

Software Design Document

E-Banking System Portal

OOSE Exp 9

November 2019

For a Web/Native Mobile Application Based Application System

1 Introduction

1.1 System Overview

The Application focuses on providing less cumbersome experience to the end user by providing a smooth and secure environment for efficient and reliable Online Banking System .

1.2 Test Approach

The Application mainly focuses on Security principles so an exemplar for the security model to used for unit as well as domain testing . The testing groups include Face Recognition ,Network Buffer capacity, Database Sql Injection , Shodan Web Application Penetration , Synchronize Flooding Attack on Server, Vulnerability Scan , Session Management. The Security testing for the Network Buffer Capacity Database Sql Injection and Shodan Web Application Penetration and Vulnerability Scan is done for secure transactions and also used to prevent multiple annonymus network login on the Same IP address. Secure Database access for the admin and monitoring the overall services of the application.

2. Test Plan

Test Plan includes the Security , Maintainability and reliable portal . The Approach include vigorous network analysis and testing on the performance in every damn aspect of functionalities which deals with Security and testing containerization done by the deployment Engineer. The Resources include Kali Linux, Metasploit ,BurpSuit , Beef xss , Armitage , Netcat ,OpenCv . Features for Testing include Transactions, Login, Register , Session Storage and Session Management User Face Recognition and Database access Security. The personal task includes Developer ,Admin, Penetration Tester, Devops Engineer .The payment gateway will accept only valid credit and debit cards.Testing will be done whether Credit/debit card number,Date of expiry and CVV details are fetched by the application correctly by the application. These can be done by manual testing. The network Security Scan is focused on maintaining the safe and secure gateway.

2.1 Features to be tested :

The Features includes Login , Register ,Payment Schedule and Payment History, Payment Transaction and Facial Recognition ,Database Security.

Face Recognition: Input Image Dataset , Input Data Consistency

Payment Schedule ,Payment History , Payment Transaction :

Database Security : Database Sql Injection :

OverAll Application Security : Network Buffer capacity, Database Sql Injection , Shodan Web Application Penetration , Synchronize Flooding Attack on Server, Vulnerability

Scan , Session Management

The security testing will be performed by arachnid tool in 1 week, Cross browser testing using Cross Browser Tool in 1 week, Performance testing using Jmeter tool in week, Usability testing using chrome runner tool in 1 week. The database testing will be performed whether all the data are stored and fetched properly from database. The non functional attributes will be testing in approximately in 1 month

Test Plan

Version	Estimated completion of testing
1.01 alpha	10/10/2019
1.02	20/10/2019
1.03	25/10/2019

Roles And Responsibilities

Sr.no	Deliverable Name	Author	Reviewer
1	Test Plan	Test Lead(RIDDHISHA)	Project Manager/ Business Analyst's/Test Lead
2	Network Buffer Overflow Defects	Penetration Tester(Vedang)	Project Manager/ Penetration Tester/Test Lead
3	Login/Database defects	Test Team(Niket)	Project Manager/ Business Analyst's/Test Lead
4	DOS preventions/WAF/IPS issues	Test Team(Vedang)	Penetration Tester/Test Lead/ Project Manager
5	Datasets consistency Defects	Test Team(Hritik)	Test Lead/ Project Manager
6	Test closure report	Test Lead(RIDDHISHA)	Project Manager

--	--	--	--

Version	Functionality to be Tested
1.01 alpha	login and registration, image datasets, network latency and waterfall requirement
1.02	Website Application Firewall, Intrusion Prevention System for secure transactions
1.03	Buffer Capacity, SSL certificate validation, Database security performing sql injection secure database access and storage

2.2 Features not to be tested :
 Enrollment Terms, Bank Offers , Transaction trends

2.3 Testing Tools and Environment:
 Number of testers needed->3
 Time needed->1 month approximately
 Hardware:8GB ram and intel processor
 Software:Windows OS, Debian Linux Version, Secure network Access Environment ,
 Virtual Machines.
 Tools needed:

Junit->Unit Testing ,Node Debugger
Citrus Tool->Integration Testing
Selenium->Automation Testing
Performance Testing->Jmeter Tool
Security Testing->Metasploit ,BurpSuit , Beef xss , Armitage , Netcat ,Nmap
Compatibility Testing->Cross Browser Tool
Usability Testing->LightHouse Tool
Database Testing->BurpSuit , Armitage

3 TEST CASES

Functionalities for a bank User

3.1 Register Functionality

3.1.1 Purpose:

To check user is able to login with username and password where username should not
,fname ,lname

accept special characters and password must be of minimum 6 characters and cannot
contain user name

The Confirm Password and Password must match

To validate Mobile Number

The captcha to be verified.

To Provide aadhar validation with aadhar id using aadhar government api

To Provide Image Recognition based on the image from the aadhar database

The User can register as only user and required security team and project lead would
have constant surveillance on the Application

3.1.2 Inputs:

Go to site:www.ebanksyns.com

Click on Register

Enter username as abc@123

Password as 123

Confirm Password as 123

Next-Button

3.1.1 Expected Outputs & Pass/Fail criteria

The result should fail on above input as the password contains special characters

Input.

Aadhar validation page <https://ebanksyns/register>

Enter aadhar id : xyz@123

3.1.2 Expected Outputs & Aadhar/Fail criteria

The result should fail on above input as the aadhar id is not recognized as a valid one.

Input.

Face Recognition Window

3.1.3 Expected Outputs & Image/Fail criteria

The result should not work Please provide a valid Face to be recognized if you are a Human.

Input.

<https://ebanksyns/register>

Enter username as abc@123

Mobile No:222222

Password as 123

3.1.4 Expected Outputs & Mobile/Fail criteria

The result should not work Please Provide a valid mobile number

3.2 Login Functionality

3.2.1 Purpose:

To Provide The Email and Password

To generate random OTP send for both email and registered valid for only 10 seconds

To provide a captcha in order to verify as a Human

Input:

<https://ebanksyns/register>

Email::abc@123

Password:11111111

OTP ::

3.2.1 Expected Outputs & Password/Fail criteria:

The email is not registered or the password is incorrect

Input:

https://ebanksyns/register

Email::abc@123

Password:11111111

OTP ::

3.2.2 Expected Outputs & OTP/Fail criteria:

The OTP is not correct or the requirect OTP is expired.

3.2.3 Expected Outputs & DDOS/Multiple/Fail criteria:

By The Bank Security Right your IP is banned for vigorous network attempts legal action may be encountered.

3.3 Transaction Functionality :

Purpose: Once the User is authenticated by passing login and register functionalities he/she can perform transactions view transaction functionalities

Input ::

<https://ebanksyns/username?12eeeaxaxaxax>

Go to Transfer Amount.

Enter the Bank Name

Enter the Bank IFSC code

Enter the Bank Branch

Validate The Captcha

3.3.1 Expected Outputs & UserInput/Fail criteria:

The Bank Name is not valid or you have entered an invalid IFSC code

3.3.2 Expected Outputs & Captcha/Fail criteria:

The captcha entered is not a valid one.

3.3.3 Expected Outputs & Session/Fail criteria:

Your Session is Expired Please Login Again

3.4 Transaction History :

Purpose: Once the User is authenticated by passing login and register functionalities he/she can perform transactions view transaction History in most best User Interactive Format.

Input:

The transaction History Log

3.4.1 Expected Outputs & Session/Fail criteria:

Your Session is Expired Please Login Again

Functionalities for Penetration Tester

3.5 : Overall Network Security Scan:

Purpose: To perform and Secure OverAll Application Security : Network Buffer capacity, Database Sql Injection , Shodan Web Application Penetration , Synchronize Flooding Attack on Server, Vulnerability Scan , Session Management

3.5.1 Expected Outputs & Offline/Fail criteria:

Required Application is brought in production phase from development

3.5.2 Expected Outputs & Domain/Fail criteria:

The Domain or the required web server is down or having a heavy traffic on server

Functionalities for Admin User:

3.6 :: Integrity in application and maintainibilty

Purpose: Input Image Dataset , Input Data Consistency,Manage All Application Functionalities

3.6.1 Expected Outputs & Domain/Fail criteria:

The Domain or the required web server is down or having a heavy traffic on server

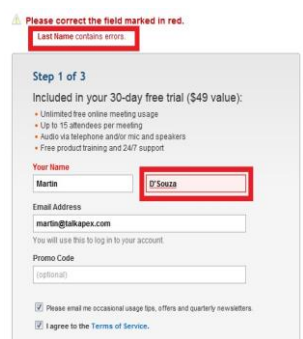
Functionalities for Devops User:

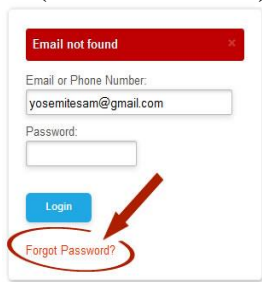
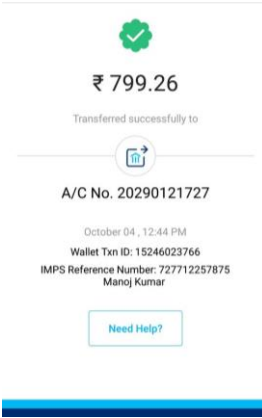
Purpose: Use of Docker Nginx in order to provide efficient deployment procedure

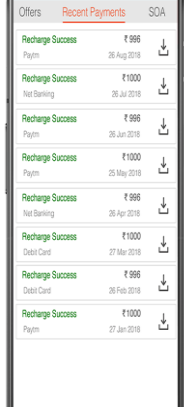
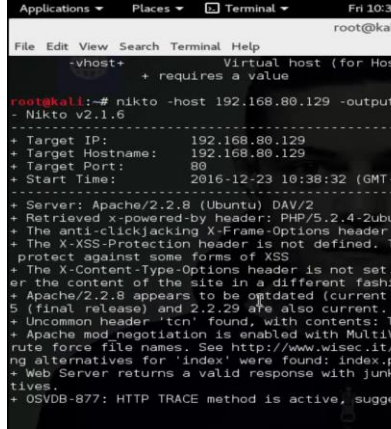
3.5.4 Expected Outputs & Phase/Fail criteria:

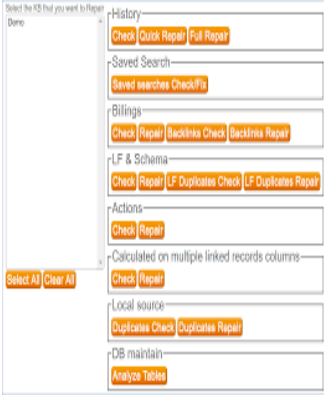
The Required Application is not ready for Deployment or in Production Phase

Test Logs for the Application


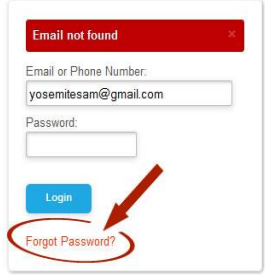
Test case id	Test case Name	Description	Input	Expected output	Actual output	Status
3.1	Register functionality	Go to site,do registration for bank portal	Go to site,do registration provide username email fname,lname password confirm password .Aadhaar or pan card image and face recognition	Welcome user to our bank Portal	Special characters also accepted	Failed(10/10/2019) At testing environment(Windows os (Chrome browser)) 

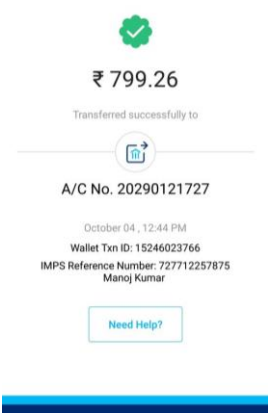
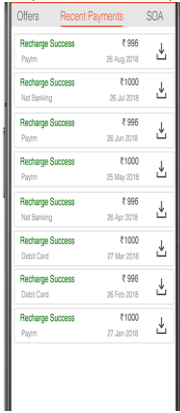
3.2	Login functionality	Provide Email and Password generate OTP for 10 seconds valid verify a user as human	Enter user name and password	User name should accept all aphanumeric but no special characters	Username or email is not registered with us	<p>Failed(10/10/2019) At testing environment(Windows os (Chrome browser))</p> 
3.3	Transaction Functionality :	Once the User is authenticated by passing login and register functionalities he/she can perform transactions view transaction functionality	<p>Enter the Bank Name</p> <p>Enter the Bank IFSC code</p> <p>Enter the Bank Branch</p> <p>Validate The Captcha</p>	Bank Should Accept all the valid IFSC codes and valid captcha and valid session	The Bank Name is a valid and the amount is transferred	<p>Passed(10/10/2019)</p> 

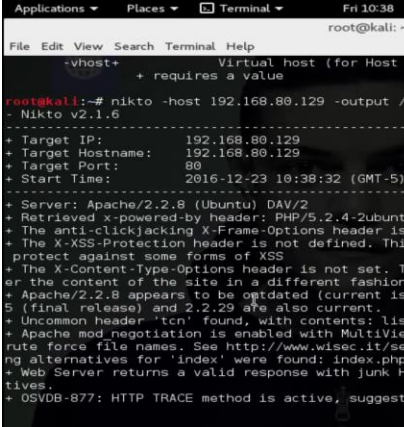

3.4	3.4 Transaction History :	Once the User is authenticated by passing login and register functionalities he/she can perform transactions view transaction History in most best User Interactive Format.	The transaction History Log	view transaction History in most best User Interactive Format.	Transaction log displayed in proper form	Passed(10/10/2019) 
3.5	Overall Network Security Scan:	Security : Network Buffer capacity, Database Sql Injection , Shodan Web Application Penetration , Synchronize Flooding Attack on Server, Vulnerability Scan , Session	None	Domain and application has a valid security ssl certificate and domain	Penetration testing results obtained positive	Passed(25/10/2019) 

		Manageme nt				
3.6	Integrity in applicati on and maintaini bilty	Input Image Dataset , Input Data Consistenc y,Manage All Application Functionali ties	None	The Domain or the required web server is down or having a heavy traffic on server	The Dom ain is Vali d data anal ytics is succ ess	Passed(25/10/2019)  <p>The screenshot shows a sidebar menu on the left with categories like 'Select the DB that you want to repair', 'History', 'Saved Search', 'Billing', 'LF & Schema', 'Actions', 'Calculated on multiple linked records columns', 'Local source', and 'DB maintain'. Each category has a list of buttons with orange text, such as 'Check', 'Quick Repair', 'Full Repair', 'Check Repair', 'Backlinks Check', 'Backlinks Repair', 'LF Duplicates Check', 'LF Duplicates Repair', 'Check Repair', 'Select All', 'Clear All', 'Duplicates Check', 'Duplicates Repair', and 'Analyze Tables'.</p>


Test Logs for the Application

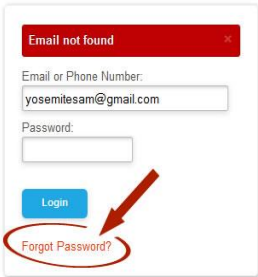
Test cas id	Test case Name	Description	Input	Expected output	Actual output	Status
3.1	Register functionality	Go to site,do registration for bank portal	Go to site,do registration provide username email fname,lname password confirm password .Aadhaar or pan card image and face recognition	Welcome user to our bank Portal	Special characters also accepted	Failed(10/10/2019) At testing environment(Windows os (Chrome browser)) 
3.2	Login functionality	Provide Email and Password generate OTP for 10 seconds valid verify a user as human	Enter user name and password	User name should accept all aphanumeric but no special characters	Username or email is not registered with us	Failed(10/10/2019) At testing environment(Windows os (Chrome browser)) 

3.3	Transaction Functionality :	Once the User is authenticated by passing login and register functionalities he/she can perform transactions view transaction functionality	Enter the Bank Name Enter the Bank IFSC code Enter the Bank Branch Validate The Captcha	Bank Should Accept all the valid IFSC codes and valid captcha and valid session	The Bank Name is a valid and the amount is transfer red	Passed(10/10/2019) 
3.4	3.4 Transaction History :	Once the User is authenticated by passing login and register functionalities he/she can perform transactions view transaction History in most best User Interactive Format.	The transactio n History Log	view transaction History in most best User Interactive Format.	Transac tion log displaye d in proper form	Passed(10/10/2019) 

3.5	Overall Network Security Scan:	Security : Network Buffer capacity, Database Sql Injection , Shodan Web Application Penetration , Synchronize Flooding Attack on Server, Vulnerability Scan , Session Management	None	Domain and application has a valid security ssl certificate and domain	Pen etra tion test ing res ults obt ain ed posi tive	Passed(25/10/2019) 
3.6	Integrity in applicatio n and maintaini bilty	Input Image Dataset , Input Data Consistency, Manage All Application Functionalitie s	None	The Domai n or the require d web server is down or having a heavy traffic on server	The Do mai n is Vali d data anal ytic s is suc cess	Passed(25/10/2019) 

Defect Reporting:

Test cas id	Test case Name	Description	Input	Expected output	Actual output	Status
3.1	Register functionality	Go to site,do registration for bank portal	Go to site,do registration provide username fname,lname password confirm password .Aadhaar or pan card image and face recognition	Welcome user to our bank Portal	Special characters also accepted	<p>Failed(10/10/2019) At testing environment(Windows os (Chrome browser))</p> 

3.2	Login functionality	Provide Email and Password generate OTP for 10 seconds valid verify a user as human	Enter user name and password	User name should accept all aphanumerics but no special characters	Username or email is not registered with us	Failed(10/10/2019) At testing environment(Windows os (Chrome browser) 
-----	---------------------	---	------------------------------	--	---	---