Software Requirements Specification

**Table of Contents**

1. Introduction 2

1.1 Purpose 2

1.2 Scope……………………………………………………………………........3

1.3 References 3

1.4 Overview 3 1.5Definitions,AcronymsandAbbreviations…………………………..........4

2. General Description 5

2.1 Product Functions 5

2.2 User CharacteristiCS……………………………………………………...5

2.3 General Constraints 5

3. Specific Requirements 6

3.1 Functional RequiremenT………………………………………………..6-9

3.2 Non-Functional Requirements

3.5.1 Performance 9

3.5.2 Reliability 10

3.5.3 Availability 10

3.5.4 Maintainability 10

# 

# 1. INTRODUCTION

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately. A vulnerability assessment process that is intended to identify threats and the risks they pose typically involves the use of automated testing tools, such as network security scanners, whose results are listed in a vulnerability assessment report.

A penetration test, also known as a pen test, is a simulated cyber-attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF). Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

**1.1 PURPOSE**

Vulnerability Assessment and Penetration Testing (VAPT) provides enterprises with a more comprehensive application evaluation than any single test alone. Using the Vulnerability Assessment and Penetration Testing (VAPT) approach gives an organization a more detailed view of the threats facing its applications, enabling the business to better protect its systems and data from malicious attacks. Vulnerabilities can be found in applications from third-party vendors and internally made software, but most of these flaws are easily fixed once found. Using a VAPT provider enables IT security teams to focus on mitigating critical vulnerabilities while the VAPT provider continues to discover and classify vulnerabilities.

## 1.2 SCOPE

With current payments ecosystem and infrastructure, wallets cannot be wholesome payments

instrument anytime soon. Instead of getting into consumer wallet business, it would be

worthwhile to create a smartphone friendly payment network which will address

interoperability issues for banks and merchants. That's a Meta problem to be solved. But after

Demonetization in November 2016 Paytm became India's largest mobile payment service

platform with over 150 million wallets and 75 million android based app downloads as of

November 2016. After 8 November 2016, PayTm's transactions and profit increased

significantly.

With current payments ecosystem and infrastructure, wallets cannot be wholesome payments

instrument anytime soon. Instead of getting into consumer wallet business, it would be

worthwhile to create a smartphone friendly payment network which will address

interoperability issues for banks and merchants. That's a Meta problem to be solved. But after

Demonetization in November 2016 Paytm became India's largest mobile payment service

platform with over 150 million wallets and 75 million android based app downloads as of

November 2016. After 8 November 2016, PayTm's transactions and profit increased

significantly.

With current payments ecosystem and infrastructure, wallets cannot be wholesome payments

instrument anytime soon. Instead of getting into consumer wallet business, it would be

worthwhile to create a smartphone friendly payment network which will address

interoperability issues for banks and merchants. That's a Meta problem to be solved. But after

Demonetization in November 2016 Paytm became India's largest mobile payment service

platform with over 150 million wallets and 75 million android based app downloads as of

November 2016. After 8 November 2016, PayTm's transactions and profit increased

significantly

The scopes of this project are:

* Protect from cyber attacks.
* Identify the possible vulnerability for a website.
* To ensure the security of website.

**1.3**  **REFRENCES**

References for the information gathered are hereby followed:

* The basic of hacking and Penetration testing by Patrick Engerbretson**.**
* Whois.
* Gray Hat Hacking: The Ethical Hacker’s Handbook Third Edition.
* Google Dorking.
* WebSite:https://one.comodo.com/blog/cyber-security/what-is-cyber-security.php.

## 1.4 OVERVIEW

# A penetration test, or pen-test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations or risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as, end-user adherence to security policies. In this we will do penetration testing on website and patch their vulnerability. To make website secure.

**1.5 Definitions, Acronyms and Abbreviations**

* **Vulnerability assessment**: A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.
* **Peneterartion testing**: A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a [web application firewall (WAF)](https://www.imperva.com/products/web-application-firewall-waf/).
* **BurpSuite (PT)L**: **Burp** or **Burp Suite** is a graphical tool for testing Web application security. The tool is written in Java and developed by PortSwigger Web Security. ... The company behind **Burp Suite** has also developed a mobile application containing similar tools compatible with iOS 8 and above.
* **Metasploit(PT):** **Metasploit** is an exploit development framework that facilitates penetration testing of IT systems. This tool initially started off as a game and was taken over by Rapid 7 for maintenance and further development.
* **Sublist3r** : **Sublist3r** is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting.
* **Nmap** : **Nmap** (Network Mapper) is a free and open-source network scanner created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich). **Nmap** is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Definitions, Acronyms and Abbreviations

• Customer :

Mean a person who has registered with Paytm for availing the Paytm Wallet and who

has accepted these Terms and Conditions and, owns/operates/has access to an internet

compatible device that supports the Paytm Wallet.

• Paytm Wallet :

Paytm Wallet means the pre-paid payment instrument issued by Paytm including

Basic Account and Prime Account.

• Person-to-Person Transfer :

Refers to a facility to transfer funds from a Paytm Wallet to any other Paytm Wallet

issued by Paytm or to any savings or current bank account.

• Merchant Establishment :

Shall mean and include physical Merchants, remote Merchants and any other outlet

that has been authorized by Paytm to accept payment using Paytm Wallet.

• Enrolment Form :

Shall mean the Paytm Wallet Enrolment Form, as is required by Paytm from the

Customer at the time of Registration for availing and / or continuation of the Paytm

Wallet.

• Basic Account :

Means Customer Paytm Wallet classified as Semi-closed system payment instruments

issued by accepting minimum customer details being Customer name, Email address,

mobile number, which permit payment and domestic money remittance as per RBI

direction on Issuance and Operation of Pre-paid Payment Instruments in India

(Reserve Bank) Directions, 2009 as amended and supplemented by the RBI from time

to time.

• Prime Account :

Means Customer Paytm Wallet which is KYC compliant and classified as Semi-

closed system payment instruments which permit Person-to-Person transfer and

payment to all identified Merchant as per RBI direction on Issuance and Operation of

Pre-paid Payment Instruments in India (Reserve Bank) Directions, 2009 as amended

and supplemented by the RBI from time to time.

• KYC :

Stands for Know your Customer and refers to the various norms, rules, laws and

statutes issued by RBI from time to time under which Paytm is required to procure

personal identification details from you before any services can be delivered. Know

your Customer (KYC) documents may be required by Paytm from the Customer at

the time of Registration and/ or on a later date, for availing and / or continuation of

the Paytm Wallet.

• Password :

Means the secret password used to secure Paytm Wallet applications, without

knowledge of which your Paytm Wallet will not be operable.

Definitions, Acronyms and Abbreviations

• Customer :

Mean a person who has registered with Paytm for availing the Paytm Wallet and who

has accepted these Terms and Conditions and, owns/operates/has access to an internet

compatible device that supports the Paytm Wallet.

• Paytm Wallet :

Paytm Wallet means the pre-paid payment instrument issued by Paytm including

Basic Account and Prime Acco

• Person-to-Person Transfer :

Refers to a facility to transfer funds from a Paytm Wallet to any other Paytm Wallet

issued by Paytm or to any savings or current bank account.

• Merchant Establishment :

Shall mean and include physical Merchants, remote Merchants and any other outlet

that has been authorized by Paytm to accept payment using Paytm Wallet.

• Enrolment Form :

Shall mean the Paytm Wallet Enrolment Form, as is required by Paytm from the

Customer at the time of Registration for availing and / or continuation of the Paytm

Wallet.

• Basic Account :

Means Customer Paytm Wallet classified as Semi-closed system payment instruments

issued by accepting minimum customer details being Customer name, Email address,

mobile number, which permit payment and domestic money remittance as per RBI

direction on Issuance and Operation of Pre-paid Payment Instruments in India

(Reserve Bank) Directions, 2009 as amended and supplemented by the RBI from time

to time.

• Prime Account :

Means Customer Paytm Wallet which is KYC compliant and classified as Semi-

closed system payment instruments which permit Person-to-Person transfer and

payment to all identified Merchant as per RBI direction on Issuance and Operation of

Pre-paid Payment Instruments in India (Reserve Bank) Directions, 2009 as amended

and supplemented by the RBI from time to time.

• KYC :

Stands for Know your Customer and refers to the various norms, rules, laws and

statutes issued by RBI from time to time under which Paytm is required to procure

personal identification details from you before any services can be delivered. Know

your Customer (KYC) documents may be required by Paytm from the Customer at

the time of Registration and/ or on a later date, for availing and / or continuation of

the Paytm Wallet.

• Password :

Means the secret password used to secure Paytm Wallet applications, without

knowledge of which your Paytm Wallet will not be operable.

Definitions, Acronyms and Abbreviations

• Customer :

Mean a person who has registered with Paytm for availing the Paytm Wallet and who

has accepted these Terms and Conditions and, owns/operates/has access to an internet

compatible device that supports the Paytm Wallet.

• Paytm Wallet :

Paytm Wallet means the pre-paid payment instrument issued by Paytm including

Basic Account and Prime Account.

• Person-to-Person Transfer :

Refers to a facility to transfer funds from a Paytm Wallet to any other Paytm Wallet

issued by Paytm or to any savings or current bank account.

• Merchant Establishment :

Shall mean and include physical Merchants, remote Merchants and any other outlet

that has been authorized by Paytm to accept payment using Paytm Wallet.

• Enrolment Form :

Shall mean the Paytm Wallet Enrolment Form, as is required by Paytm from the

Customer at the time of Registration for availing and / or continuation of the Paytm

Wallet.

• Basic Account :

Means Customer Paytm Wallet classified as Semi-closed system payment instruments

issued by accepting minimum customer details being Customer name, Email address,

mobile number, which permit payment and domestic money remittance as per RBI

direction on Issuance and Operation of Pre-paid Payment Instruments in India

(Reserve Bank) Directions, 2009 as amended and supplemented by the RBI from time

to time.

• Prime Account :

Means Customer Paytm Wallet which is KYC compliant and classified as Semi-

closed system payment instruments which permit Person-to-Person transfer and

payment to all identified Merchant as per RBI direction on Issuance and Operation of

Pre-paid Payment Instruments in India (Reserve Bank) Directions, 2009 as amended

and supplemented by the RBI from time to time.

• KYC :

Stands for Know your Customer and refers to the various norms, rules, laws and

statutes issued by RBI from time to time under which Paytm is required to procure

personal identification details from you before any services can be delivered. Know

your Customer (KYC) documents may be required by Paytm from the Customer at

the time of Registration and/ or on a later date, for availing and / or continuation of

the Paytm Wallet.

• Password :

Means the secret password used to secure Paytm Wallet applications, without

knowledge of which your Paytm Wallet will not be operable.

Definitions, Acronyms and Abbreviations

• Customer :

Mean a person who has registered with Paytm for availing the Paytm Wallet and who

has accepted these Terms and Conditions and, owns/operates/has access to an internet

compatible device that supports the Paytm Wallet.

• Paytm Wallet :

Paytm Wallet means the pre-paid payment instrument issued by Paytm including

Basic Account and Prime Account.

• Person-to-Person Transfer :

Refers to a facility to transfer funds from a Paytm Wallet to any other Paytm Wallet

issued by Paytm or to any savings or current bank account.

• Merchant Establishment :

Shall mean and include physical Merchants, remote Merchants and any other outlet

that has been authorized by Paytm to accept payment using Paytm Wallet.

• Enrolment Form :

Shall mean the Paytm Wallet Enrolment Form, as is required by Paytm from the

Customer at the time of Registration for availing and / or continuation of the Paytm

Wallet.

• Basic Account :

Means Customer Paytm Wallet classified as Semi-closed system payment instruments

issued by accepting minimum customer details being Customer name, Email address,

mobile number, which permit payment and domestic money remittance as per RBI

direction on Issuance and Operation of Pre-paid Payment Instruments in India

(Reserve Bank) Directions, 2009 as amended and supplemented by the RBI from time

to time.

• Prime Account :

Means Customer Paytm Wallet which is KYC compliant and classified as Semi-

closed system payment instruments which permit Person-to-Person transfer and

payment to all identified Merchant as per RBI direction on Issuance and Operation of

Pre-paid Payment Instruments in India (Reserve Bank) Directions, 2009 as amended

and supplemented by the RBI from time to time.

• KYC :

Stands for Know your Customer and refers to the various norms, rules, laws and

statutes issued by RBI from time to time under which Paytm is required to procure

personal identification details from you before any services can be delivered. Know

your Customer (KYC) documents may be required by Paytm from the Customer at

the time of Registration and/ or on a later date, for availing and / or continuation of

the Paytm Wallet.

• Password :

Means the secret password used to secure Paytm Wallet applications, without

knowledge of which your Paytm Wallet will not be opera

# 2. GENERAL DESCRIPTION

## Web application penetration testing is the process of using penetration testing techniques on a web application to detect its vulnerabilities. It is similar to a penetration test and aims to break into the web application using any penetration attacks or threats like SQL injection, HTTPs certification, Payment gateway bypass, XSS attacks, DOS attack,etc. To over the threds and make it make it more secure from this threads.

## 2.1 PRODUCT FUNCTION

Product Function of Penetration Testing is that in which we need to identify the threads and with the help of that threads we can overcome or patch the website.

## 2.2 USER CHARCTERSTICS

There are several users of Payzapp Network

* **Customers**

Penetration Testing make websites secure for the customer so that they can rely on the website for their personal information, data, transaction, shopping accounts etc.

* **Website owner**

In this the website owner is free to make any type of customer because he of high security feature and without worrying about the trust issues of the users .

**3. SPECIFIC REQURIMENTS**

## 3.1 FUNCTIONAL REQURIMENTS

1. Scoping

2. Information gathering

3. Vulnerability scanning

4. False positive analysis

5. Vulnerability exploitation (Penetration Testing)

6. Report generation

The following figure illustrates the different sequential stages recommended to follow for a Vulnerability Assessment or Penetration Testing:

**Stage 1 – Scoping**

Scoping is the primary step of any security assessment activity. In order to execute a VA or PenTest, the first step is to identify the scope of the assessment in terms of infrastructure against which the assessment is to be conducted, for example, servers, network devices, security devices, databases, and applications. Scoping depends on the business objective of the Vulnerability Assessment. During the scoping, a scanning window should also be agreed upon. Also, the types of attacks that are permitted should be agreed upon. After deciding on the scope of assessment, this phase also includes planning and preparation for the test, which includes deciding on the team, date, and time of the test. Another major factor that should be taken care of prior to beginning the engagement is signing a formal engagement agreement between the security tester and the party on whose infrastructure these tests will be performed. Scoping should also include identifying the count of infrastructure elements to be tested. Apart from the infrastructure scope and other program management modalities, the exact scope, the organization’s approach to the business objective, and the methodology of the assessment should be decided. For deciding on the business objective, the organization should identify the type of attack that it would like to get mimicked. An example of an objective that a company might seek is: “To find out what an external attacker can achieve by targeting externally exposed infrastructure with only the knowledge of a publicly exposed IP address.” This type of requirement will be met through an external Black box penetration testing of infrastructure and applications, and the approach and the methodology should be in accordance with that. Based on the accessibility of infrastructure from the Internet or intranet, the testing can be done from an external or internal network. Also, based on the type of details, the infrastructure testing can be Black box or Grey box. And depending on the type of infrastructure, the plugins or features of a vulnerability scanning tool should be enabled, aided by appropriate manual checks.

**Stage 2 – Information gathering**

Information gathering is the second and most important stage of a VA-PT assessment. This stage includes finding out information about the target system using both technical (WhoIS) and nontechnical passive methods such as the search engine. This step is critical as it helps in getting a better picture of the target infrastructure and its resources. As the timeline of the assessment is generally time bound, information captured during this phase helps in streamlining the effort of testing in the right direction by using the right tools and approach applicable to target systems. This step becomes more important for a Black box assessment where very limited information about the target system is shared. Information gathering is followed by a more technical approach to map the target network using utilities such as pings and Telnet and using port scanners such as NMAP. The use of such tools would enable assessors to find a live host, open services, operating systems, and other information. The information gathered through network mapping will further validate information gathered through other passive means about the target infrastructure, which is important to configure the vulnerability scanning tool. This ensures that scanning is done more appropriately.

**Stage 3 – Vulnerability scanning**

This stage involves the actual scanning of the target infrastructure to identify existing vulnerabilities of the system. This is done using vulnerability scanners such as Nessus. Prior to scanning, the tool should be configured optimally as per the target infrastructure information captured during the initial phases. Care should also be taken that the tool is able to reach the target infrastructure by allowing access through relevant intermediate systems such as firewalls. Such scanners perform protocol TCP, UDP, and ICMP scans to find open ports and services running on the target machine and match them to wellknown published vulnerabilities updated regularly in the tool’s signature database if they exist in the target infrastructure. The output of this phase gives an overall view of what kind of vulnerabilities exist in the target infrastructure that if exploited can lead to system compromise.

**Stage 4 – False positive analysis**

As an output of the scanning phase, one would obtain a list of vulnerabilities of the target infrastructure. One of the key activities to be performed with the output would be false positive analysis, that is, removing any vulnerability that is falsely reported by the tool and does not exist in reality. All scanning tools are prone to report false positives, and this analysis can be done using methods such as correlating vulnerabilities with each other and previously gathered information and scan reports, along with actually checking whether system access is available. Vulnerability scanners give their own risk rating to the identified vulnerabilities; these can be revisited considering the actual criticality of the infrastructure element (server or network device) to the network and impact of the vulnerability.

**Stage 5 – Vulnerability exploitation (Penetration Testing)**

In case system owners require proof of existing vulnerabilities or exploits to understand the extent to which an attacker can compromise a vulnerable system, testers will be required to demonstrate exploits in a controlled environment without actually making the infrastructure unavailable, unless that’s a requirement. Penetration Testing is the next step to Vulnerability Assessment aiming to penetrate the target system based on exploits available for the identified vulnerabilities. For exploitation, our own knowledge or publicly available exploits of well-known vulnerabilities can be utilized. Penetration Testing or Vulnerability Exploitation can be broadly divided into phases such as pre exploitation, exploitation, and post exploitation. Activities in the pre-exploitation phase are explained in phases 1 to 4, that is, enumerating the infrastructure and identifying the vulnerability. Once any vulnerability is exploited to gain access to the system, the attacker should aim to further detail the network by sniffing traffic, mapping the internal network, and trying to obtain a higher privilege account to gain the maximum level of access to the system. This will enable testers to launch further attacks on the network to further increase the scope of compromised systems. The post exploitation step will also involve clearing of tracks by conducting activities such as clearing logs and disabling antivirus. As a post-exploitation phase tester, you can demonstrate how an attacker can maintain access to the system through backdoors and rootkits.

**Stage 6 – Report generation**

After completing the assessment as per the scope of work, final reporting needs to be done covering the following key areas:

• A brief introduction about the assessment

• The scope of assessment

• The management/executive summary • A synopsis of findings with risk severity • Details about each finding with their impact and your recommendations to fix the vulnerability.

## 3.2 NON-FUNCTIONAL REQURIMENTS

### 3.2.1 PERFOMANCE

The application is fast, secure and trustworthy.

### 3.2.2 RELIABILITY

In this Transaction will become more secure. DDOS attack will not work after certification.

### 3.2.3 AVAILABILITY

It is available for all the user’s.

### 3.2.4 MAINTAINABILITY

### As per the updation of new technologies we need to update the security so that none of the hacking can be performed.