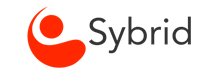


SYBRID SECURITY SERVICES

Product Datasheet

SYBRID PRIVATE LIMITED



Copyright © 2019 by SYBRID Technology Division

All rights reserved. This document or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a document review.

The SYSEC® logo is property of SYBRID where other logos used in document are the property of their respective owners

Table of Contents

[1. Introduction 5](#_Toc62814064)

[2. Objective 5](#_Toc62814065)

[3. Concept 5](#_Toc62814066)

[3.1. Guidelines 5](#_Toc62814067)

[3.1.1. Mechanism 6](#_Toc62814068)

[3.2. Method 7](#_Toc62814069)

[3.3. Compliance 8](#_Toc62814070)

[3.3.1. ISO 27001 for OWASP 8](#_Toc62814071)

[3.3.2. PCI for OWASP 8](#_Toc62814072)

[3.3.3. ISO 27001 for PTES 10](#_Toc62814073)

[3.4. Platform 10](#_Toc62814074)

[3.5. Tools 10](#_Toc62814075)

[3.6. Development 10](#_Toc62814076)

[3.6.1. Tools combination & sequence 10](#_Toc62814077)

[3.6.2. Scripting for integration of tools over kali platform for VA & PT 10](#_Toc62814078)

[3.6.3. Build for Vulnerability Test. 10](#_Toc62814079)

[3.6.4. Build for Pen Test 11](#_Toc62814080)

[4. Scope of Vulnerability Assessment 11](#_Toc62814081)

[5. Process of Vulnerability Assessment 11](#_Toc62814082)

[5.1. Information Gathering 11](#_Toc62814083)

[5.2. Threat and Risks Modeling 11](#_Toc62814084)

[5.3. Vulnerability Analysis 12](#_Toc62814085)

[5.4. Reporting 12](#_Toc62814086)

[6. Scope of Pentest Assessment 12](#_Toc62814087)

[7. Process of Penetration Test 13](#_Toc62814088)

[7.1. Information Gathering 13](#_Toc62814089)

[7.2. Threat and Risks Modeling 13](#_Toc62814090)

[7.3. Vulnerability Analysis 14](#_Toc62814091)

[7.4. Exploitation 14](#_Toc62814092)

[7.5. Post-Exploitation Report 14](#_Toc62814093)

[Appendixes 15](#_Toc62814094)

[Appendix A: 16](#_Toc62814095)

[Appendix B: 26](#_Toc62814096)

[Appendix C: 35](#_Toc62814097)

[Appendix D: 39](#_Toc62814098)

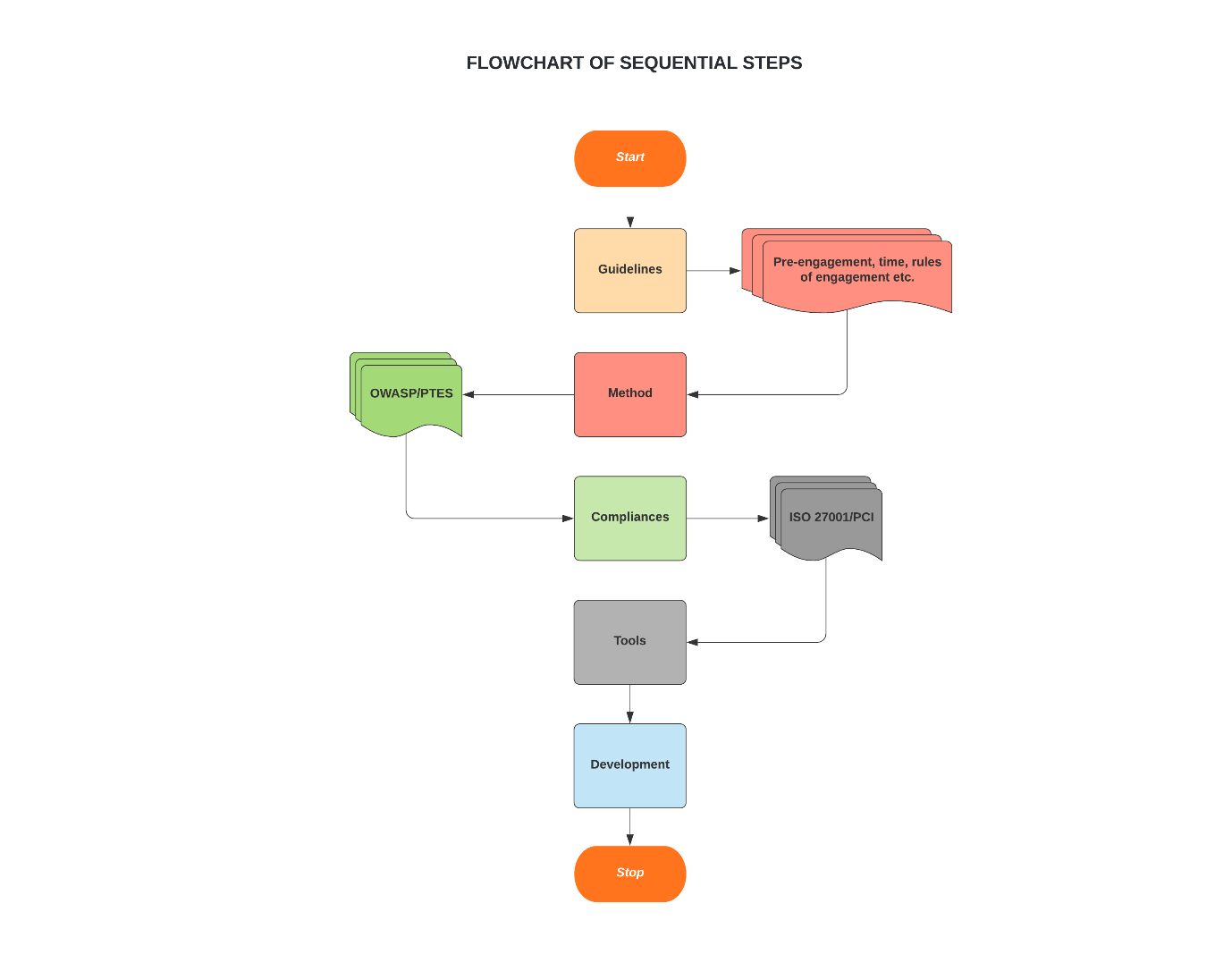
# Introduction

The purpose of the report is to build up a solution to conduct vulnerability assessment and penetration test on the organization level. The main target will be an IP by which we can search for the machines which are providing services and through scanning, finding the vulnerabilities and afterwards if required, exploiting those vulnerabilities. The vulnerabilities found during test out of them some of them are selected by an organization to get them checked and fixed. Moreover, compliances are included on behalf of which different methodologies are mapped to fulfill the required security features for an organization. The tools serving the purpose of testing are selected in accordance with the compliance which are also open-source and later, during the development stage those will be integrated, and the platform will provide services as per the requirement of the client.

# Objective

* To build a platform for vulnerability assessment and penetration testing.
* Methodologies selected and mapped in accordance with compliance requirements.
* Use of open-source tools to serve the purpose.
* Integrating tools and serving the required purpose as a platform.

# Concept



## Guidelines

To build a platform, the process is break down in two parts: first for the vulnerability assessment and second for penetration testing. The vulnerability assessment will perform only the analysis of the application or network and penetration test if needed will exploit those vulnerabilities further. The selection of methods is mentioned in 3.2. However, this one platform will provide services based on open-source tools which by integration will be the part in building this platform.

### Mechanism

#### Pre-Engagement

Pre-engagement is a step before conducting any of the test mentioned above, a meeting should be called to get the idea of the project and working out the scope of the test and the objective. The results of the test should be discussed as sometimes the outcome contains no clear results because purpose might be demonstration of the vulnerabilities which are exploitable and exists within the organization’s network. The form in which the results of the outcomes are showed should also be discussed with the organization.

#### Goal

Every penetration test should be goal-oriented which is to test and identify the specific vulnerabilities which could result in compromising the business or mission objectives of the client. It is not only to find un-patched systems but to identify the risks that could adversely impact the organization.

#### Metrics for Time Estimation

The time estimation depends on the expertise of the tester and whatever the time frame decided it better to add a padding of 20% to total time which acts as a backup as in scenarios continuous failure to scanning the target may lead to overtime. Also, it is possible that the network segment may go down or the founded vulnerability may result into involving many levels of management to address. Both of such events are time consuming and significantly could impact the original time which is why 20% added.

#### IP Ranges and Domains

Before starting a penetration test, all the targets must be identified. The target must be obtained from the client in the initial phase. Targets can be in the form of IP addresses, network ranges, or domain names by the customer. Moreover, it is also important to define that if there is any firewalls, IDS/IPS or networking equipment between the tester and the final target and as they are or not part of the scope. As, in some instances target only provides with the details of the name of the organization and expects the tester to identify the rest on their own. Also, check the IP’s provided to make sure whether they are valid and owned by the client itself or not because these could lead to severe legal consequences.

#### Dealing with the Third Parties

It is also observed that sometimes the client does not tell or forget to talk about the third involved so which means testing a service or application being hosted by the third party. In recent years, cloud services are widely implemented everywhere, and it is need of today to let those third party know or seek permission from them for testing. Failing to take permissions will possibly bring us in front of law.

#### Cloud Services

Testing cloud services may incur an issue of that data from multiple organizations are stored on one physical medium. The cloud services providers need to be alerted to the testing and needs acknowledge that the test is taking place and granting permission to testing organization to test. Moreover, security contract should be there that can be helpful in the event of finding security vulnerability which could impact the other cloud customers. Also, the cloud providers have specific procedures for penetration testers to follow, and may require request forms, scheduling or explicit permission from them before testing can begin.

#### ISP

The ISP terms and conditions should be considered before launching any attack because in many commercial situations the ISP will have specific conditions for testing. In certain situations, the ISP may block the traffic which is considered malicious. The client may approve the risk, but it must be always communicated before the beginning. Web hosting with the third parties, the scope and timing of the test needs to be clearly communicated with web hosting provider.

#### Incident Reporting Process

It is important to discuss the organizations incident response capabilities before the start of the engagement process. The penetration test is not just about testing the environment but to check the capabilities of the incident response team. If an entire engagement process can be completed without the target’s internal security teams ever noticing, then it means there is a big major gap in the security posture. Also inform some from the incident team about the test so the incident team does not start to call every member.

#### Rules of Engagement

As the scope defines what will be tested, the rules of engagement define how that testing is to occur.

#### Information Gathering

Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible to be utilized when performing vulnerability assessment or performing exploitation. The more information gathers during this phase, the more vectors of attack be able to use in the future.

#### Threat Modelling

This section defines a threat modeling approach as required for a correct execution of a vulnerability assessment or penetration testing. The standard does not use a specific model, but instead requires that the model used be consistent in terms of its representation of threats, their capabilities, and their qualifications as per the organization being tested, and the ability to repeatedly be applied to future tests with the same results. The standard focuses on two key elements of traditional threat modeling - *assets and attacker* (threat community/agent).

#### Vulnerability Assessment

Vulnerability testing is the process of discovering flaws in systems and applications which can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration, or insecure application design.

#### Exploitation

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions.

#### Reporting

This document is intended to define the base criteria for penetration testing reporting. While it is highly encouraged to use your own customized and branded format, the following should provide a high-level understanding of the items required within a report as well as a structure for the report to provide value to the reader.

## Method

The selection of method is based on the methodologies. For testing of web-based applications OWASP is selected as it is very known methodology for testing of web-based applications. To test the network infrastructure the PTES methodology is selected. Both methodologies have complete set of online documentation which also includes tools. The OWASP has 10 controls which deals with the web-based applications and guides proper testing in both phases whether only the vulnerability or also the penetration testing. PTES is a procedure of conduction penetration which can be adopted easily, and which is why it is very widely used for vulnerability and penetration testing.

## Compliance

As there are many compliances available online and up till now two of them i.e., ISO 27001 and PCI were used to observe controls provided by methods. The OWASP is mainly focused and tested under both compliances where PTES only with ISO 27001. The comparison to what the methods could relate with compliances are given below:

### ISO 27001 for OWASP

The security controls considered for ISO 27001 for OWASP are as:

* Annex A.5 – Information Security Policies
* Annex A.6 – Organization of Information Security
* Annex A.7 – Human Resource Security
* Annex A.8 – Asset Management
* Annex A.9 – Access Control
* Annex A.10 – Cryptography
* Annex A.11 – Physical & Environmental Security
* Annex A.12 – Operations Security
* Annex A.13 – Communications Security
* Annex A.14 – System Acquisition, Development & Maintenance
* Annex A.15 – Supplier Relationships
* Annex A.16 – Information Security Incident Management
* Annex A.17 – Information Security Aspects of Business Continuity Management
* Annex A.18 – Compliance

The detailed documentation is provided in appendix A.

### PCI for OWASP

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **PCI DSS Security Controls** | **OWASP Top 10 - Mapping** | **STATUS** |
| *1* | **USE AND MAINTAIN FIREWALLS** | The maintenance of firewalling is addressed by OWASP, officially OWASP has mentioned tool name “WAF” for managing firewall. Also, providing protection against common attacks like cross-site scripting (XSS) and SQL Injection where both comes under the rules of OWASP. | **✅** |
| *2* | **PROPER PASSWORD PROTECTIONS** | To protect passwords, OWASP has password protection set of rule which is authentication, mentioning all the possible solutions for password protection. To dig more information they have online page with reference to all the possible solutions i.e. https://owasp.org/www-pdf-archive/OWASP\_Application\_Security\_Verification\_Standard\_4.0-en.pdf. | **✅** |
| *3* | **PROTECT CARDHOLDER DATA** | OWASP has many ways to provide proper set of security controls on protection of card holder data. According to PCI, encryption should be done to protect the information of the client and OWASP also guides for testing of weak encryption standards. Moreover, they also has solution to cover sensitive data exposure, insecure deserialization and broken authentication for protecting the cardholder data in many ways. | **✅** |
| *4* | **ENCRYPT TRANSMITTED DATA** | The testing of this part is also provided by OWASP. To protect the data OWASP tests for the weak ciphers, SSL/TLS, insufficient transport layer protection and moreover the sensitive/unencrypted channels through which traffic is sent. | **✅** |
| *5* | **USE AND MAINTAIN ANTI-VIRUS** | There is no specifically mentioned use of anti-virus, however, the security configuration principle of OWASP in which patches need to be updated and maintained may serve the purpose. | **~** |
| *6* | **PROPERLY UPDATED SOFTWARE** | The OWASP guides to keep the security patches up to date to maintain all the libraries and frameworks securely configured. | **✅** |
| *7* | **RESTRICT DATA ACCESS** | The access control principle provides complete guidelines how to manage access controls on data, moreover, session management is also provided by the OWASP where to keep the session protected in order to protect data leakage. | **✅** |
| *8* | **UNIQUE IDS FOR ACCESS** | The OTG has a complete set of rules for creating id and providing access controls. To provide security everything is available in the checklist along with different sets of testing. | **✅** |
| *9* | **RESTRICT PHYSICAL ACCESS** | The physical access is mentioned to some extent under components with known vulnerabilities. To keep secure access to everything it is needed to avoid use of components with known vulnerabilities. | **✅** |
| *10* | **CREATE AND MAINTAIN ACCESS LOGS** | Logging and monitoring is one of the principle of OWASP to keep the data secure otherwise attack could be possible in form of tampering, extracting or destruction of data etc. | **✅** |
| *11* | **SCAN AND TEST FOR VULNERABILITIES** | OWASP itself is methodology to find vulnerabilities in the infrastructure. The top 10 principles is well known to do all scanning and testing with tools as officially mentioned online. | **✅** |
| *12* | **DOCUMENT POLICIES** | The cheat sheets for tasks are available but no such documentation for policy is mentioned by OWASP. | 🞬 |

### ISO 27001 for PTES

The security controls as mentioned in section 3.3.1 are same and detailed analysis is in the appendix section B.

## Platform

The platform is Debian based 64-bit operating system KALI Linux. It is well known platform among penetration testers and to conduct vulnerability assessments. It comes with pre-loaded tools and can be used for different infrastructures.

## Tools

The selection criteria for tools are that they are open-sourced and moreover fulfilling over requirement of integration although which will be checked during the development phase. The tools selected are not final and more tools could be added further as per the requirements. The tools which are selected is come with fulfilling the criteria of the compliances.

(TOOLS-PLATFORM-WORKING)

## Development

### Tools combination & sequence

The combination of tools is based on the procedure of gathering intelligence afterwards according to requirements performing vulnerability assessments and for that different combination of tools will be used and if penetration test will be required then for exploits different set of tools will be selected for testing. The controls of OWASP for web applications and PTES for network infrastructure are used and in even in future will be used to make different combinations of tools. Multiple tools like snort, OpenVas etc. will be built on kali Linux platform and will serve the purpose as per requirement as if someone needed them for vulnerability assessment and similarly if someone asks for exploits then to gather information regarding vulnerabilities such tools will be used again. Also, this platform is not limited to only these tools as this is initial stage of research and further as per requirements more tools will be come under it. Afterwards, reporting tools are also which can build a solid report however different features will be selected as per the requirements.

### Scripting for integration of tools over kali platform for VA & PT

The next phase after combination and sequence is their scripts. As selection is based on open source, so the scripts could be modified or specific part of them will be extracted and those features will be used to build up the strong platform. The scripts used for building vulnerability assessment will be different, but they will also be used in the penetration testing.

### Build for Vulnerability Test.

As mentioned, the vulnerability assessments will include the combination of intelligence gathering, enumeration, vulnerability scanner and post reporting tools. The build for them is based on the requirements set and more tools could be added to add more features in the platform.

### Build for Pen Test

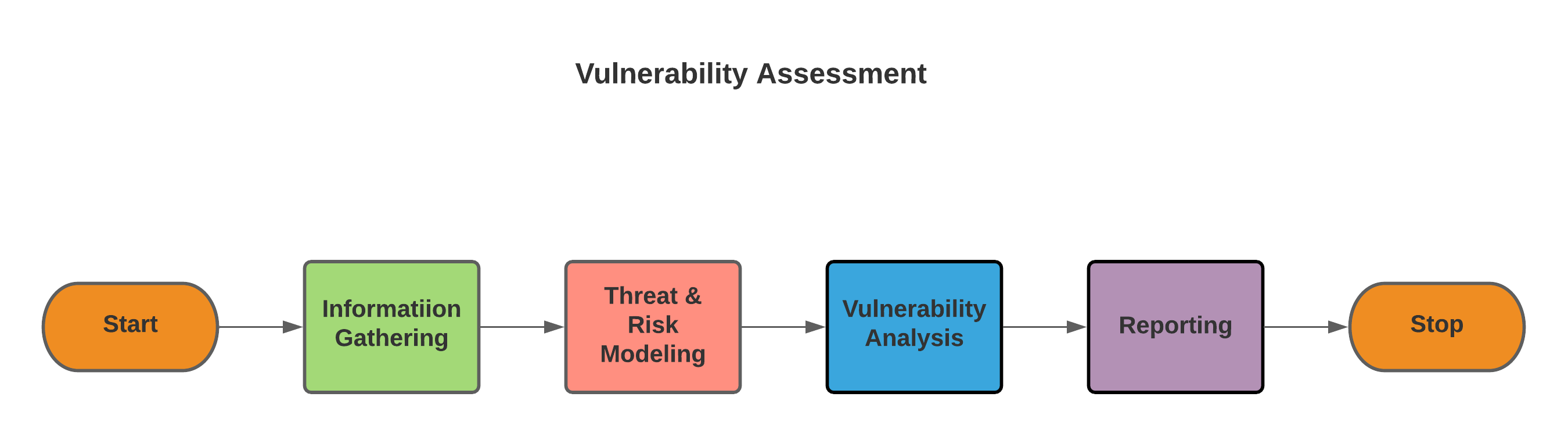
As mentioned, the penetration test will include the combination of intelligence gathering, enumeration, vulnerability scanners, exploiting tools and some external resources like dictionaries globally used to do brute force etc., and post reporting tools. The build for them is also based on the requirements set and more tools could be added to add more features in the platform.

# Scope of Vulnerability Assessment

The scope of the test will be decided before performing any scan for assessment. Defining the scope is very important that what specifically is going to be tested and under what conditions. The scope is to identify the machines, systems and network, optional requirements and sometimes the staff involved. The other thing is to understand the mindset of the client that what services the client wants to get tested and to what extent the scans will be performed as there are conditions when no results are obtained or sometimes those vulnerabilities are obtained which are not exploitable but still needs to get fixed. The range of IP addresses should be discussed to know which of them are in the engagement process. It must be verified that the client owns all the components as involving the target environments: DNS server, email server, actual hardware their web servers run on and their firewall/IDS/IPS solution. At the end, the best approach is coming up with disclosure agreement and rules of engagement to fix the boundaries.

*The sample of rules of engagement for vulnerability assessment are mentioned appendix C.*

# Process of Vulnerability Assessment



## Information Gathering

Information gathering is the foundation of performing vulnerability assessment. The more useful information about the target the more chances of successes to find vulnerabilities. Some information is obtained simply by doing Google and some of it obtained through automated tools. The information could be of any type like business nature, physical location, business terms, business structure etc. moreover, if state is involved then this form of gathering information is level 3, including a lot of manual and heavy analysis also deep understanding is obtained during the whole process. The information will be gathered in form of end points of the client which can be physical, electronic or human. There are several things to observe as identification and naming of the target, consider the rules of engagement if any, make time metrics for the assessment and always keep the end goal of the test. After all the above process proceed to next phase.

## Threat and Risks Modeling

The model focusses on the two key element which are assets and attacker. Each one is respectively broken down into business assets and business processes and the threat communities and their capabilities. While doing the modeling the business SWOT analysis will be considered and capabilities of the business which will target the technical side. So, basically it will be those activities performed for improving security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. Threat modeling is a planned activity for identifying and assessing application threats and vulnerabilities defining threat agents and assets. The questions during this phase which will be addressed are as:

* What are we working on?
* What can go wrong?
* What are we going to do about it?
* Did we do a good job

## Vulnerability Analysis

The process of discovering flaws in the system and applications which can lead towards halting or escalation privileges. The flaws can come from anywhere range from host and misconfiguration or issues in the application designs.

While performing vulnerability analysis of any type the tester should properly scope the testing for applicable depth and breadth to meet the goals and/or requirements of the desired outcome. To reach the goals, things to consider are location of an assessment tool, authentication requirements, target networks, segments, hosts, application, inventories, etc.

The analysis is based on active or passive scanning involving automated tools as network scanners, service based, banner grabbing, web application scanners, directory listing, voice network scanners, monitoring traffic, etc. The vulnerabilities obtained are also marked as per there severity level grading on a scale 0 to 10 and report is presented in post-test report.

## Reporting

The post reporting is a report which can be customized depending upon the nature of the assessment or as per the requirement of the client. Although, the report should include all the aspects of the assessment from first to last stage. The general structure of the report which is followed is as:

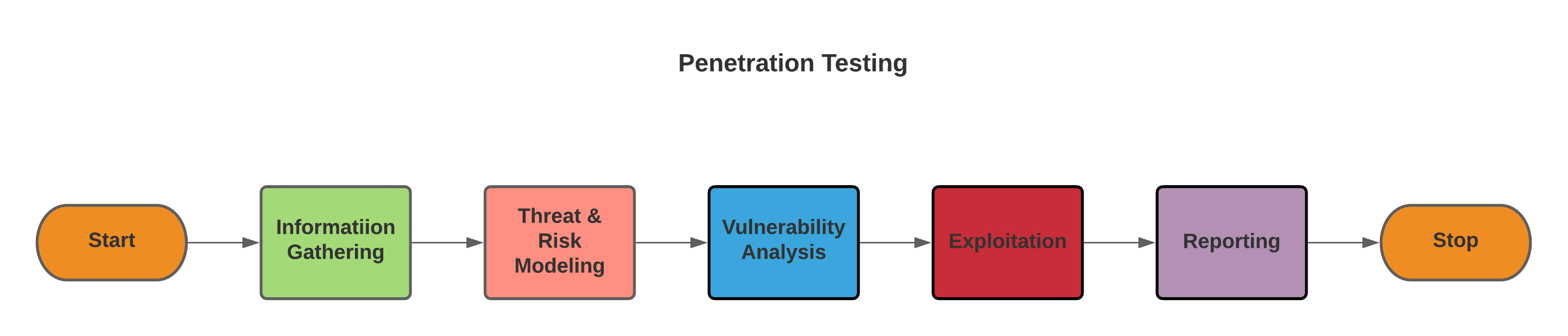
* Executive summary
* Background
* Risk Ranking
* Findings
* Technical Details
  + Information gathering
  + Threat & Risk model
  + Vulnerability Analysis
* Conclusion/Solution

# Scope of Pentest Assessment

The scope of the test will be decided before performing any scan and exploit for penetration testing. Defining the scope is very important that what specifically is going to be tested and under what conditions also the exploits to what extent are demanded from the client end. The scope is to identify the machines, systems and network, optional requirements and sometimes the staff involved. The other thing is to understand the mindset of the client that what services the client wants to get tested and to what extent the scans will be performed and then which vulnerabilities the client want to check for exploits as there are conditions when no results are obtained or sometimes those vulnerabilities are obtained which are not exploitable but still needs to get fixed and also such vulnerabilities if not exploitable then hassle of conducting penetration test will be costly and time consuming which is why scope needs to get defined. The range of IP addresses should be discussed to know which of them are in the engagement process. Moreover, it is also to know which IP specifically the client wants to get exploited as there might be range of IP’s. It must be verified that the client owns all the components as involving the target environments: DNS server, email server, actual hardware their web servers run on and their firewall/IDS/IPS solution. At the end, the best approach is coming up with disclosure agreement and rules of engagement to fix the boundaries.

*The sample of rules of engagement for penetration testing are mentioned appendix D.*

# Process of Penetration Test



## Information Gathering

Information gathering is the foundation of performing penetration test. The more useful information about the target the more chances of successes to find vulnerabilities and exploiting those vulnerabilities. Some information is obtained simply by doing Google and some of it obtained through automated tools. The information could be of any type like business nature, physical location, business terms, business structure etc. moreover, if state is involved then this form of gathering information is level 3, including a lot of manual and heavy analysis also deep understanding is obtained during the whole process. The information will be gathered in form of end points of the client which can be physical, electronic or human. There are several things to observe as identification and naming of the target, consider the rules of engagement if any, make time metrics for the assessment and always keep the end goal of the test. After all the above process proceed to next phase.

## Threat and Risks Modeling

The model focusses on the two key element which are assets and attacker. Each one is respectively broken down into business assets and business processes and the threat communities and their capabilities. While doing the modeling the business SWOT analysis will be considered and capabilities of the business which will target the technical side. So, basically it will be those activities performed for improving security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. Threat modeling is a planned activity for identifying and assessing application threats and vulnerabilities defining threat agents and assets. The questions during this phase which will be addressed are as:

* What are we working on?
* What can go wrong?
* What are we going to do about it?
* Did we do a good job

## Vulnerability Analysis

The process of discovering flaws in the system and applications which can lead towards halting or escalation privileges. The flaws can come from anywhere range from host and misconfiguration or issues in the application designs.

While performing vulnerability analysis of any type the tester should properly scope the testing for applicable depth and breadth to meet the goals and/or requirements of the desired outcome. To reach the goals, things to consider are location of an assessment tool, authentication requirements, target networks, segments, hosts, application, inventories, etc.

The analysis is based on active or passive scanning involving automated tools as network scanners, service based, banner grabbing, web application scanners, directory listing, voice network scanners, monitoring traffic, etc. The vulnerabilities obtained are also marked as per there severity level grading on a scale 0 to 10 and report is presented in post-test report.

## Exploitation

This phase is based on the prior phase i.e. vulnerability analysis. At this phase it is tried to get establish access to a system or resource by bypassing security restrictions. The exploitation phase should be much planned for a precision strike. The focus is laid to identify the main entry point into the organization and to identify high value target assets. If the phase completes properly than a high valued target list is compiled and suggestions for the attack vectors are provided. The exploitation is detailed process and sometimes based on hit and trial approach however the vulnerability analysis is the base which should be good so to get maximum of the success.

## Post-Exploitation Report

The post reporting is a report which can be customized depending upon the nature of the assessment or as per the requirement of the client. Although, the report should include all the aspects of the assessment from first to last stage. The general structure of the report which is followed is as:

* Executive summary
* Background
* Risk Ranking
* Findings
* Technical Details
  + Information gathering
  + Threat & Risk model
  + Vulnerability Analysis
  + Exploits
* Conclusion/Solution

# Appendixes

## Appendix A:

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27001 Security Controls and OWASP** | | |  |
| **Section** | **Information security control** | **Compliance** | **Remarks** |
| **A5** | **Information security policies** |  |  |
| **A5.1** | **Management direction for information security** |  |  |
| A5.1.1 | Policies for information security | NO |  |
| A5.1.2 | Review of the policies for information security | NO |  |
| **NOTES** | The management of the policies is not defined and not applicable on OWASP, as it is a testing methodology but it can review the policies but strictly being around to its' top 10. | |  |
| **A6** | **Organization of information security** |  |  |
| **A6.1** | **Internal organization** |  |  |
| A6.1.1 | Information security roles and responsibilities | YES |  |
| A6.1.2 | Segregation of duties | YES |  |
| A6.1.3 | Contact with authorities | NO |  |
| A6.1.4 | Contact with special interest groups | NO |  |
| A6.1.5 | Information security in project management | NO |  |
| **NOTES** | Defining roles in accordance with the access controls and similarly segregating the duties come under OWASP top 10 however if it based on organizations internal structure than OWASP is not linked. | |  |
| **A6.2** | **Mobile devices and teleworking** |  |  |
| A6.2.1 | Mobile device policy | NO |  |
| A6.2.2 | Teleworking |  | PARTIAL |
| **NOTES** | The working structure under teleworking can be tested by OWASP under the given set of policies of the organization. | |  |
| **A7** | **Human resource security** |  |  |
| **A7.1** | **Prior to employment** |  |  |
| A7.1.1 | Screening | NO |  |
| A7.1.2 | Terms and conditions of employment | NO |  |
| **NOTES** | This section has no link with the OWASP top 10 principles. | |  |
| **A7.2** | **During employment** |  |  |
| A7.2.1 | Management responsibilities | NO |  |
| A7.2.2 | Information security awareness, education and training | YES |  |
| A7.2.3 | Disciplinary process | NO |  |
| **NOTES** | For the awareness OWASP has proper set of documentation which is officially available online and organization can study and could make policies accordingly. | |  |
| **A7.3** | **Termination and change of employment** |  |  |
| A7.3.1 | Termination or change of employment responsibilities | YES |  |
| **NOTES** | The termination of employees or responsibilities has no direct link with the OWASP however, considering the access controls or to sensitive data exposure then OWASP could be linked otherwise has no direct link with this section. | |  |
| **A8** | **Asset management** |  |  |
| **A8.1** | **Responsibility for assets** |  |  |
| A8.1.1 | Inventory of assets | NO |  |
| A8.1.2 | Ownership of assets | NO |  |
| A8.1.3 | Acceptable use of assets | YES |  |
| A8.1.4 | Return of assets | NO |  |
| **NOTES** | OWASP however highlights dealing with using components of known vulnerabilities however there is need to make up the inventory of the assets to reduce their usage and prevent from any further damage if any. | |  |
| **A8.2** | **Information classification** |  |  |
| A8.2.1 | Classification of information | NO |  |
| A8.2.2 | Labelling of information |  | PARTIAL |
| A8.2.3 | Handling of assets | NO |  |
| **NOTES** | No information classification found in the OWASP however OWASP in monitoring and logging asks to monitor the web applications which can be further enhanced in terms of information classification i.e. confidential, private, public etc. Logging and monitoring by OWASP is mentioned but to very limited scale which can be used for fulfilling this section of OWASP. | |  |
| **A8.3** | **Media handling** |  |  |
| A8.3.1 | Management of removable media | NO |  |
| A8.3.2 | Disposal of media | NO |  |
| A8.3.3 | Physical media transfer | NO |  |
| **NOTES** | Media handling w.r.t web applications is an important part which should be described because loss or theft of any media or if dumping of media goes wrong than an organization could suffer severe circumstances and OWASP has no criteria mentioned to handle the media as per the above stated points. | |  |
| **A9** | **Access control** |  |  |
| **A9.1** | **Business requirements of access control** |  |  |
| A9.1.1 | Access control policy | NO |  |
| A9.1.2 | Access to networks and network services | YES |  |
| **NOTES** | The policy depends upon the organization and every penetration tester should come with the rules of engagement and disclosure agreements so it does not apply on the OWASP but a basic pre-engagement step for every pen-tester. However, if considering the OWASP checklist documentation it can be seen there are number of experiments fulfilling the criteria for access controls. | |  |
| **A9.2** | **User access management** |  |  |
| A9.2.1 | User registration and de-registration | YES |  |
| A9.2.2 | User access provisioning | YES |  |
| A9.2.3 | Management of privileged access rights | YES |  |
| A9.2.4 | Management of secret authentication information of users | YES |  |
| A9.2.5 | Review of user access rights | YES |  |
| A9.2.6 | Removal or adjustment of access rights | YES |  |
| **NOTES** | This section is managed very carefully by OWASP, in the OTG checklist full control is managed in terms of testing this domain. | |  |
| **A9.3** | **User responsibilities** |  |  |
| A9.3.1 | Use of secret authentication information | YES |  |
| **NOTES** | The secret authentication is defined not directly but testing in terms of session management, cache checks, weak credentials etc. also the testing of authentication indirectly fulfills the secret authentication. | |  |
| **A9.4** | **System and application access control** |  |  |
| A9.4.1 | Information access restriction | YES |  |
| A9.4.2 | Secure log-on procedures | YES |  |
| A9.4.3 | Password management system | YES |  |
| A9.4.4 | Use of privileged utility programs | YES |  |
| A9.4.5 | Access control to program source code | YES |  |
| **NOTES** | The access controls alongside broken authentication is very well managed in the OWSAP, very well list of testing presented in the checklist along with the tools. | |  |
| **A10** | **Cryptography** |  |  |
| **A10.1** | **Cryptographic controls** |  |  |
| A10.1.1 | Policy on the use of cryptographic controls | NO |  |
| A10.1.2 | Key management |  | PARTIAL |
| **NOTES** | Specifically, key management is not mentioned in the scope of OWASP, however, considering cryptographic approach OWASP checks for encryption standards and also one of the main point of sensitive data exposures describes importance of data. Moreover, insecure deserialization also focusses on the this schema. | |  |
| **A11** | **Physical and environmental security** |  |  |
| **A11.1** | **Secure areas** |  |  |
| A11.1.1 | Physical security perimeter | NO |  |
| A11.1.2 | Physical entry controls | NO |  |
| A11.1.3 | Securing offices, rooms and facilities |  | PARTIAL |
| A11.1.4 | Protecting against external and environmental threats |  | PARTIAL |
| A11.1.5 | Working in secure areas | NO |  |
| A11.1.6 | Delivery and loading areas | NO |  |
| **NOTES** | OWASP is a testing methodology specifically for web applications and it is about testing the applications based on web or cloud. So, it does not involve any channels to secure physical structure. | |  |
| **A11.2** | **Equipment** |  |  |
| A11.2.1 | Equipment siting and protection | NO |  |
| A11.2.2 | Supporting utilities | YES |  |
| A11.2.3 | Cabling security | NO |  |
| A11.2.4 | Equipment maintenance | YES |  |
| A11.2.5 | Removal of assets |  | PARTIAL |
| A11.2.6 | Security of equipment and assets off-premises |  | PARTIAL |
| A11.2.7 | Secure disposal or reuse of equipment | YES |  |
| A11.2.8 | Unattended user equipment | YES |  |
| A11.2.9 | Clear desk and clear screen policy | NO |  |
| **NOTES** | The OWASP in its sensitive data exposure and components with known vulnerabilities section address some of the issues to not use components or remove any components with known vulnerabilities. | |  |
| **A12** | **Operations security** |  |  |
| **A12.1** | **Operational procedures and responsibilities** |  |  |
| A12.1.1 | Documented operating procedures | YES |  |
| A12.1.2 | Change management | YES |  |
| A12.1.3 | Capacity management | NO |  |
| A12.1.4 | Separation of development, testing and operational environments | NO |  |
| **NOTES** | The documentation is the initial phase for any pen-tester however OWASP also provides documentation standards including OTG and OTG checklist also other documentations officially where change management is defined in terms of access controls and authorization part. However, capacity management is not applicable which is to be done between the organizations and therefore OWASP does not provide any support related to it. | |  |
| **A12.2** | **Protection from malware** |  |  |
| A12.2.1 | Controls against malware | YES |  |
| **NOTES** | This is the main thing which OWASP is known for so it basically provides all the guidelines in various way defined in OTG/ OTG checklist, which discusses various standards in accordance to protection against malware. | |  |
| **A12.3** | **Backup** |  |  |
| A12.3.1 | Information backup |  | PARTIAL |
| **NOTES** | Backup is not directly defined but however OWASP in various ways targets to backup the files or make them encrypted to ensure confidentiality and integrity. | |  |
| **A12.3** | **Logging and monitoring** |  |  |
| A12.4.1 | Event logging | YES |  |
| A12.4.2 | Protection of log information | YES |  |
| A12.4.3 | Administrator and operator logs | YES |  |
| A12.4.4 | Clock synchronization |  | PARTIAL |
| **NOTES** | OWASP provides in its top 10 section related to insufficient logging and monitoring and shows the importance to manage and protect logs in order to stay safe from an exploits. | |  |
| **A12.5** | **Control of operational software** |  |  |
| A12.5.1 | Installation of software on operational systems | YES |  |
| **NOTES** | The security and misconfiguration section of OWASP deals with the insecure or outdated patches which should be updated or removed and hence any installation depends on such configuration files. | |  |
| **A12.6** | **Technical vulnerability management** |  |  |
| A12.6.1 | Management of technical vulnerabilities | YES |  |
| A12.6.2 | Restrictions on software installation | YES |  |
| **NOTES** | The management of technical vulnerabilities and proper testing method alongside tools are discussed in the OWASP top 10. The access controls and authorization deals with the restriction part of the software installation. | |  |
| **A12.7** | **Information systems audit considerations** |  |  |
| A12.7.1 | Information systems audit controls | YES |  |
| **NOTES** | The controls in access controls section of OWASP also authorization deals with the above stated auditing. | |  |
| **A13** | **Communications security** |  |  |
| **A13.1** | **Network security management** |  |  |
| A13.1.1 | Network controls | YES |  |
| A13.1.2 | Security of network services | YES |  |
| A13.1.3 | Segregation in networks |  | PARTIAL |
| **NOTES** | The controls along with testing are very well described in the OWASP, access controls and testing of several services on the network like WebDAV, FTP, backend DB server etc. are defined by OWASP also in the OTG checklist. The network segregation is defined as in-directly involving controls of access and services. | |  |
| **A13.2** | **Information transfer** |  |  |
| A13.2.1 | Information transfer policies and procedures | NO |  |
| A13.2.2 | Agreements on information transfer | NO |  |
| A13.2.3 | Electronic messaging | YES |  |
| A13.2.4 | Confidentiality or nondisclosure agreements | YES |  |
| **NOTES** | The transfer of information is addressed in terms of encryption and testing of information access, authorization and injection etc. | |  |
| **A14** | **System acquisition, development & maintenance** |  |  |
| **A14.1** | **Security requirements of information systems** |  |  |
| A14.1.1 | Information security requirements analysis and specification | NO |  |
| A14.1.2 | Securing application services on public networks | YES |  |
| A14.1.3 | Protecting application services transactions | YES |  |
| **NOTES** | The need of requirements should be defined in the OWASP which has importance in understanding the infrastructure to work on, also on the other side application services are defined and ways to protect in different formats are very well mentioned in the OTG along with services transactions. | |  |
| **A14.2** | **Security in development and support processes** |  |  |
| A14.2.1 | Secure development policy | NO |  |
| A14.2.2 | System change control procedures | YES |  |
| A14.2.3 | Technical review of applications after operating platform changes | YES |  |
| A14.2.4 | Restrictions on changes to software packages | YES |  |
| A14.2.5 | Secure system engineering principles | NO |  |
| A14.2.6 | Secure Development Environment | NO |  |
| A14.2.7 | Outsourced development | NO |  |
| A14.2.8 | System security testing | YES |  |
| A14.2.9 | System acceptance testing | NO |  |
| **NOTES** | The OWASP is cloud based methodology to find the vulnerabilities in the web application but to protect provide solutions accordingly but system engineering rules and testing is not application on OWASP as engineering is something different however after the implementation of engineering principles OWASP can test the web based services or applications. | |  |
| **A14.3** | **Test data** |  |  |
| A14.3.1 | Protection of test data |  | PARTIAL |
| **NOTES** | It depends what kind of test data is there if it is in accordance with the OWASP then it can be testing with top 10 rules of OWASP. | |  |
| **A15** | **Supplier relationships** |  |  |
| **A15.1** | **Information security in supplier relationships** |  |  |
| A15.1.1 | Information security policy for supplier relationships | NO |  |
| A15.1.2 | Addressing security within supplier agreements | NO |  |
| A15.1.3 | ICT supply chain | NO |  |
| **NOTES** | The above section is solely based on the organization and the policies they have with their suppliers. | |  |
| **A15.2** | **Supplier service delivery management** |  |  |
| A15.2.1 | Monitoring and review of supplier services | NO |  |
| A15.2.2 | Managing changes to supplier services | NO |  |
| **NOTES** | The OWASP has no engagements with these policies as they are organization based. | |  |
| **A16** | **Information security incident management** |  |  |
| **A16.1** | **Management of information security incidents & improvements** |  |  |
| A16.1.1 | Responsibilities and procedures | NO |  |
| A16.1.2 | Reporting information security events | NO |  |
| A16.1.3 | Reporting information security weaknesses | NO |  |
| A16.1.4 | Assessment of and decision on information security events | NO |  |
| A16.1.5 | Response to information security incidents | NO |  |
| A16.1.6 | Learning from information security incidents | NO |  |
| A16.1.7 | Collection of evidence | NO |  |
| **NOTES** | The incidence response plan is managed by the incident response team, this has no link with the OWASP however, organization should have its' own security team to deal and plan if some incident occurs. Moreover, incidence response team can consider OWASP top 10 to build up the security model. | |  |
| **A17** | **Information security aspects of BCM** |  |  |
| **A17.1** | **Information security continuity** |  |  |
| A17.1.1 | Planning information security continuity | NO |  |
| A17.1.2 | Implementing information security continuity | NO |  |
| A17.1.3 | Verify, review and evaluate information security continuity | NO |  |
| **NOTES** | Deciding the continuity model is the internal responsibility of the organization but an organizaiton can check OWASP top 10 to make a model but directly OWASP has no link with this part. | |  |
| **A17.2** | **Redundancies** |  |  |
| A17.2.1 | Availability of information processing facilities | NO |  |
| **NOTES** | The business continuity management is to make sure things are available even is breakdown occurs so it is not applicable for OWASP however the internal testing team is responsible for the smooth running of business if any incidence takes place. | |  |
| **A18** | **Compliance** |  |  |
| **A18.1** | **Compliance with legal and contractual requirements** |  |  |
| A18.1.1 | Identification of applicable legislation and contractual requirements | NO |  |
| A18.1.2 | Intellectual property rights | NO |  |
| A18.1.3 | Protection of records | YES |  |
| A18.1.4 | Privacy and protection of personally identifiable information | YES |  |
| A18.1.5 | Regulation of cryptographic controls |  | PARTIAL |
| **NOTES** | If considering the testing aspect then OWASP fulfills the protection however if building up the compliance then OWASP has no link with this section. | |  |
| **A18.2** | **Information security reviews** |  |  |
| A18.2.1 | Independent review of information security |  | PARTIAL |
| A18.2.2 | Compliance with security policies and standards | NO | Not applicable |
| A18.2.3 | Technical compliance review | NO | Not applicable |
| **NOTES** | The review section for the compliance of the organization is limited because OWASP has to stick with its top 10 rules. | |  |

## Appendix B:

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27001 Security Controls and PTES** | |  |  |
| **Section** | **Information security control** | **Compliance** | **Remarks** |
| **A5** | **Information security policies** |  |  |
| **A5.1** | **Management direction for information security** |  |  |
| A5.1.1 | Policies for information security | NO |  |
| A5.1.2 | Review of the policies for information security | NO |  |
| **NOTES** | The management of the policies is not defined and not applicable however the pre-engagement step include rules of engagement and timing metrics etc. |  |  |
| **A6** | **Organization of information security** |  |  |
| **A6.1** | **Internal organization** |  |  |
| A6.1.1 | Information security roles and responsibilities | NO |  |
| A6.1.2 | Segregation of duties | NO |  |
| A6.1.3 | Contact with authorities | NO |  |
| A6.1.4 | Contact with special interest groups | NO |  |
| A6.1.5 | Information security in project management | NO |  |
| **NOTES** | PTES does not deal with this section. |  |  |
| **A6.2** | **Mobile devices and teleworking** |  |  |
| A6.2.1 | Mobile device policy | NO |  |
| A6.2.2 | Teleworking |  | PARTIAL |
| **NOTES** | The PTES only involves a little part of testing in terms of Wi-Fi. |  |  |
| **A7** | **Human resource security** |  |  |
| **A7.1** | **Prior to employment** |  |  |
| A7.1.1 | Screening | NO |  |
| A7.1.2 | Terms and conditions of employment | NO |  |
| **NOTES** | This section has no link with the PTES technical guidelines. |  |  |
| **A7.2** | **During employment** |  |  |
| A7.2.1 | Management responsibilities | NO |  |
| A7.2.2 | Information security awareness, education and training |  | PARTIAL |
| A7.2.3 | Disciplinary process | NO |  |
| **NOTES** | For the awareness organizations may refer to PTES technical guidelines. |  |  |
| **A7.3** | **Termination and change of employment** |  |  |
| A7.3.1 | Termination or change of employment responsibilities | NO |  |
| **NOTES** | There is no policy or any principle under this section. |  |  |
| **A8** | **Asset management** |  |  |
| **A8.1** | **Responsibility for assets** |  |  |
| A8.1.1 | Inventory of assets | NO |  |
| A8.1.2 | Ownership of assets | NO |  |
| A8.1.3 | Acceptable use of assets | NO |  |
| A8.1.4 | Return of assets | NO |  |
| **NOTES** | The PTES should have asset management but although it is not present in PTES. |  |  |
| **A8.2** | **Information classification** |  |  |
| A8.2.1 | Classification of information | NO |  |
| A8.2.2 | Labelling of information | NO |  |
| A8.2.3 | Handling of assets | NO |  |
| **NOTES** | PTES does not classify any information however, there are tools which can dig the websites and harvest the important information from the network. |  |  |
| **A8.3** | **Media handling** |  |  |
| A8.3.1 | Management of removable media | NO |  |
| A8.3.2 | Disposal of media | NO |  |
| A8.3.3 | Physical media transfer | NO |  |
| **NOTES** | PTES does not include any documentation regarding physical medium issues. |  |  |
| **A9** | **Access control** |  |  |
| **A9.1** | **Business requirements of access control** |  |  |
| A9.1.1 | Access control policy | NO |  |
| A9.1.2 | Access to networks and network services | YES |  |
| **NOTES** | There is no policy however there are range of tools mentioned by PTES to test the networks and services. |  |  |
| **A9.2** | **User access management** |  |  |
| A9.2.1 | User registration and de-registration | YES |  |
| A9.2.2 | User access provisioning | YES |  |
| A9.2.3 | Management of privileged access rights | YES |  |
| A9.2.4 | Management of secret authentication information of users | YES |  |
| A9.2.5 | Review of user access rights | YES |  |
| A9.2.6 | Removal or adjustment of access rights | YES |  |
| **NOTES** | Removal or adjustment of access rights are not provided by PTES however through intelligence gathering section several tools can be used which will provide many useful information. |  |  |
| **A9.3** | **User responsibilities** |  |  |
| A9.3.1 | Use of secret authentication information | YES |  |
| **NOTES** | To prevent the above situation, PTES provides ability to test the network by brute forcing or sniffing using tools like Wireshark etc. moreover, running vulnerability scanners can provide more vulnerabilities related to authentication issues. |  |  |
| **A9.4** | **System and application access control** |  |  |
| A9.4.1 | Information access restriction |  | PARTIAL |
| A9.4.2 | Secure log-on procedures |  | PARTIAL |
| A9.4.3 | Password management system |  | PARTIAL |
| A9.4.4 | Use of privileged utility programs |  | PARTIAL |
| A9.4.5 | Access control to program source code |  | PARTIAL |
| **NOTES** | There is no clause to implement restriction, however after vulnerability assessment one can know how to secure the above stated information. |  |  |
| **A10** | **Cryptography** |  |  |
| **A10.1** | **Cryptographic controls** |  |  |
| A10.1.1 | Policy on the use of cryptographic controls | NO |  |
| A10.1.2 | Key management |  | PARTIAL |
| **NOTES** | PTES can address these issues as mentioned online in key distribution attack section but there is no well defined explanation for this section. |  |  |
| **A11** | **Physical and environmental security** |  |  |
| **A11.1** | **Secure areas** |  |  |
| A11.1.1 | Physical security perimeter | NO |  |
| A11.1.2 | Physical entry controls | NO |  |
| A11.1.3 | Securing offices, rooms and facilities | NO |  |
| A11.1.4 | Protecting against external and environmental threats | NO |  |
| A11.1.5 | Working in secure areas | NO |  |
| A11.1.6 | Delivery and loading areas | NO |  |
| **NOTES** | PTES has no set of rules to deal with the physical and environmental section. |  |  |
| **A11.2** | **Equipment** |  |  |
| A11.2.1 | Equipment siting and protection | NO |  |
| A11.2.2 | Supporting utilities | NO |  |
| A11.2.3 | Cabling security | NO |  |
| A11.2.4 | Equipment maintenance | NO |  |
| A11.2.5 | Removal of assets | NO |  |
| A11.2.6 | Security of equipment and assets off-premises | NO |  |
| A11.2.7 | Secure disposal or reuse of equipment | NO |  |
| A11.2.8 | Unattended user equipment | NO |  |
| A11.2.9 | Clear desk and clear screen policy | NO |  |
| **NOTES** | The PTES framework does not cover this section. |  |  |
| **A12** | **Operations security** |  |  |
| **A12.1** | **Operational procedures and responsibilities** |  |  |
| A12.1.1 | Documented operating procedures | YES |  |
| A12.1.2 | Change management | YES |  |
| A12.1.3 | Capacity management | NO |  |
| A12.1.4 | Separation of development, testing and operational environments | NO |  |
| **A12.2** | **Protection from malware** |  |  |
| A12.2.1 | Controls against malware | YES |  |
| **A12.3** | **Backup** |  |  |
| A12.3.1 | Information backup |  | NO |
| **A12.3** | **Logging and monitoring** |  |  |
| A12.4.1 | Event logging | NO |  |
| A12.4.2 | Protection of log information | NO |  |
| A12.4.3 | Administrator and operator logs | NO |  |
| A12.4.4 | Clock synchronization | NO |  |
| **A12.5** | **Control of operational software** |  |  |
| A12.5.1 | Installation of software on operational systems | NO |  |
| **A12.6** | **Technical vulnerability management** |  |  |
| A12.6.1 | Management of technical vulnerabilities | NO |  |
| A12.6.2 | Restrictions on software installation | NO |  |
| **A12.7** | **Information systems audit considerations** |  |  |
| A12.7.1 | Information systems audit controls | NO |  |
| **NOTES** | In the above section A-12; the PTES deals in accordance to protect system form malwares through testing process and also to check whether the vulnerabilities could be exploitable or not through exploitation process. |  |  |
| **A13** | **Communications security** |  |  |
| **A13.1** | **Network security management** |  |  |
| A13.1.1 | Network controls | YES |  |
| A13.1.2 | Security of network services | YES |  |
| A13.1.3 | Segregation in networks | NO |  |
| **A13.2** | **Information transfer** |  |  |
| A13.2.1 | Information transfer policies and procedures | NO |  |
| A13.2.2 | Agreements on information transfer | NO |  |
| A13.2.3 | Electronic messaging | YES |  |
| A13.2.4 | Confidentiality or nondisclosure agreements | NO |  |
| **NOTES** | In section A-13; network issues are addressed through scanning the vulnerabilities using openVas, Nessus, neXpose etc. and after finding vulnerabilities checking for the exploits. The section 4 of PTES deals with exploitation. |  |  |
| **A14** | **System acquisition, development & maintenance** |  |  |
| **A14.1** | **Security requirements of information systems** |  |  |
| A14.1.1 | Information security requirements analysis and specification | NO |  |
| A14.1.2 | Securing application services on public networks | NO |  |
| A14.1.3 | Protecting application services transactions | YES |  |
| **A14.2** | **Security in development and support processes** |  |  |
| A14.2.1 | Secure development policy | NO |  |
| A14.2.2 | System change control procedures | NO |  |
| A14.2.3 | Technical review of applications after operating platform changes | YES |  |
| A14.2.4 | Restrictions on changes to software packages | NO |  |
| A14.2.5 | Secure system engineering principles | YES |  |
| A14.2.6 | Secure Development Environment | YES |  |
| A14.2.7 | Outsourced development | NO |  |
| A14.2.8 | System security testing | YES |  |
| A14.2.9 | System acceptance testing | NO |  |
| **A14.3** | **Test data** |  |  |
| A14.3.1 | Protection of test data | NO |  |
| **NOTES** | Section A-14; the main aim of securing services can be achieved by implementing PTES principles of gathering information, scanning for vulnerabilities and exploiting vulnerabilities if needed. However, no information is provided for restriction, or outsourcing etc. But can be achieved after scanning for vulnerabilities in the network. |  |  |
| **A15** | **Supplier relationships** |  |  |
| **A15.1** | **Information security in supplier relationships** |  |  |
| A15.1.1 | Information security policy for supplier relationships | NO |  |
| A15.1.2 | Addressing security within supplier agreements | NO |  |
| A15.1.3 | ICT supply chain | NO |  |
| **A15.2** | **Supplier service delivery management** |  |  |
| A15.2.1 | Monitoring and review of supplier services | NO |  |
| A15.2.2 | Managing changes to supplier services | NO |  |
| **NOTES** | There are no details for supplier relationships (A15) in PTES. |  |  |
| **A16** | **Information security incident management** |  |  |
| **A16.1** | **Management of information security incidents & improvements** | NO |  |
| A16.1.1 | Responsibilities and procedures | NO |  |
| A16.1.2 | Reporting information security events | NO |  |
| A16.1.3 | Reporting information security weaknesses | NO |  |
| A16.1.4 | Assessment of and decision on information security events | NO |  |
| A16.1.5 | Response to information security incidents | NO |  |
| A16.1.6 | Learning from information security incidents | NO |  |
| A16.1.7 | Collection of evidence |  |  |
| **NOTES** | The incidence response plan is managed by the incident response team, this has no link with the PTES however, organization should have its' own security team to deal and plan if some incident occurs. |  |  |
| **A17** | **Information security aspects of BCM** |  |  |
| **A17.1** | **Information security continuity** |  |  |
| A17.1.1 | Planning information security continuity | NO |  |
| A17.1.2 | Implementing information security continuity | NO |  |
| A17.1.3 | Verify, review and evaluate information security continuity | NO |  |
| **A17.2** | **Redundancies** | NO |  |
| A17.2.1 | Availability of information processing facilities | NO |  |
| **NOTES** | Section A17; The business continuity management is to make sure things are available even is breakdown occurs and deciding the continuity model is the internal responsibility of the organization. | NO |  |
| **A18** | **Compliance** |  |  |
| **A18.1** | **Compliance with legal and contractual requirements** |  |  |
| A18.1.1 | Identification of applicable legislation and contractual requirements |  |  |
| A18.1.2 | Intellectual property rights | NO |  |
| A18.1.3 | Protection of records | NO |  |
| A18.1.4 | Privacy and protection of personally identifiable information | NO |  |
| A18.1.5 | Regulation of cryptographic controls | NO |  |
| **NOTES** | If considering the testing aspect then PTES fulfills the protection however if building up the compliance then PTES has no link with this section. |  |  |
| **A18.2** | **Information security reviews** |  |  |
| A18.2.1 | Independent review of information security | NO |  |
| A18.2.2 | Compliance with security policies and standards | NO |  |
| A18.2.3 | Technical compliance review | NO |  |
| **NOTES** | Section A18; PTES is a procedure of implementing the vulnerability scan and the penetration test. So, there are many possibilities that this might not directly link to compliance but however the end approach is to protect the data. |  |  |

## Appendix C:

**Rules of Engagement**

Company-ABC takes the security of our guests and colleagues very seriously. Company-ABC hopes to raise its already high level of security standards, as well as learn from and collaborate with highly skilled Pentesters at XVZ Security Ltd. in order to keep our businesses and customers safe.

By taking this Pentesting project of Company-ABC you agree to follow all of the requirements below.

**1.      SLA**

* Duration: W1 – W 15
* Produce a comprehensive Vulnerability assessment report and Activity narrations.

**2.      Disclosure Policy**

Do not discuss this program or any vulnerabilities (even resolved ones) outside of the program without express consent from the undersigned.

**3.      Vulnerability Assessment Rules**

* Do not collect any personally identifiable information, authentication information, or credit card information from Company-ABC guests.
* Do not destroy or alter discovered data.
* Do not inappropriately store Company-ABC information in public locations.
* Do not intentionally harm guests as well as their experience.
* Do not publicly or privately disclose any vulnerabilities belonging to Company-ABC - existing or remediated - to anyone other than the undersigned.
* Contact undersigned about questions regarding vulnerabilities or any issues.
* Current Company-ABC employees and contractors should not be participated in this pentest.
* You cannot participate in this pentest if you have been an employee or a contractor of Company-ABC in the past six months.
* Please provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, the issue will not be accepted.
* Social engineering (e.g., phishing, vishing, smishing) is prohibited.
* Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.
* Limit automation/rate scraping to 100 requests per minute.
* Remove all changes you have made during the Vulnerability assessment.

**4.      Submission Requirements**

* All reports must be submitted through the ABC platform.
* Consolidated Pentest report must meet Task 4 requirements.

**5.      Testing Requirements**

**Test Accounts**

**Create** Company-ABC **test accounts to these specifications:**

* First name: < Company-ABC > (for multiple accounts - <handle>one, <handle>two, etc.).
* Last name: "**Test**".    
    
  Reservation Requirements    
    
  **If you must create bookings for testing purposes, follow these rules:**
* Test bookings should be made four months into the future at a minimum.
* All test bookings should be cancelled **as soon as possible**.
* Do not book London or Melbourne properties for testing purposes

**6.      In Scope**

**Assets**

* Company-ABC.com (no subdomain).
* [www.Company-ABC.com](http://www.Company-ABC.com) (no additional subdomains).
* world.Company-ABC.com (no additional subdomains).
* assets.Company-ABC.com (no additional subdomains).    
    
  **Vulnerabilities**
* Authentication bypass.
* Back-end system access via front-end systems.
* Business logic bypass resulting in financial gain to an attacker (e.g., forced rate change).
* Container escape.
* Discovery of Company-ABC data on other storage services.
* Highly creative means of automating account checking or rate scraping (e.g., botting).
* Highly creative means of discovering origin IP.
* Highly creative means of spoofing email messages.
* Other systems that may host Company-ABC information.
* SQL Injection.
* Cross-Site Request Forgery.
* Exploitable Cross-Site Scripting.
* Web Application Firewall (WAF) bypass.
* Any other, which are not out of scope.

**7.      Out of Scope**

**Assets**

* Any Company-ABC not specifically listed as in-scope.
* Company-ABC and Herts properties and their physical and networks infrastructure.
* Company-ABC and Herts corporate information systems.
* Third-party companies that perform business transactions for Company-ABC and/or Herts employees and contractors.    
    
  **Vulnerabilities**
* Vulnerabilities without discernible impact on Company-ABC IT systems or guest privacy.
* Attacks requiring physical access to a user’s device.
* Attacks requiring physical access to a Company-ABC employee, contractor or guest device.
* Autocomplete on web forms.
* Clickjacking, unless an effective exploit can be demonstrated.
* Client browser vulnerabilities.
* Denial of Service attacks on Company-ABC infrastructure.
* Limited content reflection or content spoofing.
* Missing best practices.
* Password and account recovery policies.
* Password policies, i.e., complexity.
* Phishing or spear phishing attacks.
* Rate-limiting issues.
* Reports originating from automated tools or scanners (e.g., Burp, Acunetix, WebInspect).
* Self-exploitation.
* Social engineering attacks.
* Software version disclosure.
* SSL / TLS best practices.
* Vulnerabilities that cannot be reproduced.
* Click jacking on pages with no sensitive actions.
* Unauthenticated/logout/login CSRF.
* Attacks requiring MITM or physical access to a user's device.
* Previously known vulnerable libraries without a working Proof of Concept.
* Comma Separated Values (CSV) injection without demonstrating a vulnerability.
* Missing best practices in SSL/TLS configuration.
* Any activity that could lead to the disruption of our service (DoS).
* Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS

1. **Safe Harbor**

Any activities conducted in a manner consistent with this policy will be considered authorized conduct and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Thank you for helping keep Company-ABC Hotels and our users safe!

## Appendix D:

**Rules of Engagement**

Company-ABC takes the security of our guests and colleagues very seriously. Company-ABC hopes to raise its already high level of security standards, as well as learn from and collaborate with highly skilled Pentesters at XYZ Security Ltd. in order to keep our businesses and customers safe.

By taking this Pentesting project of Company-ABC you agree to follow all of the requirements below.

**1.      SLA**

* Duration: W1 – W 15
* Produce a comprehensive Pen test report and Activity narrative.

**2.      Disclosure Policy**

Do not discuss this program or any vulnerabilities (even resolved ones) outside of the program without express consent from the undersigned.

**3.      Pentesting Rules**

* Do not collect any personally identifiable information, authentication information, or credit card information from Company-ABC guests.
* Do not destroy or alter discovered data.
* Do not inappropriately store Company-ABC information in public locations.
* Do not intentionally harm guests as well as their experience.
* Do not publicly or privately disclose any vulnerabilities belonging to Company-ABC - existing or remediated - to anyone other than the undersigned.
* Contact undersigned about questions regarding vulnerabilities or any issues.
* Current Company-ABC employees and contractors should not be participated in this pentest.
* You cannot participate in this pentest if you have been an employee or a contractor of Company-ABC in the past six months.
* Please provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, the issue will not be accepted.
* Social engineering (e.g., phishing, vishing, smishing) is prohibited.
* Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.
* Limit automation/rate scraping to 100 requests per minute.
* Remove all changes you have made during the pen test.

**4.      Submission Requirements**

* All reports must be submitted through the ABC platform.
* Consolidated Pentest report must meet Task 4 requirements.
* Attack Narrative reports must meet Task 5 requirements.

**5.      Testing Requirements**

**Test Accounts**

**Create** Company-ABC **test accounts to these specifications:**

* First name: < Company-ABC > (for multiple accounts - <handle>one, <handle>two, etc.).
* Last name: "**Test**".    
    
  Reservation Requirements    
    
  **If you must create bookings for testing purposes, follow these rules:**
* Test bookings should be made four months into the future at a minimum.
* All test bookings should be cancelled **as soon as possible**.
* Do not book London or Melbourne properties for testing purposes.

**6.      In Scope**

**Assets**

* Company-ABC.com (no subdomain).
* [www.Company-ABC.com](http://www.Company-ABC.com) (no additional subdomains).
* world.Company-ABC.com (no additional subdomains).
* assets.Company-ABC.com (no additional subdomains).    
    
  **Vulnerabilities**
* Authentication bypass.
* Back-end system access via front-end systems.
* Business logic bypass resulting in financial gain to an attacker (e.g., forced rate change).
* Container escape.
* Discovery of Company-ABC data on other storage services.
* Highly creative means of automating account checking or rate scraping (e.g., botting).
* Highly creative means of discovering origin IP.
* Highly creative means of spoofing email messages.
* Other systems that may host Company-ABC information.
* SQL Injection.
* Cross-Site Request Forgery.
* Exploitable Cross-Site Scripting.
* Web Application Firewall (WAF) bypass.
* Any other, which are not out of scope.

**7.      Out of Scope**

**Assets**

* Any Company-ABC not specifically listed as in-scope.
* Company-ABC and Herts properties and their physical and networks infrastructure.
* Company-ABC and Herts corporate information systems.
* Third-party companies that perform business transactions for Company-ABC and/or Herts employees and contractors.    
    
  **Vulnerabilities**
* Vulnerabilities without discernible impact on Company-ABC IT systems or guest privacy.
* Attacks requiring physical access to a user’s device.
* Attacks requiring physical access to a Company-ABC employee, contractor or guest device.
* Autocomplete on web forms.
* Clickjacking, unless an effective exploit can be demonstrated.
* Client browser vulnerabilities.
* Denial of Service attacks on Company-ABC infrastructure.
* Limited content reflection or content spoofing.
* Missing best practices.
* Password and account recovery policies.
* Password policies, i.e., complexity.
* Phishing or spear phishing attacks.
* Rate-limiting issues.
* Reports originating from automated tools or scanners (e.g., Burp, Acunetix, WebInspect).
* Self-exploitation.
* Social engineering attacks.
* Software version disclosure.
* SSL / TLS best practices.
* Vulnerabilities that cannot be reproduced.
* Clickjacking on pages with no sensitive actions.
* Unauthenticated/logout/login CSRF.
* Attacks requiring MITM or physical access to a user's device.
* Previously known vulnerable libraries without a working Proof of Concept.
* Comma Separated Values (CSV) injection without demonstrating a vulnerability.
* Missing best practices in SSL/TLS configuration.
* Any activity that could lead to the disruption of our service (DoS).
* Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS

**8.      SQL Injection Policy**

* Do not alter any data.
* Do not change or interrupt server or database functionality.
* Do not destroy any data.
* Do not read or save sensitive data belonging to guests other than yourself.
* Blindly counting rows and columns of databases is permissible.
* Generating outbound DNS requests is permissible.
* Listing database names and columns is permissible.
* Logic responses are permissible.

1. **Safe Harbor**

Any activities conducted in a manner consistent with this policy will be considered authorized conduct and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Thank you for helping keep Company-ABC Hotels and our users safe!