnerability Assessment and Penetration Testing**

|  |  |
| --- | --- |
| **What is the primary reason for undergoing testing?** (Check all that apply) | Data Security Reasons  Recent Security Issue  Annual Security Review  Other (Please Specify Below)  *Click here to provide details.* |
| **What areas of your business would you like to be tested? (Check all that apply)** | Vulnerability Scan Only (PCI Compliant)  Internal Network Pen Testing (Including Vulnerability Scan)  External Network Pen Testing (Including Vulnerability Scan)  Wireless Network Testing  Internal Web Application Testing  External Web Application Testing  Social Engineering Testing |
| **Which specific focus areas are a concern?** (Check all that apply) | General Security Controls  PCI DSS  Yearly Penetration Test  Quarterly ASV External Scan  SOC 2 & 3  HIPAA  Other (Please Specify Below)  *Click here to provide details.* |
| **Are any internal authorizations required before testing begins?** | Yes  No |
| **When was the last security assessment or penetration test performed?** | 1-3 Months  3-6 Months  6-12 Months  Never |
| **When do you want the Penetration Testing conducted?**  Our typical testing is conducted between 10:00 - 19:00 IST. | During Business Hours  After Business Hours  On Weekends  *Click here to provide details.* |
| **Do you have any specific timelines / deadlines by which testing has to be completed?** | Yes  No  *If yes, please provide details here.* |
| **Can testing be performed remotely?** | On-site at client’s location  Remote testing  Remote testing with client provided VM using VPN access |
| **Testing Style** | Black Box - Without OS Credentials  Gray Box - With OS Credentials |
| **Are there any devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?** | |  | | --- | | Please List Devices: | |  | |  | |  | |
| **What type of testing environment will be available?** (Check all that apply) | Production Environment  Test Environment  Development Environment |
| **PCI DSS SUB-SECTION** | |
| **How many credit card transactions are processed annually?** | More than 6M  1M to 6M  20k to 1M  Fewer than 20k  N/A |
| **Are credit card transactions accepted online?** | Yes  No |
| **HIPAA SUB-SECTION** | |
| **Is Protected Health Information Stored or Processed?** | Yes  No |
| **Is this information accessible via the Internet?** | Yes  No |
| **INTERNAL NETWORK DETAILS SECTION** | |
| **Provide the IP addresses or ranges to be tested. (format: xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/xx):** | |  | | --- | | IP Addresses / Ranges | |  | |  | |  | |
| **EXTERNAL NETWORK DETAILS SECTION** | |
| **Provide the URLs\IPs for each Website to be tested (URL and IP address needed, example: www.abc.com / xxx.xxx.xxx.xxx):** | |  | | --- | | IP Addresses / Ranges / URLs | |  | |  | |  | |
| **Do you have Network architecture diagram?** | Yes  No  *If yes, please provide details here.* |

# **Section 5: Device Configuration Audit**

|  |  |
| --- | --- |
| **What is the primary reason for the test?**  **For example:**  - Regulatory (Bank/PCI/CHECK/ISO)  - Project/Product Security Assurance  - Client Requirement etc. | *General, Regulatory, Client requirement*  *Click here to provide details.* |
| **Are there any specific security concerns with regards to the application?** | *Click here to provide details.* |
| **Is this test part of a development cycle?**  (Before a go live date/Audit Date) | Yes  No  *Click here to provide details.* |
| **Are any internal authorizations required before testing begins?** | Yes  No |
| **Has this device configuration reviewed before?** | Yes  No  *If yes, please provide details here.* |
| **Do you have any specific timelines / deadlines by which Audit has to be completed?** | Yes  No  *If yes, please provide details here.* |
| **Can testing be performed remotely?** | On-site at client’s location  Remote testing  Remote testing with VPN access |
| **Audit Style** | Provides offline configuration file  Provide Audit/ Read only account on devices |
| **Number of Devices** | *Total number of devices that will be part of configuration audit* |
| **Types of Devices** | *E.g. Routers, Firewall, Servers, Desktop etc.* |

# **Section 6: Secure Code Review**

|  |  |
| --- | --- |
| **What is the primary reason for the test?**  **For example:**  - Regulatory (Bank/PCI/CHECK/ISO)  - Project/Product Security Assurance  - Client Requirement etc. | *General, Regulatory, Client requirement*  *Click here to provide details.* |
| **Are there any specific security concerns with regards to the application?** | *Click here to provide details.* |
| **Has the application been developed?** | Internally  Externally |
| **Is this test part of a development cycle?**  (Before a go live date/Audit Date) | Yes  No  *Click here to provide details.* |
| **Are any internal authorizations required before testing begins?** | Yes  No |
| **Has this application code reviewed before?** | Yes  No  *If yes, please provide details here.* |
| **Do you have any specific timelines / deadlines by which code review has to be completed?** | Yes  No  *If yes, please provide details here.* |
| **Can testing be performed remotely?** | On-site at client’s location  Remote testing using provide code access offline  Remote testing with VPN access |
| **Lines of Code \* LOC** | *List of files with lines of code*  *Note: You can use Note: You can use CLOC tool which will help you to count the number of lines in the source code. All the instructions are mentioned for installation and calculations. Below mentioned is the URL of this tool.*  *URL:* [*http://cloc.sourceforge.net/*](http://cloc.sourceforge.net/)   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Language | Files |  | Blank | Comment | Code | | Ex. Java | 20xx |  | 111xxx | 120xx | 299xxx | |  |  |  |  |  |  | |  |  |  |  |  |  | |

# **Section 7: Cloud Security Assessment**

|  |  |
| --- | --- |
| **What is the primary reason for the test?**  **For example:**  - Regulatory (Bank/PCI/CHECK/ISO)  - Project/Product Security Assurance  - Client Requirement etc. | *General, Regulatory, Client requirement*  *Click here to provide details.* |
| **Are there any specific security concerns with regards to the infrastructure?** | *Click here to provide details.* |
| **Are any internal authorizations required before testing begins?** | Yes  No |
| **Do you have any specific timelines / deadlines by which review has to be completed?** | Yes  No  *If yes, please provide details here.* |
| **How many services are hosted in the cloud infrastructure?** (Please share the list of services) | *Click here to provide details.* |
| **Architecture / policy documentation for the in-scope infrastructure/application** | *Click here to provide details.* |
| **No of environments in the cloud infrastructure i.e. AWS Organization** | *Click here to provide details.* |
| **If your cloud environment hosts code as infrastructure, please provide the user roles who can access the code e.g. developer user** | *Click here to provide details.* |
| **List of user roles currently available in the cloud environment.** (active users enabled in the cloud) | *Click here to provide details.* |
| **Process documents i.e. IT security policy, User management, Data Security, Password Policy.** | *Click here to provide details.* |

# **Appendix A: Application Architecture Diagrams**

Please include any relevant application architecture diagrams with this questionnaire, to help us better understand the scope and estimate the effort involved. [If Available]

# **Appendix B: Environment for Testing**

If application to be tested on production environment, prior approvals and permissions required from company owning the application. Authorization letter to be submitted in EnSec Solution submitted format.

# **Appendix C: Access to the Application**

Access to the target application, can be provided to EnSec Solution analyst in any one of the below mentioned options to perform remote testing:

**For UAT application testing:**

1. Whitelist EnSec Solution static IP, to allow the whitelisted IP to access the target application.
2. Client company to create a client to site VPN to establish a secured VPN connection between EnSec Solution and client network.

**For Production application testing:**

1. Once authorizations and permission provided by client, EnSec Solution can access the production application over internet.

A grey lock on a globe

Description automatically generated