



**Project title-**  
**“Secure Login & Threat Prevention In Bank  
Management System”**

Project for  
INFORMATION SECURITY MANAGEMENT  
(BCSE354E)

**Submitted by**

Swetha S(21BIT0678),  
Shivani K(21BIT0681),  
Kaliraj A(21BIT0687),  
Jumana Begum M(21BIT0694),  
Shabavudeen M(21BIT0699),  
Nishyanth Nandagopal(21BIT0160)

**Submitted to**

PROF MOHANA PRIYA P

## **Abstract**

This project aims to enhance the security of a bank management website by implementing strong password policies, encrypted passwords, and additional authentication measures. These measures help mitigate the risks of brute force attacks, SQL injection, cross-site scripting (XSS), and unauthorized access. The project focuses on improving the security and integrity of sensitive financial data, ensuring a safer online banking experience for users.

## **Scope**

The scope of the project includes implementing strong password policies to prevent brute-force attacks, encrypting passwords using AES-128 for security, preventing SQL injection attacks to avoid unauthorized access to the website, using email-based one-time passwords for secure authentication when users try to modify data, and implementing measures to prevent cross-site scripting (XSS) attacks. These measures are aimed at enhancing the security of the website and protecting sensitive user data from various common security threats.

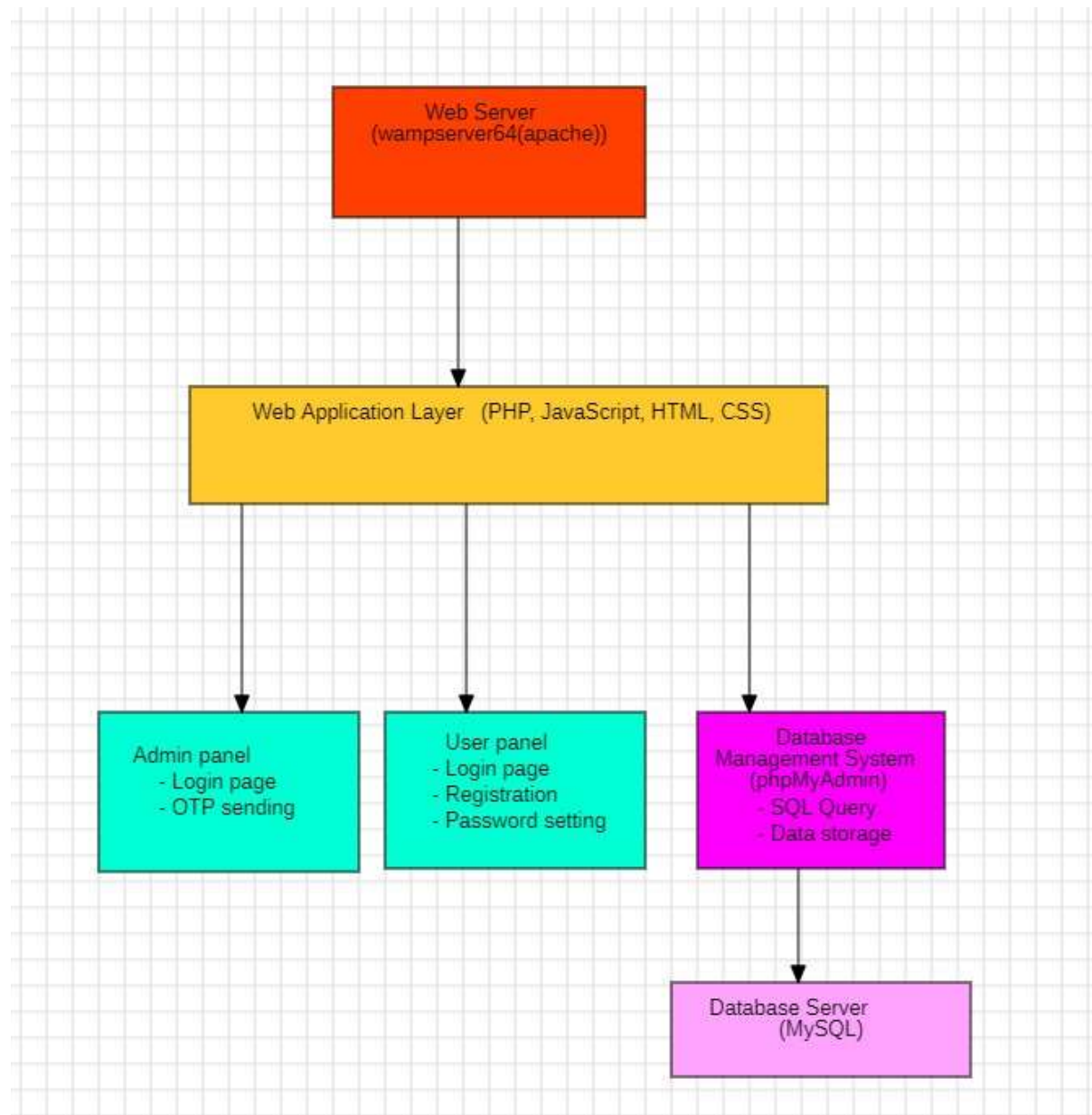
## **Introduction**

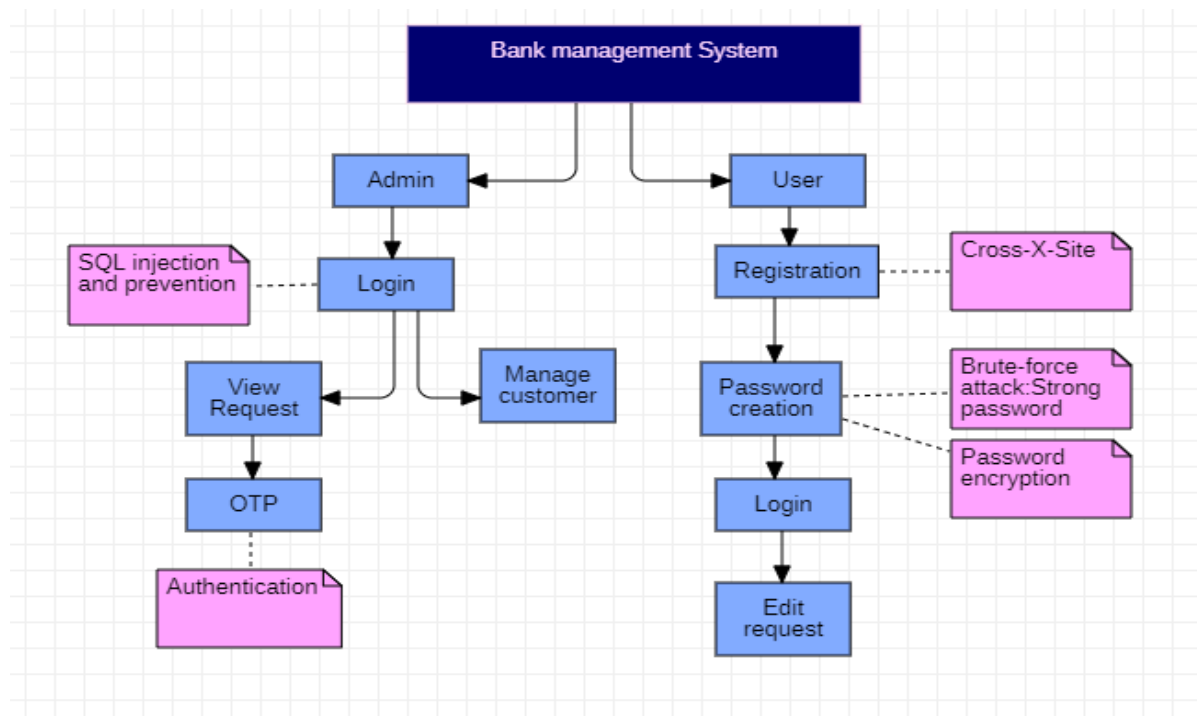
The security of online banking systems is crucial to protect users' financial information from malicious attacks. This project addresses this need by implementing various security measures in a bank management website. By enforcing strong password policies, encrypting passwords using AES-128, and adding additional authentication steps such as email-based one-time passwords (OTP) for modifying user details, the website's security is significantly enhanced. These measures help prevent common security threats like brute force attacks, SQL injection, XSS, and unauthorized access, making the website more secure for users.

## **Architecture**

The architecture of the bank management website is designed to ensure the security and integrity of the system. It consists of several key components, including the user interface, the application logic, the database, and the security features. The user interface allows users to interact with the website, while the application logic handles user requests and processes data. The database stores user information securely, and the security features, such as strong password

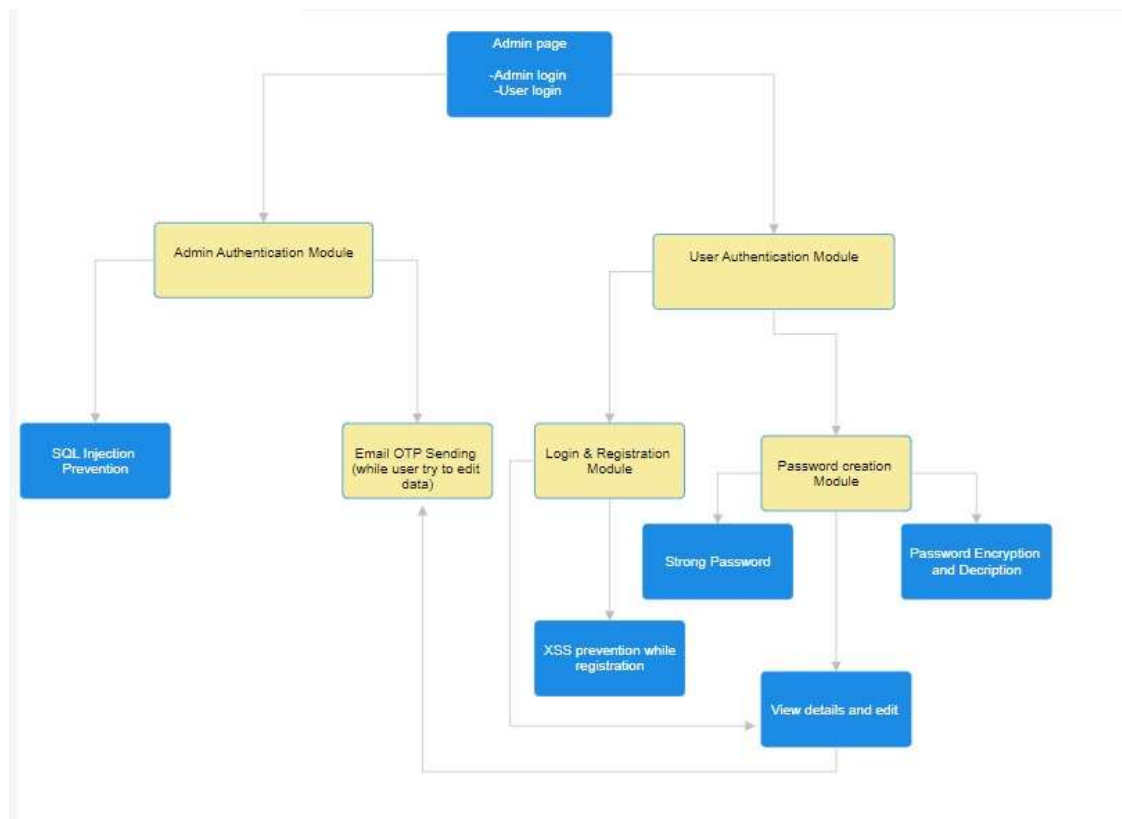
policies and encryption, protect this data from unauthorized access. The architecture is designed to be robust and scalable, ensuring the website can handle a large number of users securely.





## Modules

The bank management website is divided into several modules, each responsible for a specific functionality. The modules include the user authentication module, which handles user login and registration, the password management module, which enforces strong password policies and encrypts passwords, the data modification module, which adds additional authentication measures for modifying user details, and the security module, which protects the website from common security threats. Each module works together to ensure the security and integrity of the website's data and functionality.



## Experimental setup

- Database management system (DBMS) software -WAMPSEVER ( phpmyadmin)
- Programming language - PHP,JAVASCRIPT,HTML,CSS.
- Database Management – MySQL
- Integrated Development Environment (IDE) for coding and testing - Visual Studio Code

**Home page** : It contains admin and user login link

**Admin login page** :While login we added SQL injection prevention technique. This page also responsible for sending OTP to user's email when user request to edit their data. Session hijacking is prevented.

**User login page** : While login we added sql injection prevention technique . This page also contains registration option if not registered. After registration password setting will be done during this we added strong password requirements . .Additional to this , we added authentication like permission request from admin. In this User login page we included the Cross Site Scripting prevention technique to prevent the attack which is affect the website.

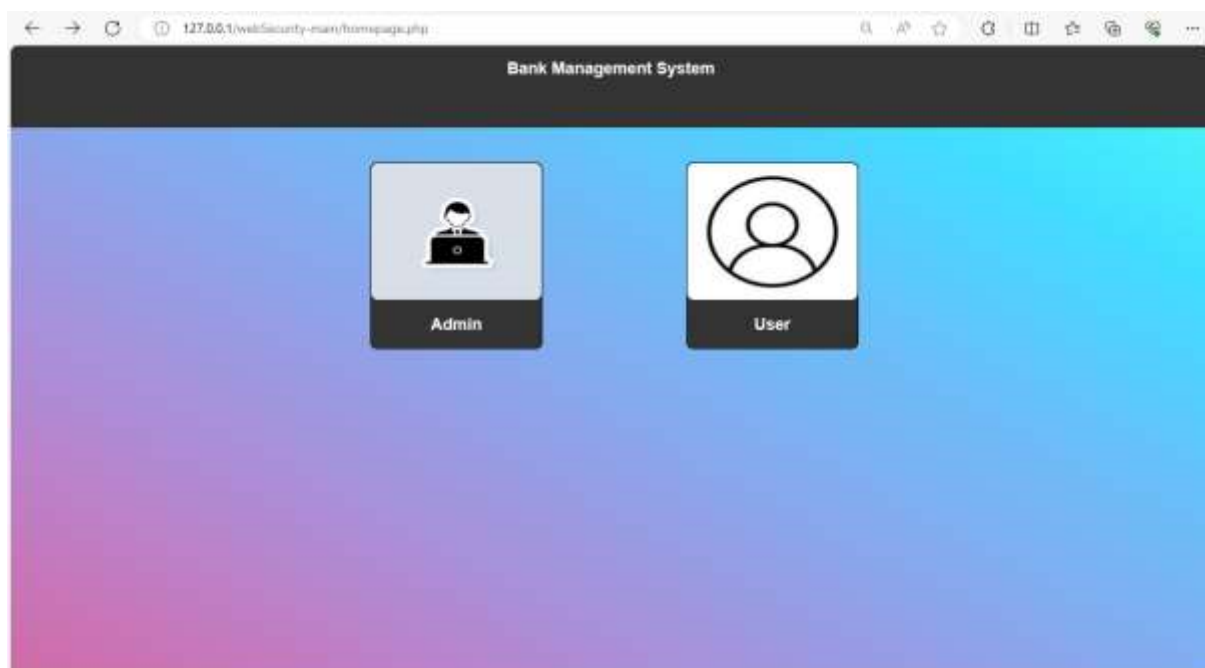
And also in user login system, we included the technique which encrypt passwords before storing them in the database to enhance security. This page also contains the prevention technique from the session hijacking attack is a type of attack where an attacker takes the user's active session to gain unauthorized access to a web Application.

## Novelty

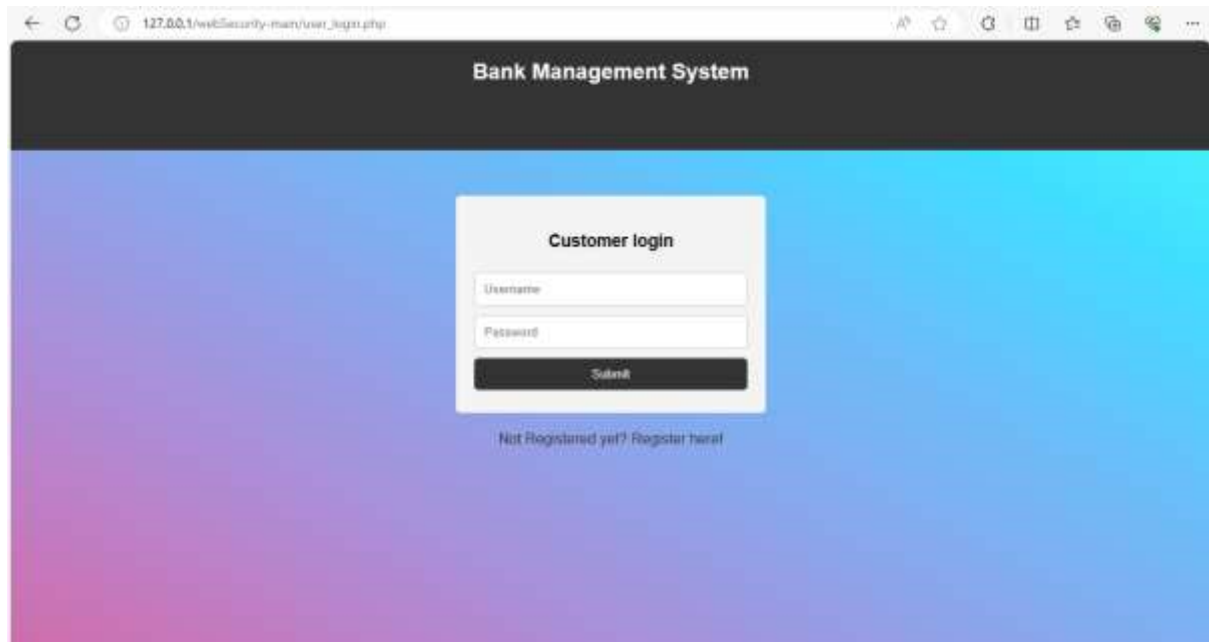
The novelty of this project lies in its comprehensive approach to security. By combining strong password policies, encrypted passwords, additional authentication measures, and protection against common security threats, the project provides a robust and secure solution for online banking. The project's focus on enhancing the security and integrity of sensitive financial data sets it apart from other similar projects, making it a valuable contribution to the field of cybersecurity.

## Implementation

### HOME PAGE:



## CUSTOMER PAGE:



A screenshot of a web browser displaying the 'Bank Management System' customer login page. The browser's address bar shows '127.0.0.1/webSecurity-man/user\_login.php'. The page has a dark header with the title 'Bank Management System'. The main content area has a blue-to-purple gradient background. In the center, there is a white box titled 'Customer login' containing two input fields for 'Username' and 'Password', and a black 'Submit' button. Below the box, a link says 'Not Registered yet? Register here!'

Bank Management System

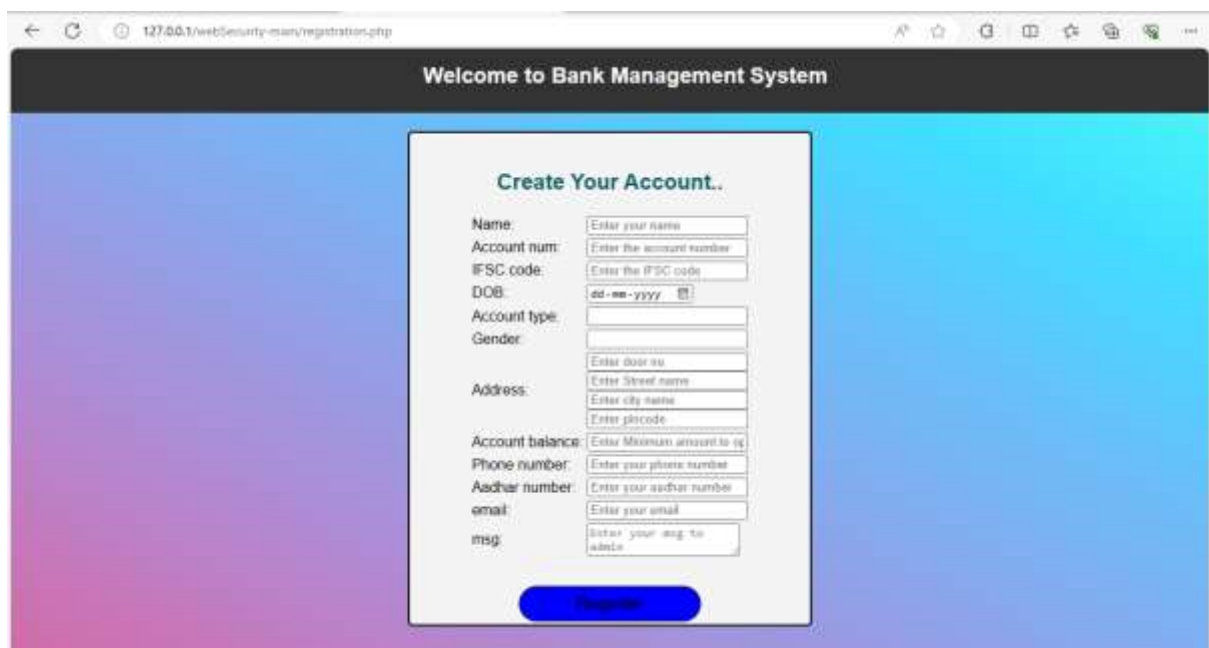
Customer login

Username

Password

Submit

Not Registered yet? Register here!



A screenshot of a web browser displaying the 'Bank Management System' registration page. The browser's address bar shows '127.0.0.1/webSecurity-man/registration.php'. The page has a dark header with the title 'Welcome to Bank Management System'. The main content area has a blue-to-purple gradient background. In the center, there is a white box titled 'Create Your Account..'. It contains a list of registration fields: Name, Account num, IFSC code, DOB (with a date picker), Account type, Gender, Address (with sub-fields for door no, Street name, city name, and pincode), Account balance, Phone number, Aadhar number, email, and msg. A blue 'Register' button is at the bottom of the form.

Welcome to Bank Management System

Create Your Account..

Name: Enter your name

Account num: Enter the account number

IFSC code: Enter the IFSC code

DOB: dd-mm-yyyy

Account type:

Gender:

Enter door no

Address: Enter Street name

Enter city name

Enter pincode

Account balance: Enter Maximum amount to eq

Phone number: Enter your phone number

Aadhar number: Enter your aadhar number

email: Enter your email

msg: Enter your msg to admin

Register

127.0.0.1/webSecurity-main/password\_creation.php

## Bank Management System

### Create Your Password

Username

Password

☐ Show Password

**Note:**

- > Make sure that your new password should contain atleast 1 uppercase, 1 lowercase, 1 number and 1 special character.
- > Make sure that your password should be more than 8 characters.
- > Make sure that your new password and confirm password should be same.
- > Make sure that your new password should not be your old password.
- > The confirmation message will be sent to your respective email id.

127.0.0.1/webSecurity-main/editreq.php

## Bank Management System

### Update Profile

Field name

Account Number

Existing value

New value



## ADMIN PAGE:

The image displays two screenshots of a web application interface for a Bank Management System.

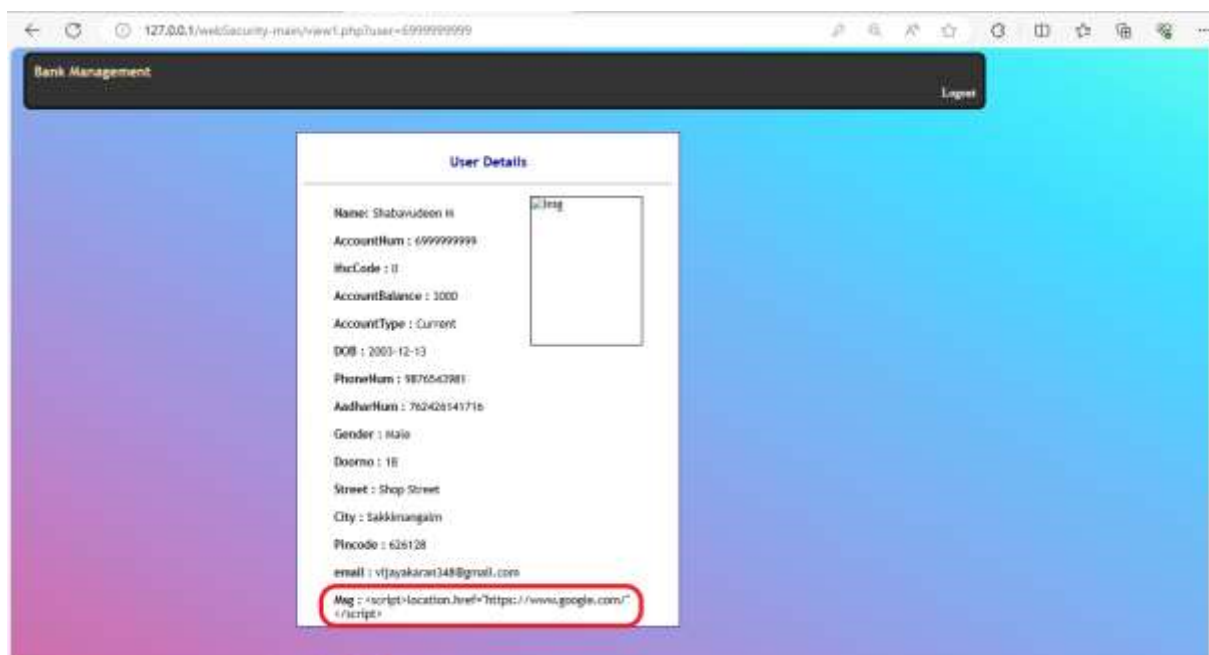
The top screenshot shows the "Admin login" page. The browser address bar indicates the URL is `127.0.0.1/webSecurity-man/s_login.php`. The page has a dark header with the title "Bank Management System". The main content area has a blue-to-purple gradient background. In the center, there is a white box titled "Admin login" containing two input fields: "Username" and "Password", followed by a "Submit" button. Below the login box, a link says "Not Registered yet? Register here!".

The bottom screenshot shows the "Admin" dashboard. The browser address bar indicates the URL is `127.0.0.1/webSecurity-man/admin_home.php`. The page has a dark header with the title "Admin". The main content area has the same blue-to-purple gradient background. It features two large, square buttons with white icons and black text labels: "Customer Request" (with a speech bubble and arrow icon) and "Manage Customer" (with a user profile icon).

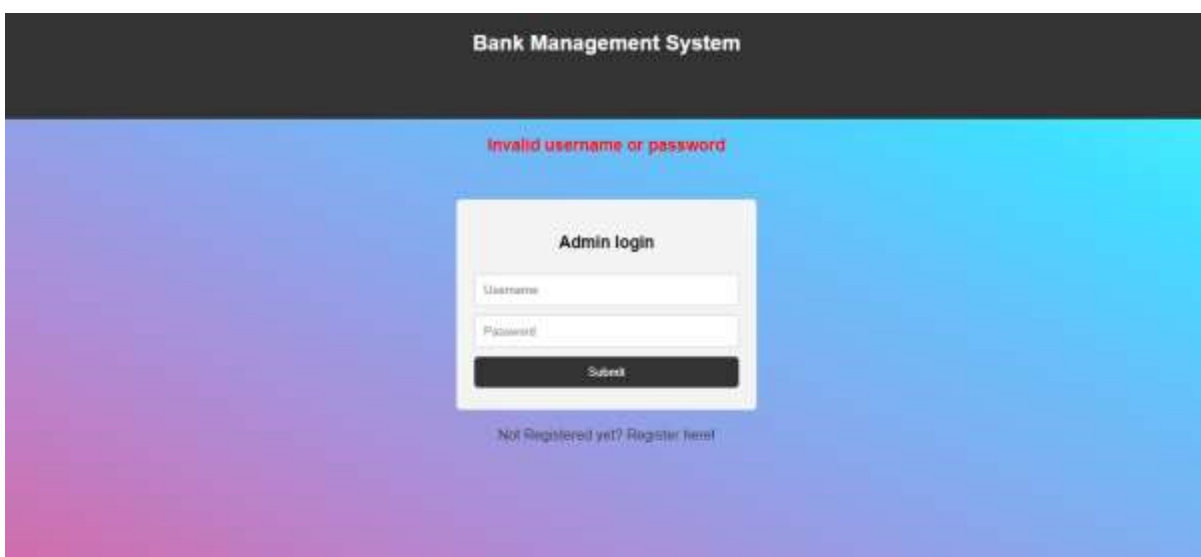
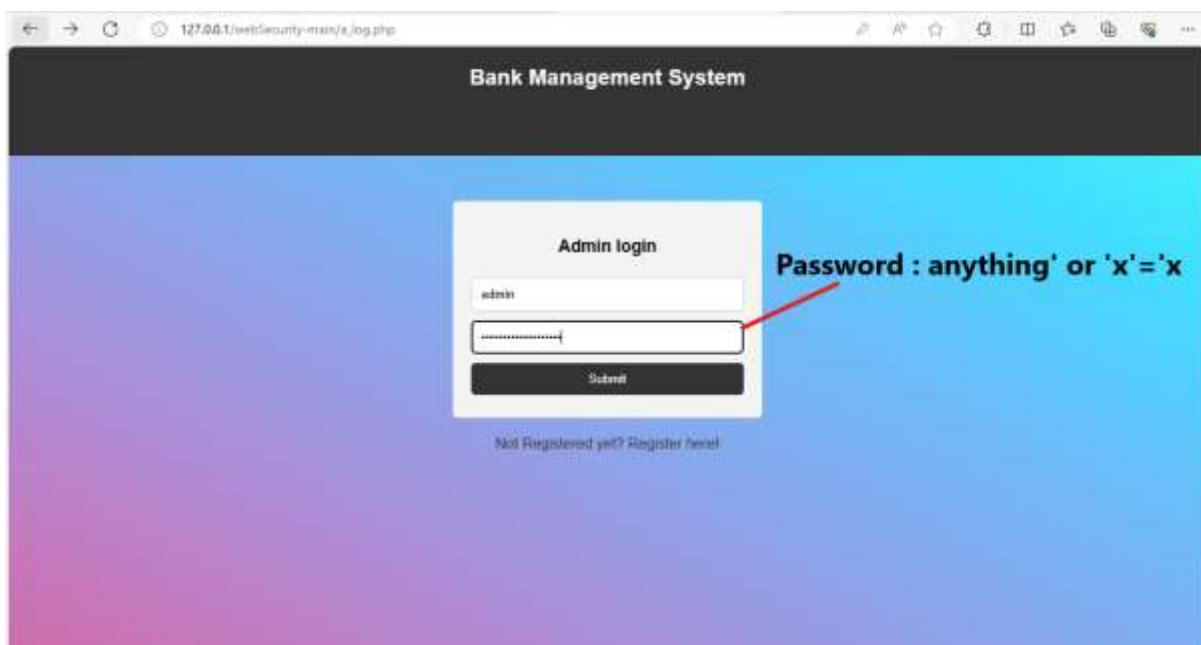
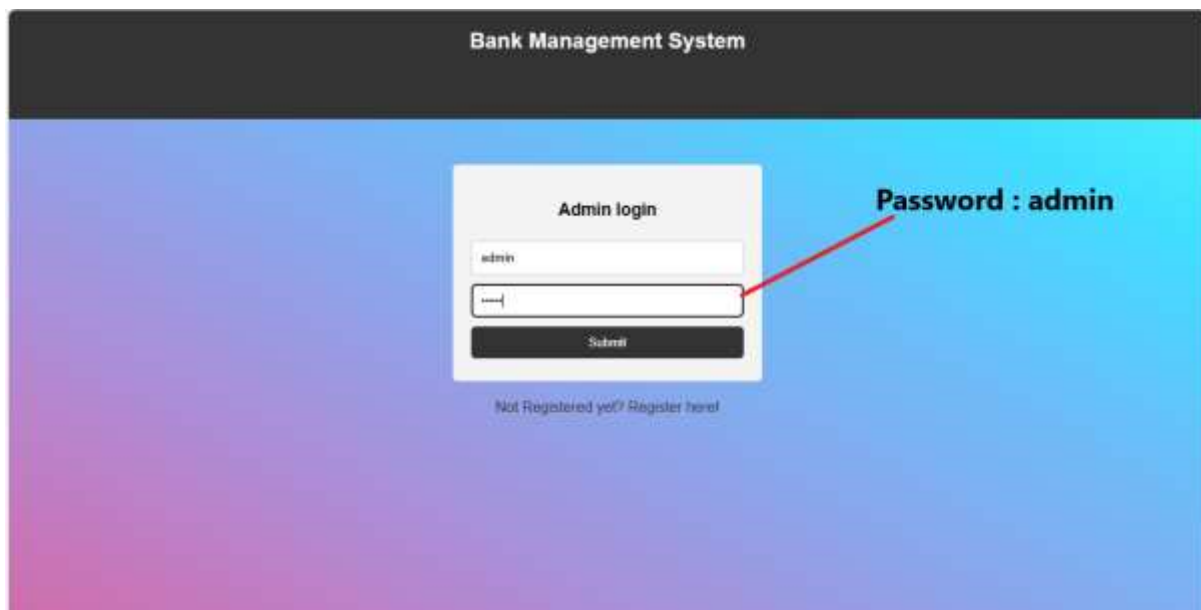
Details From Customers						
Requests From Customers						
S.NO	FieldName	Account number	Existing Value	New Value	OTP	Update
1	city	123456	II	Perambalur	<input type="button" value="Send OTP"/>	<input type="button" value="Update"/>

## Testing and Screenshots

### XSS PREVENTION:



### SQL INJECTION PREVENTION:



## PASSWORD CREATION:

The image displays two screenshots of a web application titled "Bank Management System" for password creation. The browser address bar shows "127.0.0.1/webSecurity-main/password\_creation.php".

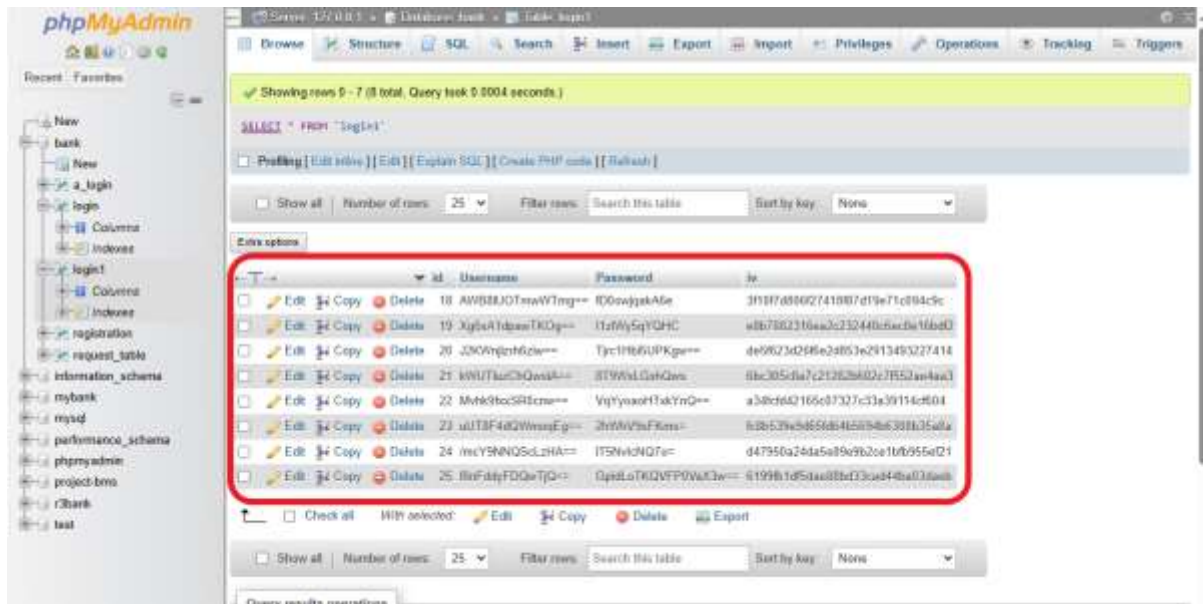
**Top Screenshot:** The "Create Your Password" form has empty "Username" and "Password" fields. Below the password field is a "Show Password" checkbox and an "Update Password" button. A red-bordered box contains the following "Note:"

**Note:**

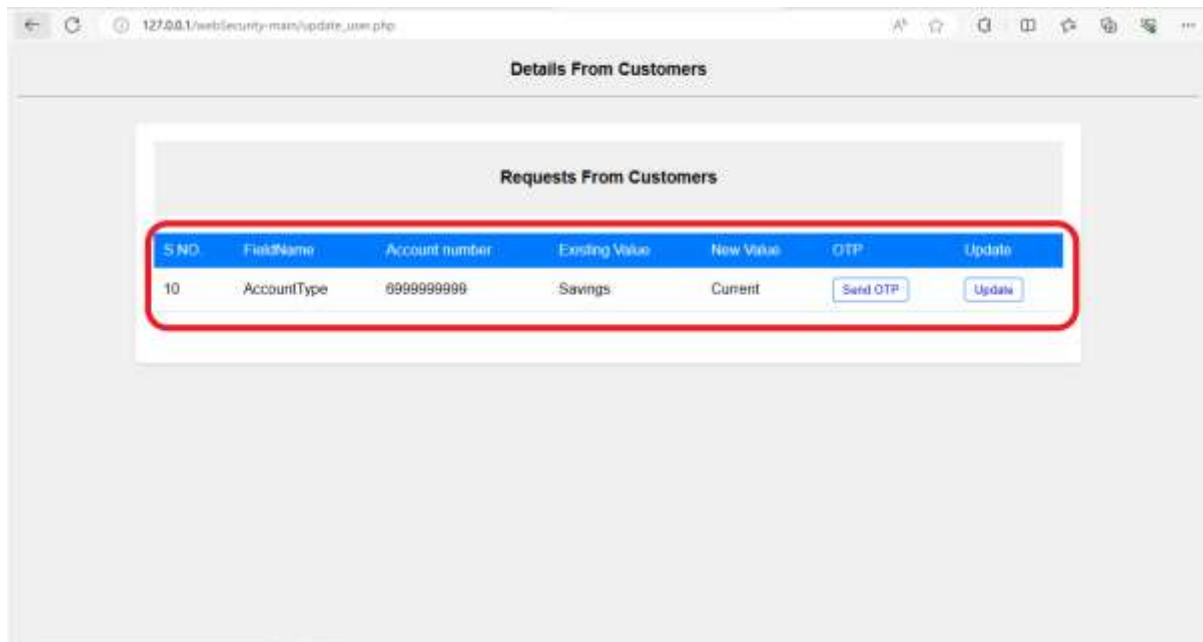
- >Make sure that your new password should contain atleast 1 uppercase,1 lowercase,1 number and 1 special character.
- >Make sure that your password should be more than 8 characters.
- >Make sure that your new password and confirm password should be same.
- >Make sure that your new password should not be your old password.
- >The confirmation message will be sent to your respective email id.

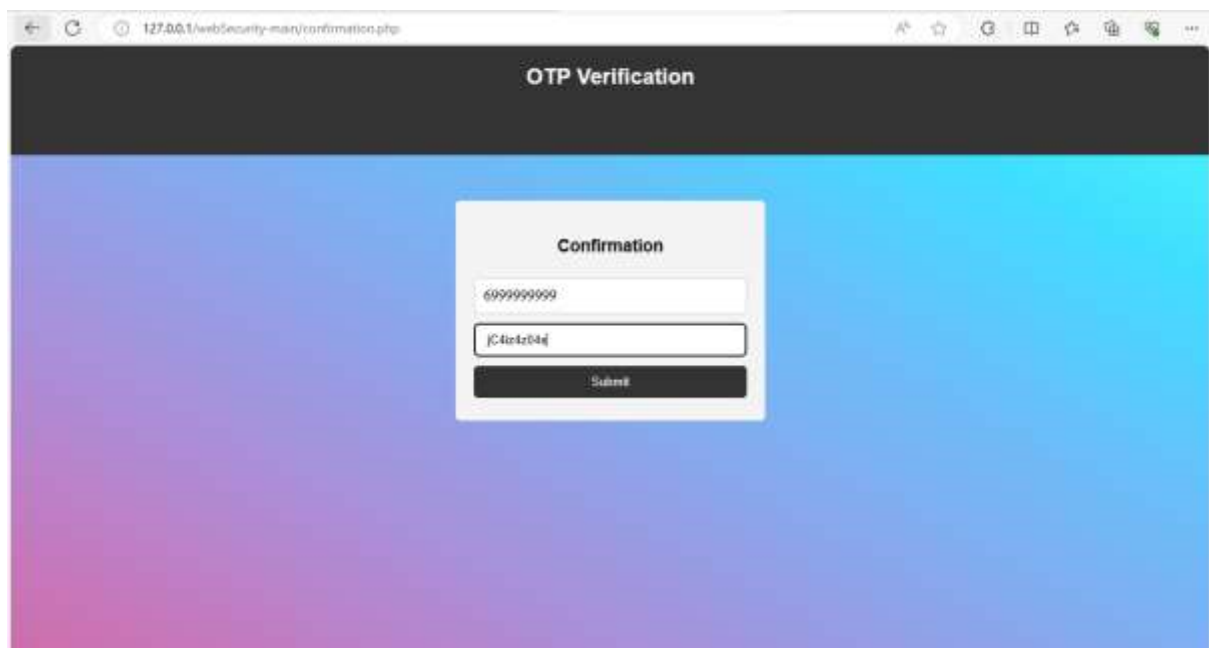
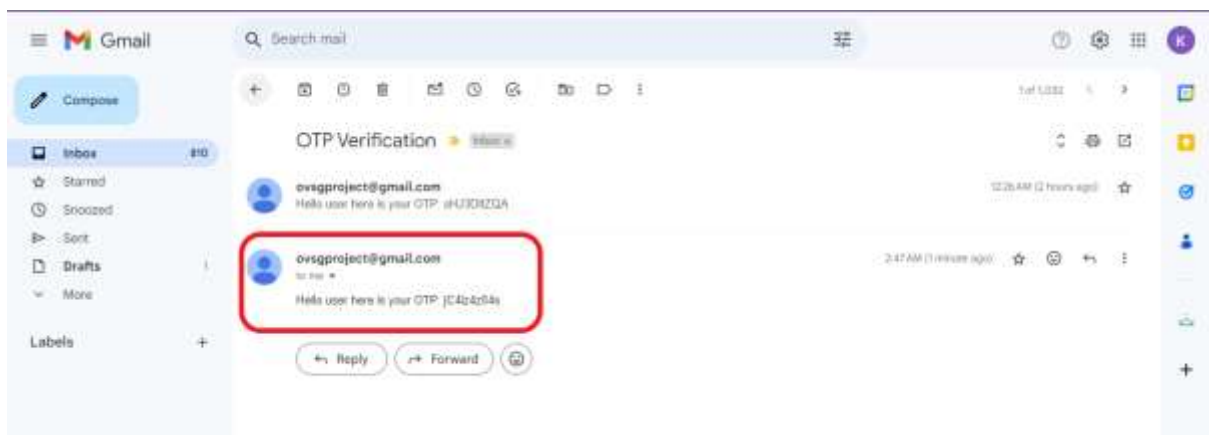
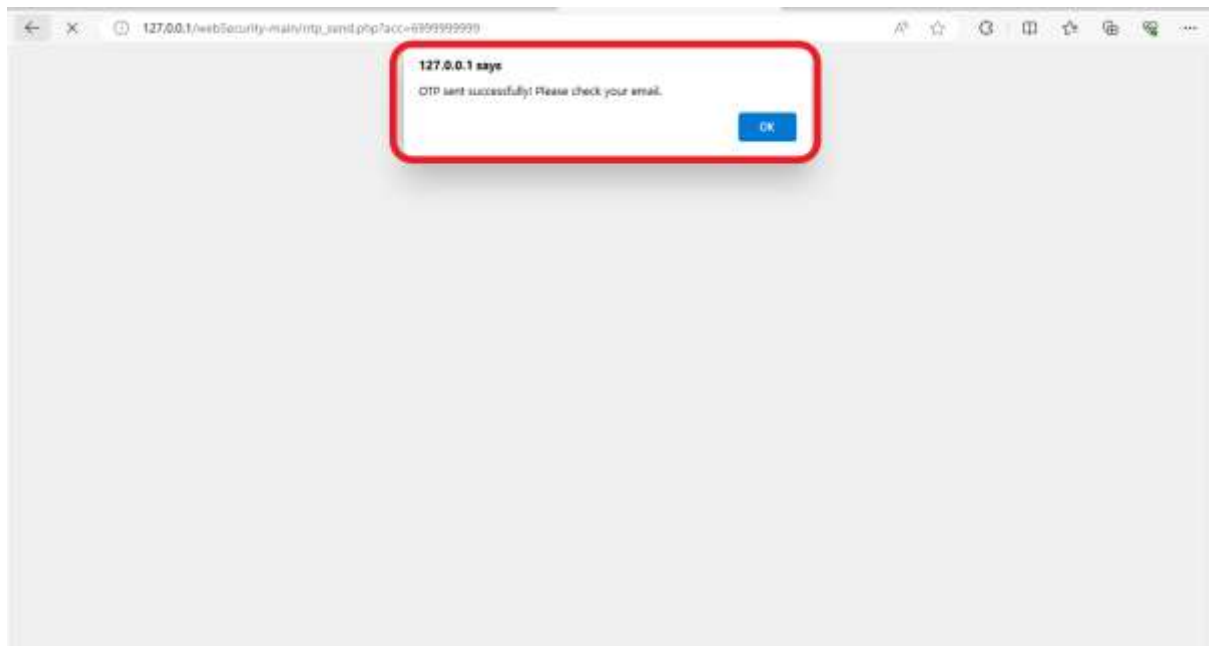
**Bottom Screenshot:** The form is shown after some input. The "Username" field has a green border and contains "6356995999". The "Password" field has a red border and contains "\*\*\*\*\*". Below the password field, the text "Provide a strong password" is displayed in red, followed by the "Show Password" checkbox and the "Update Password" button. The same "Note:" box is present at the bottom.

## ENRYPTION AND DECRYPTION:



## EDIT REQUEST-OTP AUTHENTICATION





## **Conclusion**

In conclusion, this project successfully enhances the security of a bank management website by implementing various measures such as strong password policies, encrypted passwords, and additional authentication steps. These measures help protect sensitive financial data from common security threats like brute force attacks, SQL injection, cross-site scripting (XSS), and unauthorized access. By improving the security and integrity of the website, users can have a safer online banking experience. The project's comprehensive approach to security makes it a valuable contribution to the field of information security and cybersecurity.