**# XSS Vulnerability in the online-banking-system Editor**

The `/net-banking/customer\_add\_action.php` file contains code that directly outputs user-inputted variables (e.g., `$sql1`, `$sql2`, `$sql3`, `$sql4`) and database error messages (`$conn->error`) to the HTML page **without any HTML escaping**.

For example:

```php

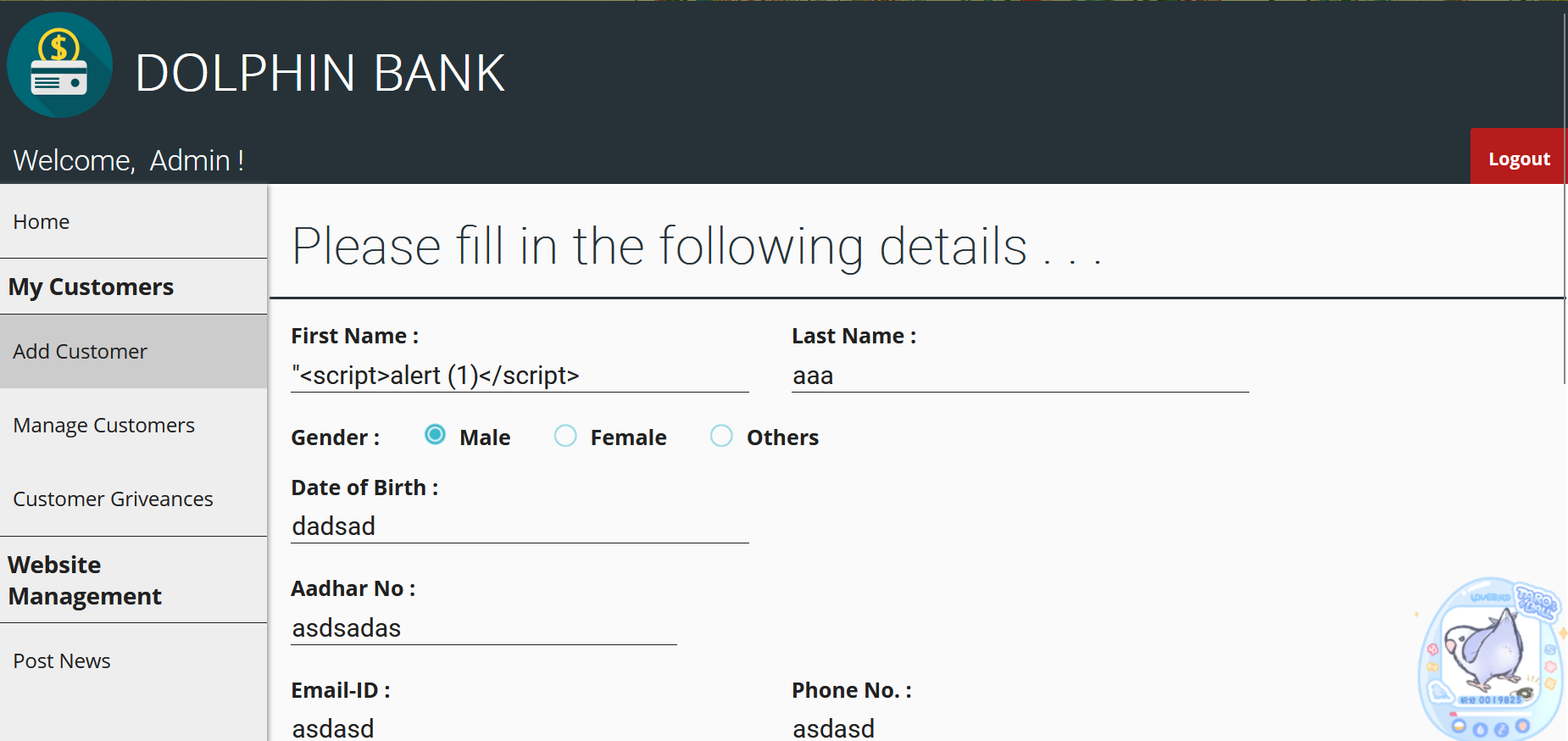
echo "Error: " . $sql1 . "<br>" . $conn->error . "<br>";

echo "Error: " . $sql4 . "<br>" . $conn->error . "<br>";

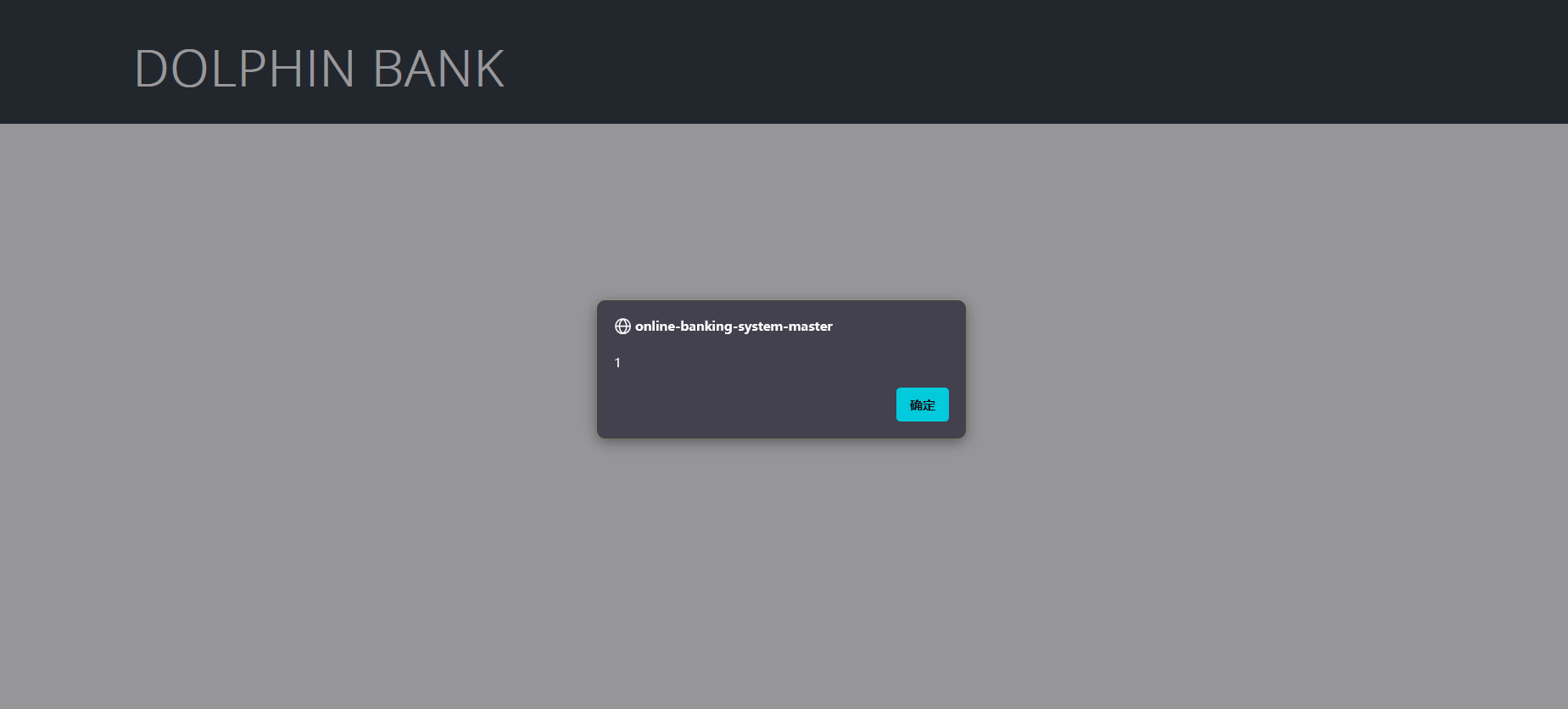
```

This results in an XSS injection vulnerability on the `/customer\_add.php` page.

When entering `<script>alert (1)</script>` in the "First Name" field:



This will trigger an XSS pop-up.

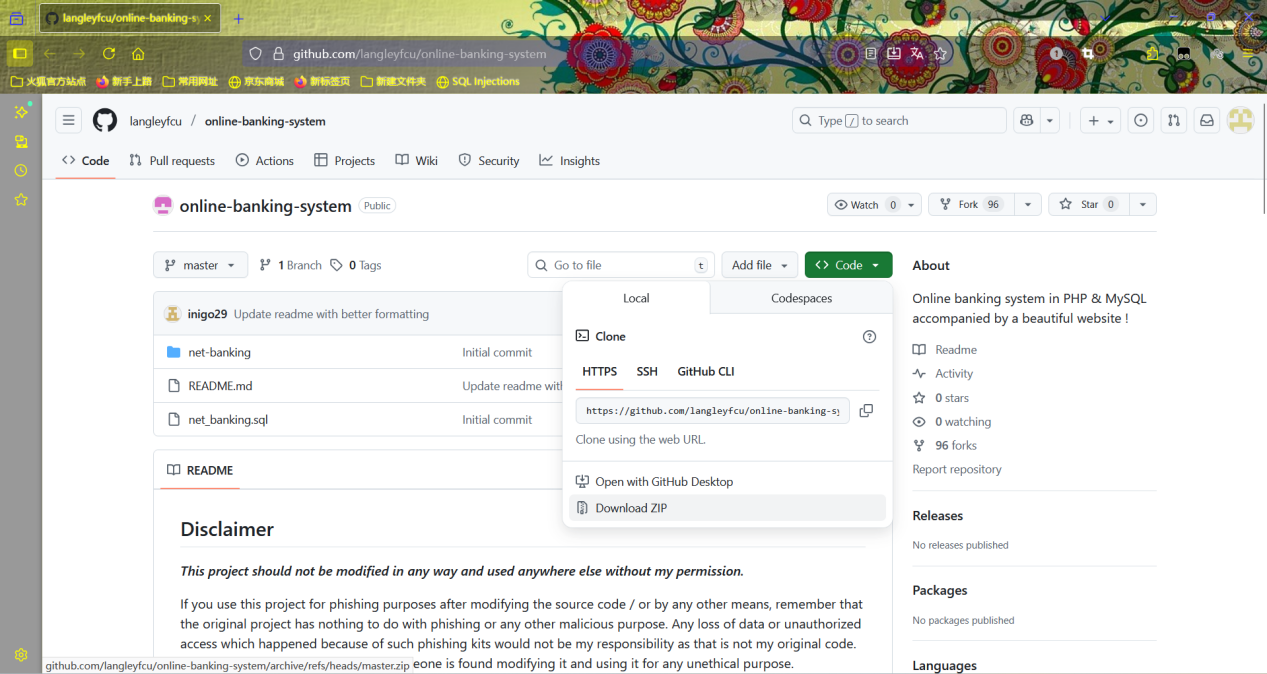


**# Project Setup and Reproduction**

**## 1. Download the Project**

Download URL: https://github.com/langleyfcu/online-banking-system

Click the "Download ZIP" button on this page to get the project files.

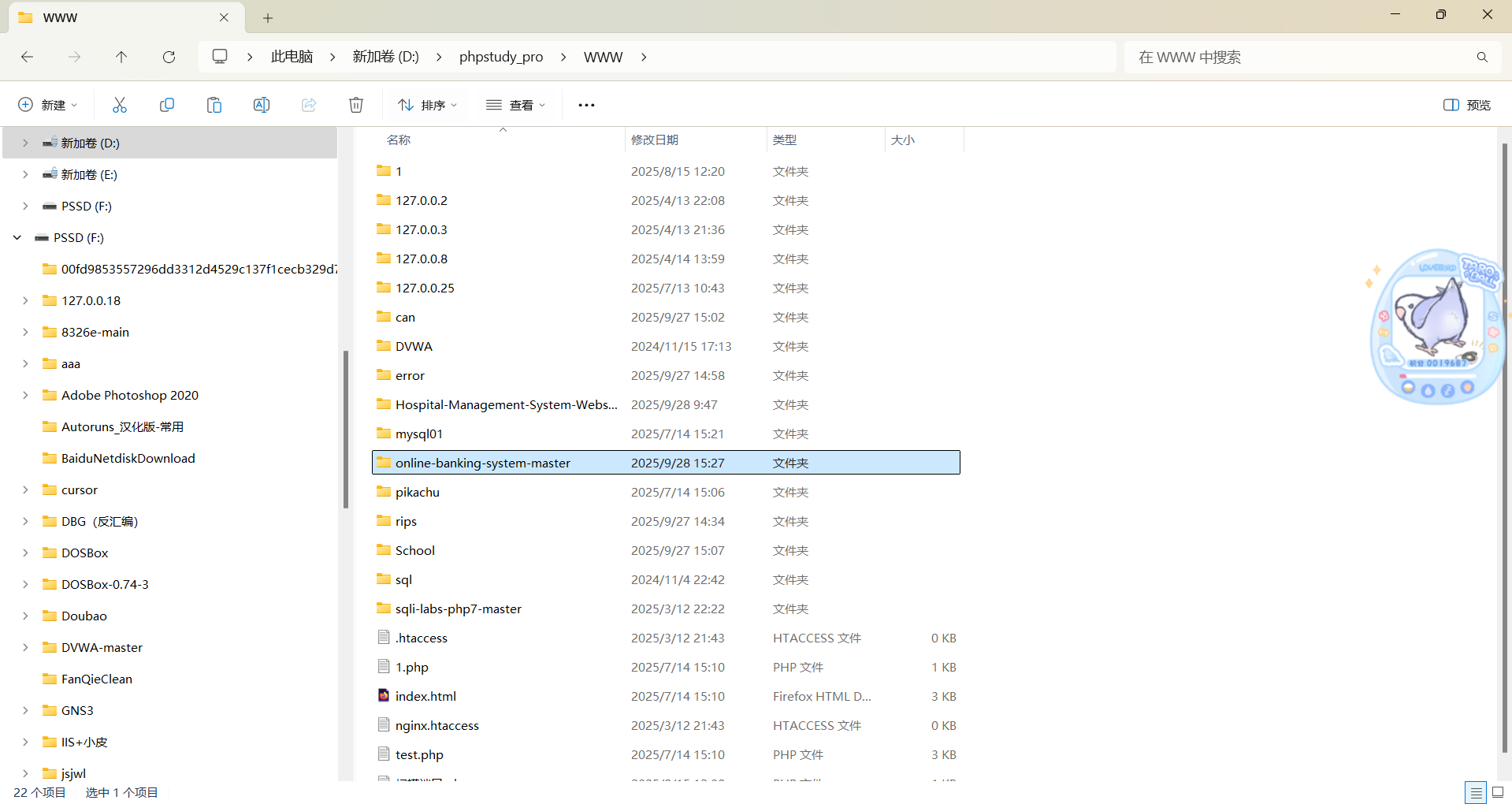


**## 2. Directory Structure**



**## 3. Deploy the Project**

1. Extract the downloaded ZIP file and place it under the `www` directory of phpStudy.



2. In phpStudy, create a new root directory with the path: `phpstudy\_pro/WWW/online-banking-system-master/net-banking`.



**## 4. Import the Database**

Import the `net\_banking` database into your local database environment (e.g., MySQL in phpStudy).



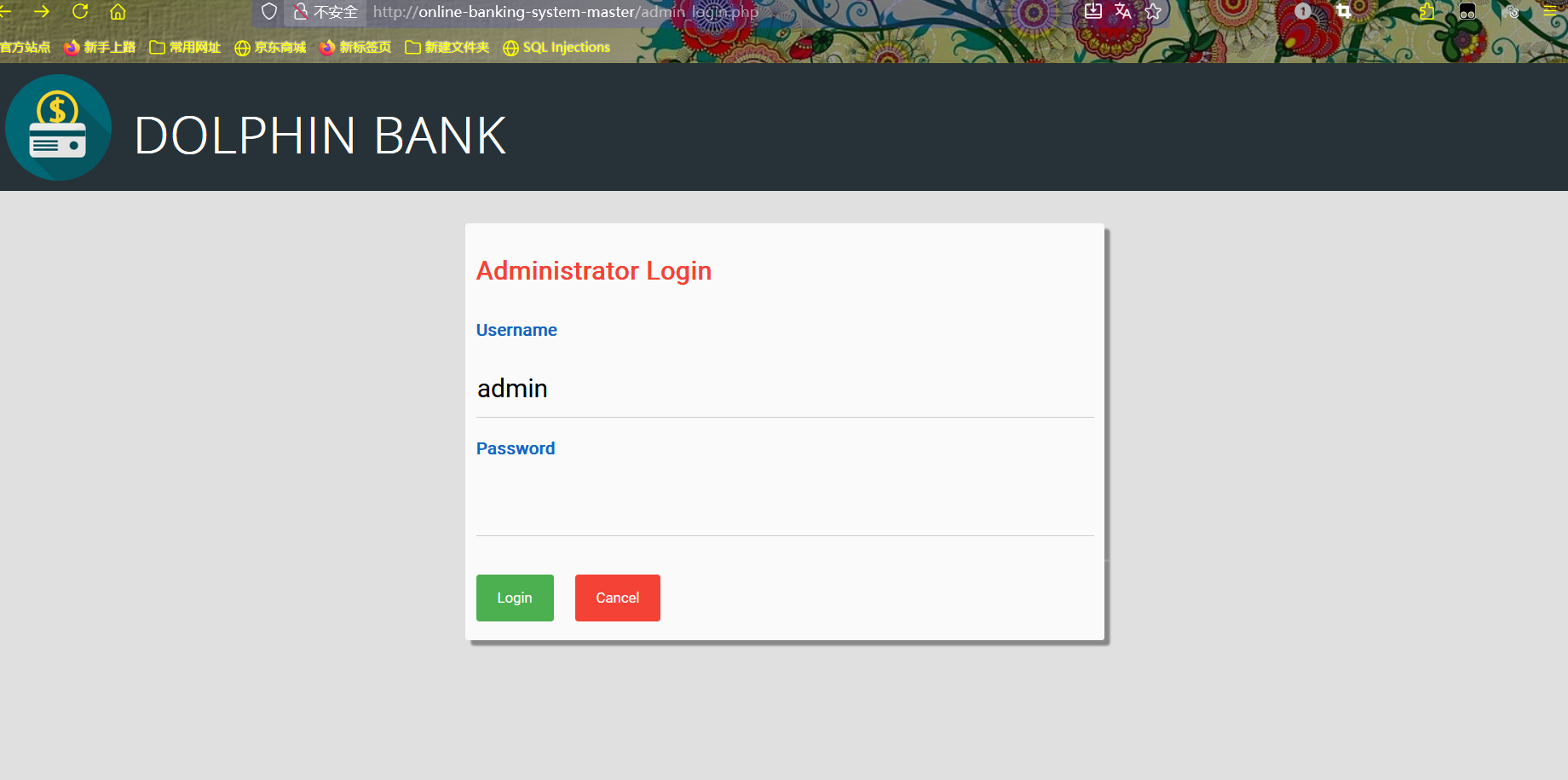
**## 5. Modify Configuration Files**

Update the username and password in the `connect.php` file to match your local database credentials.



**## 6. Log In to the System**

1. Open the URL: `http://[your-local-server]/online-banking-system-master/admin\_login.php` to access the login page.



2. Default login credentials (found in the database):

   - **\*\*Administrator\*\***:

     Username: `admin` | Password: `password123`

   - **\*\*Customers\*\***:

     - Nafees Zakee: Username: `zakee94` | Password: `nafees123`

     - Md Salman Ali: Username: `salman` | Password: `salman123`

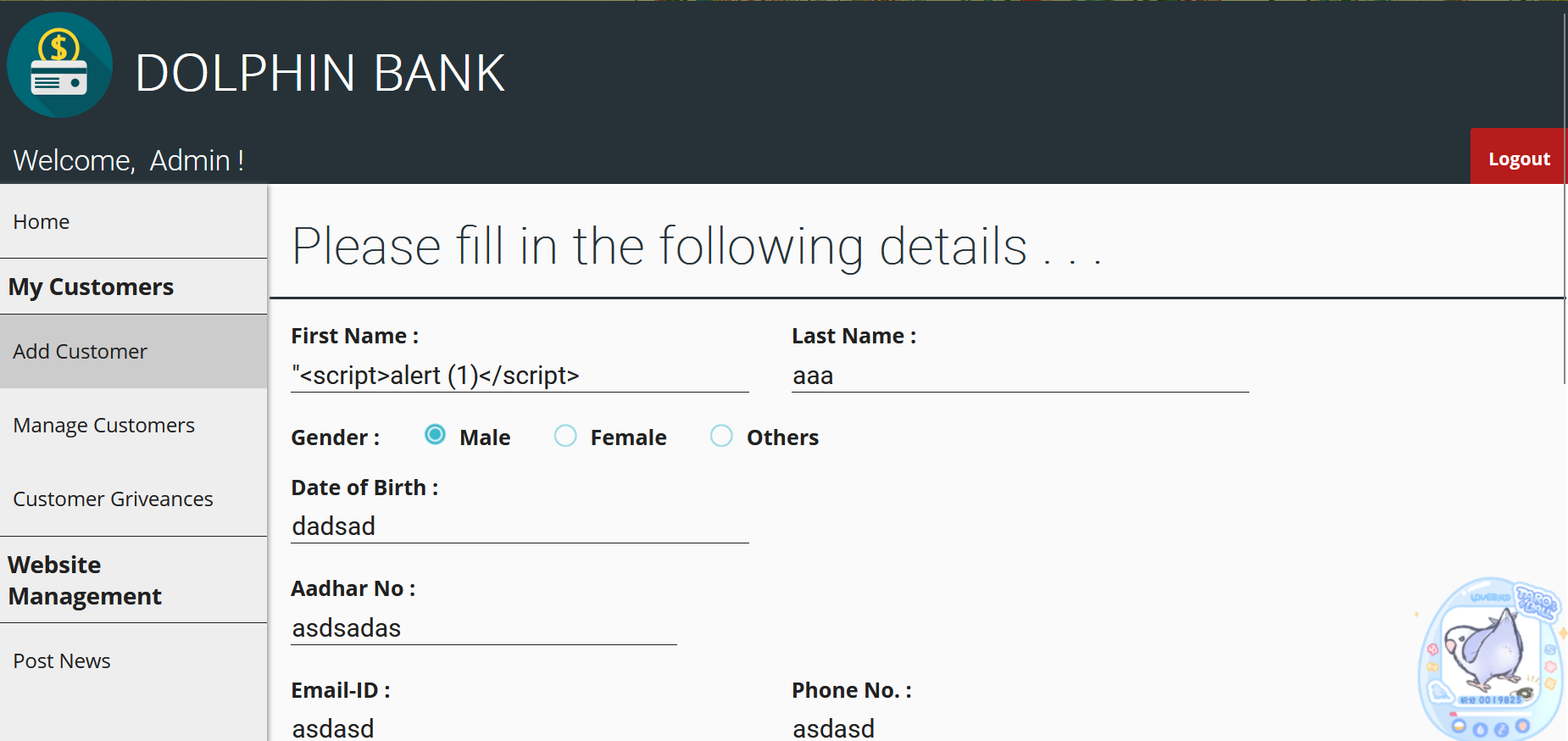
     - Tushar Kr. Pandey: Username: `tushar` | Password: `tushar123`

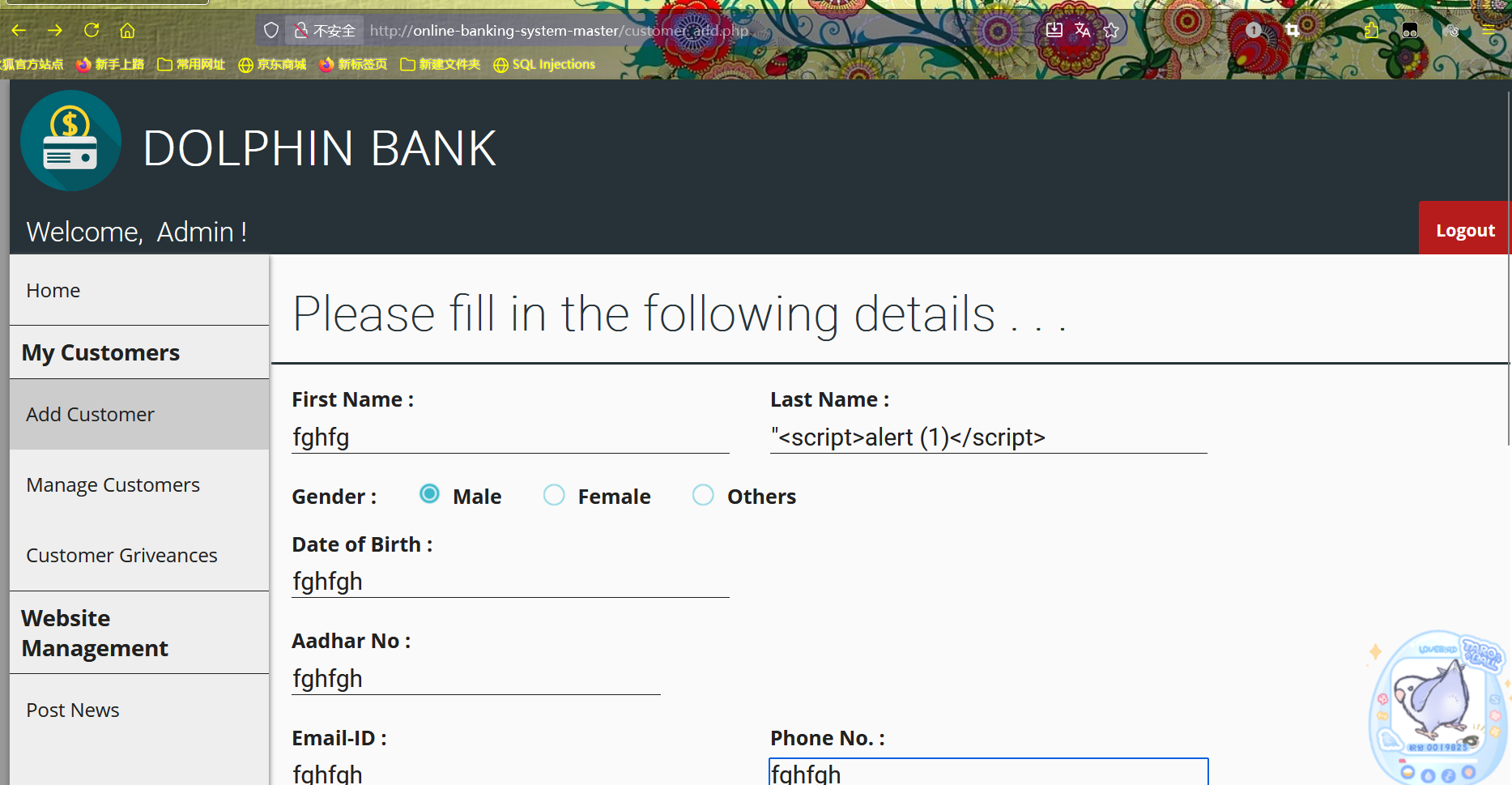
     - Jon Snow: Username: `jon` | Password: `snow123`

**## 7. Test the XSS Vulnerability**

1. After logging in as an administrator, access the `/customer\_add.php` page.

2. Enter `<script>alert (1)</script>` in the "First Name" field (or other input fields like "Last Name"—XSS may also trigger here).





3. Click the "Submit" button. The XSS pop-up will appear, confirming the vulnerability.

