**# XSS Vulnerability in php-business-website**

An XSS vulnerability exists on the `admin/contact.php` page.

The vulnerability arises from the following code in `admin/contact.php`:

```php

$twitter = $\_POST['twitter'];

$sql = "UPDATE contact SET twitter=? WHERE id=1";

$query->eQuery($sql, [$twitter]);

echo json\_encode(['success' => true, 'message' => 'Twitter link has been updated!', 'twitter' => $twitter]);

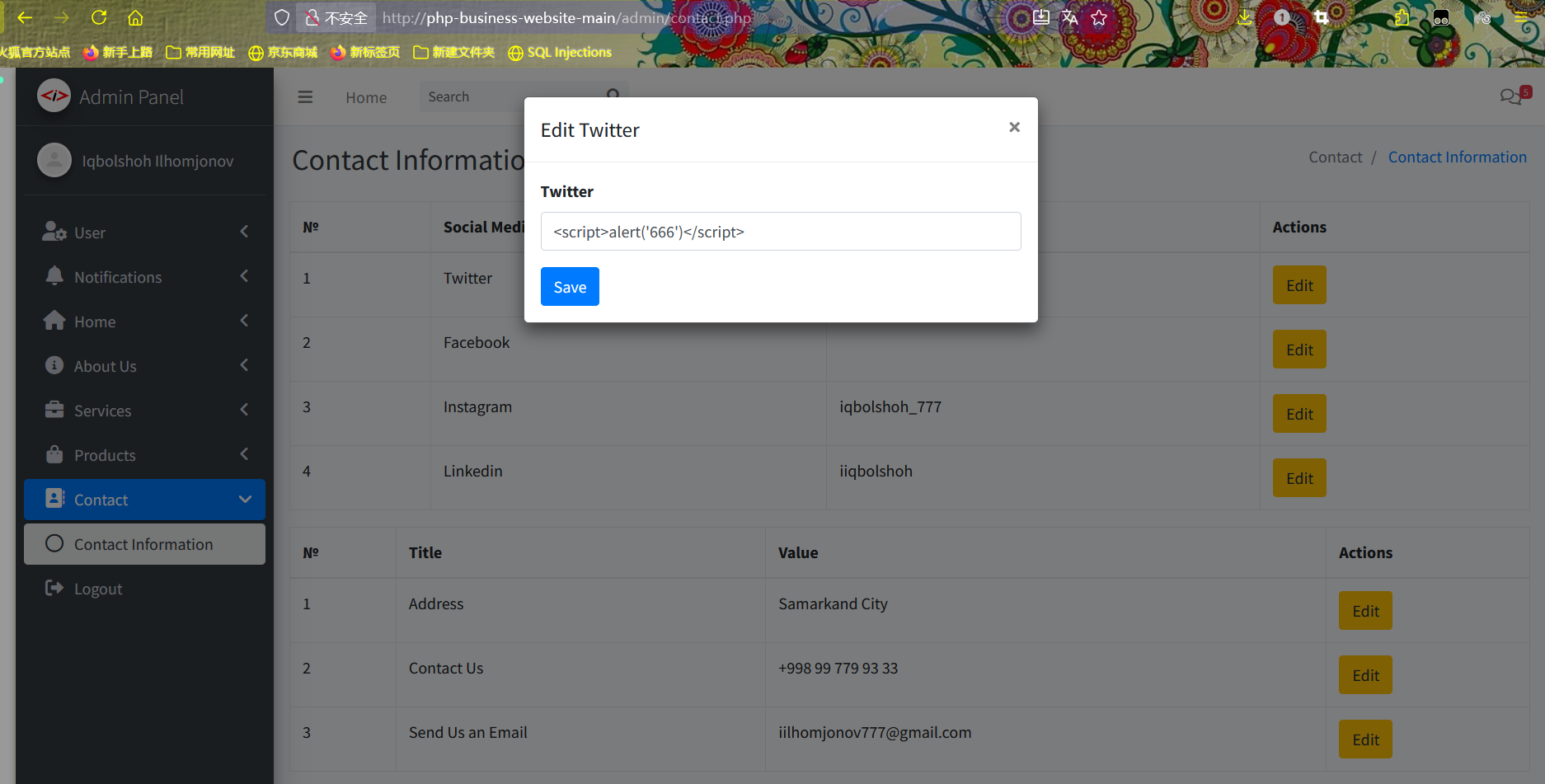
```

This code **\*\*does not perform output filtering on the user-input `$twitter`\*\***; it directly returns the original user input to the frontend, where it may be rendered into the DOM. If the frontend inserts the received `twitter` field into the DOM (e.g., using methods like `innerHTML` or `v-html`) and `$twitter` contains malicious scripts (such as `<script>alert('steal cookie')</script>` or `<img src=x onerror=alert(1)>`), the browser will execute these scripts, leading to an attack.

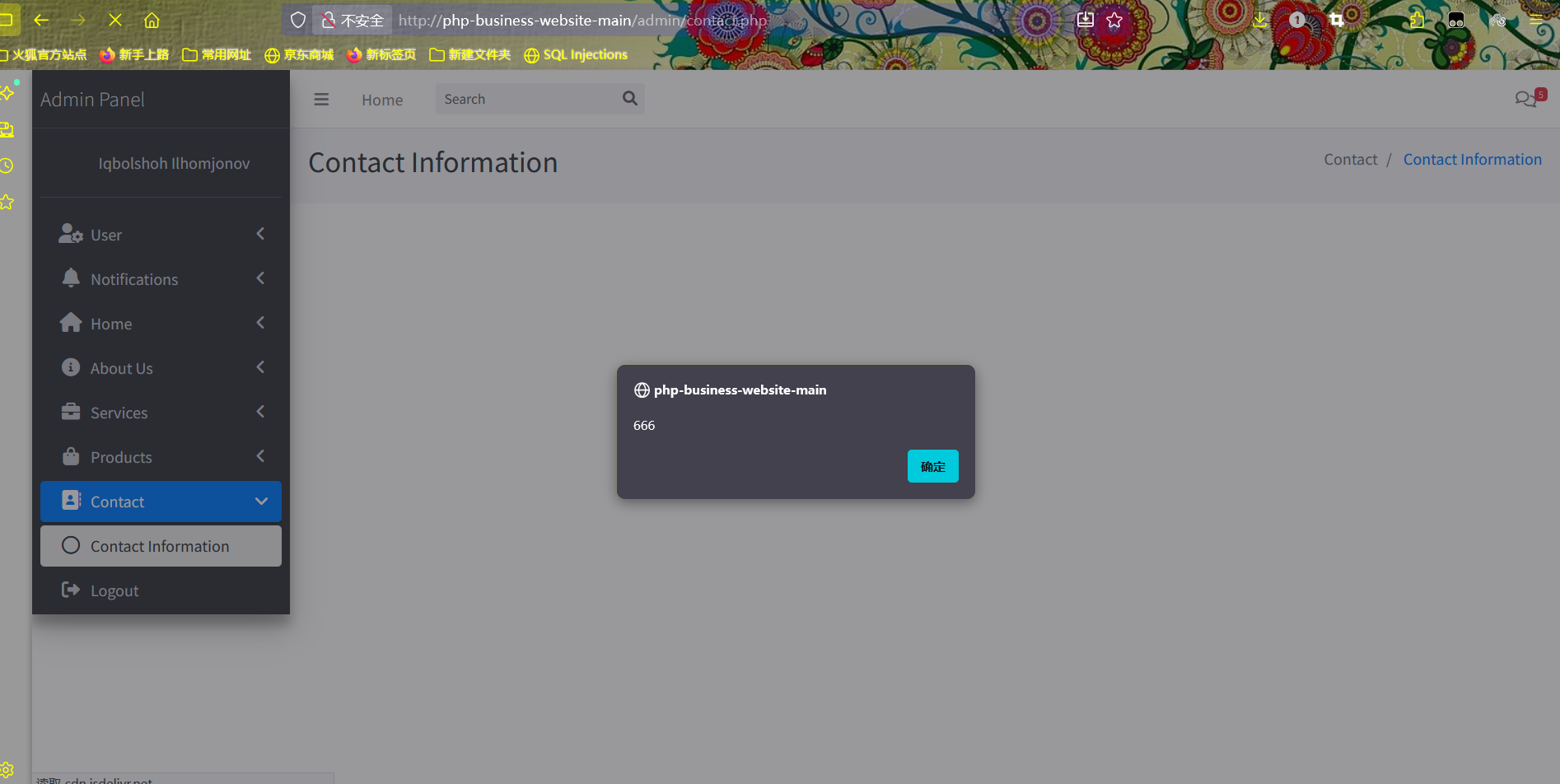
To exploit this vulnerability:

1. Navigate to `http://php-business-website-main/admin/contact.php`

2. Click "Edit" and enter `<script>alert('666')</script>` in the Twitter input field



This will trigger a **\*\*stored XSS\*\*** attack.

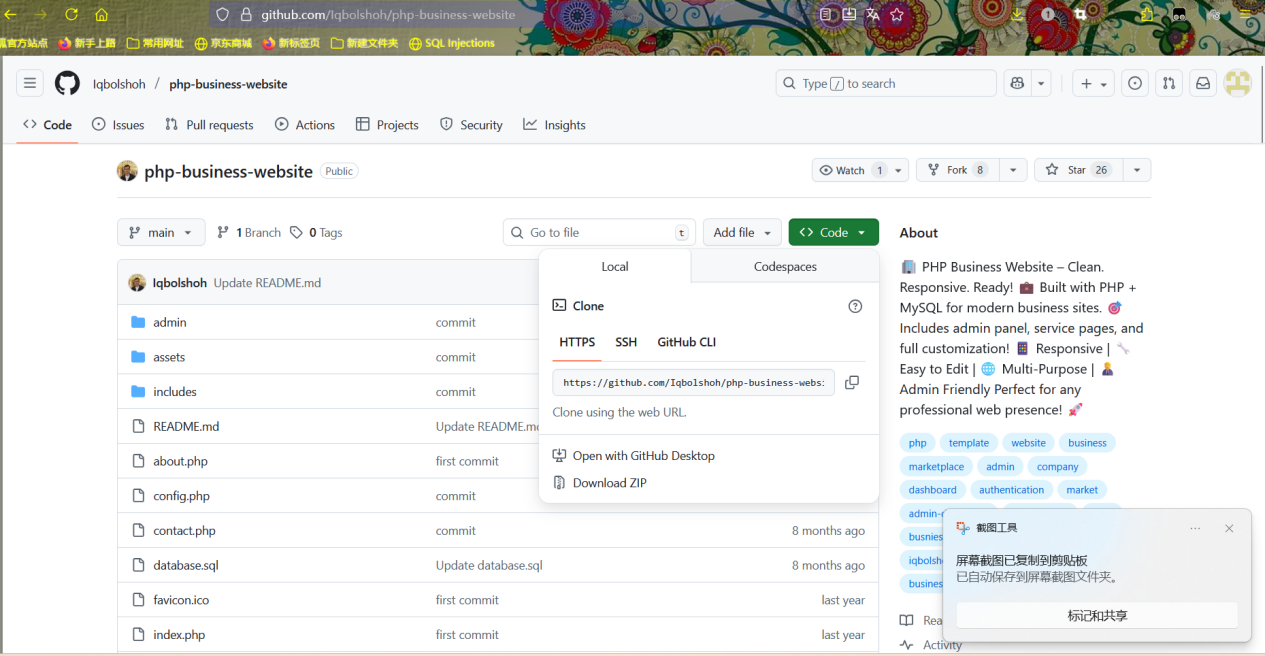


**# Project Setup & Vulnerability Reproduction**

**## GitHub Project URL**

https://github.com/Iqbolshoh/php-business-website

**## Download Page & General Directory Structure**



**## Setup Tutorial (PHPStudy)**

**### 1. Start Services**

Open PHPStudy and launch Apache and MySQL.

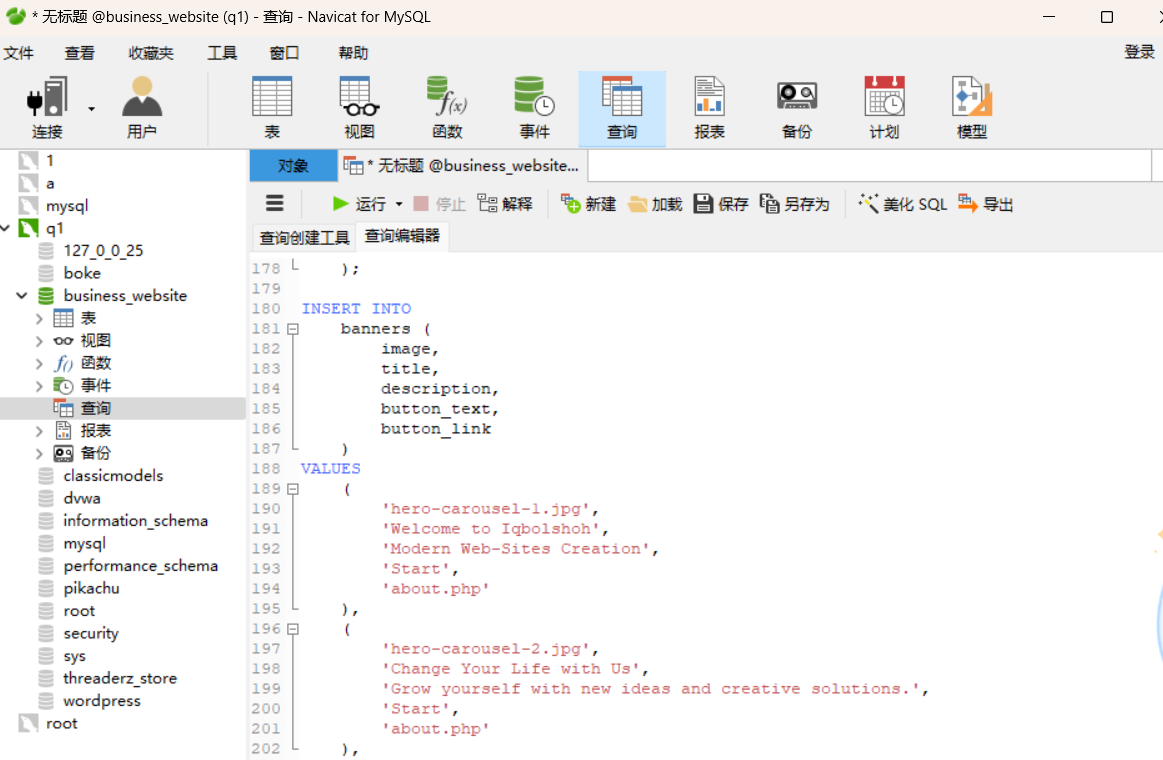
**### 2. Place Files**

Extract the downloaded project files and place them under `phpstudy\_pro/WWW`.

**### 3. Import Database Structure**

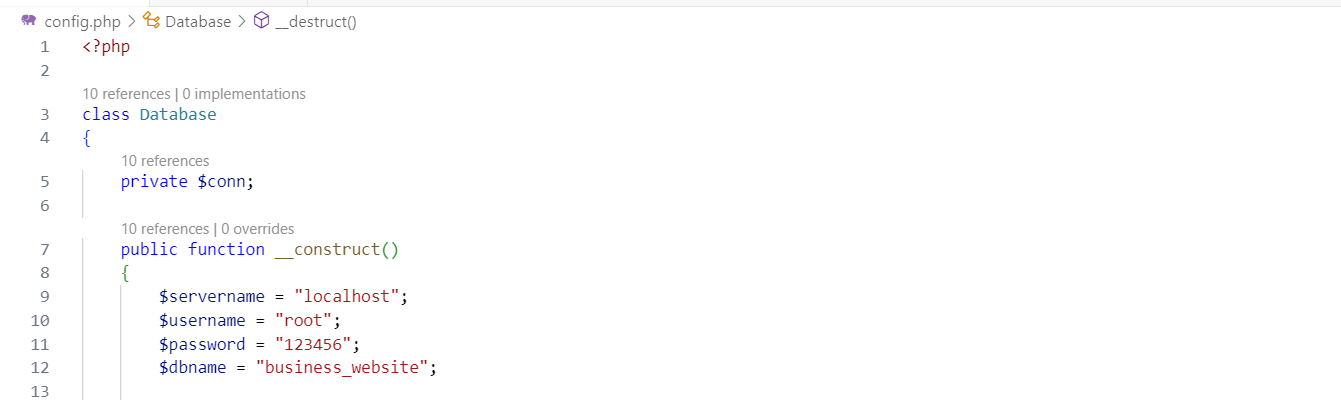
1. Open Navicat for MySQL and connect to your database.

2. Create a new query and run the SQL code from the downloaded `database.sql` file.



**### 4. Configure Database Connection**

Edit `config.php` and update the host, username, password, and database name to match your environment (default settings: host = `localhost`, username = `root`, password = empty, database name = `business\_website`).



**### 5. Create a New Website in PHPStudy**

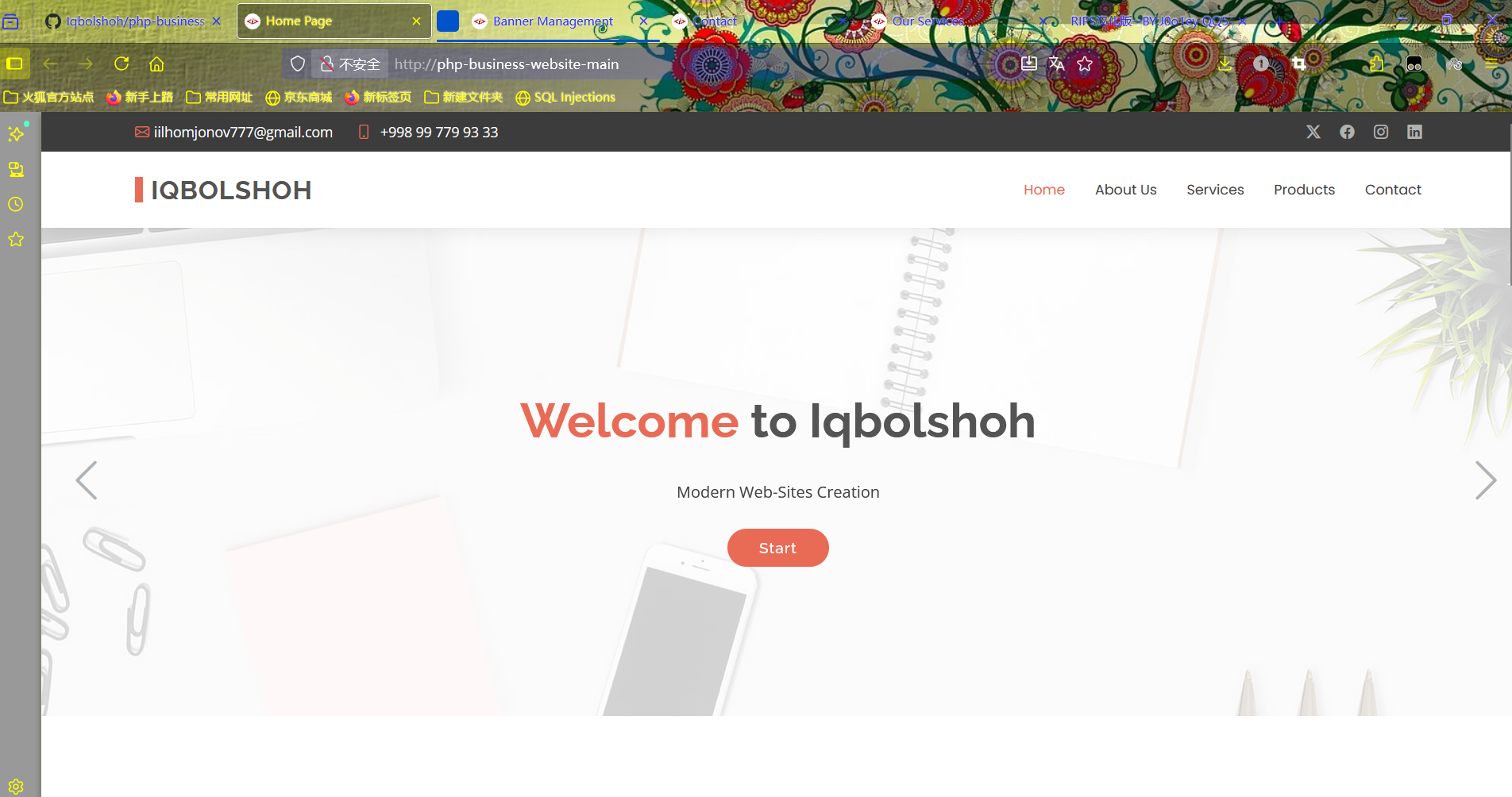
In PHPStudy, create a new website and set its root directory to `D:/phpstudy\_pro/WWW/php-business-website-main`.



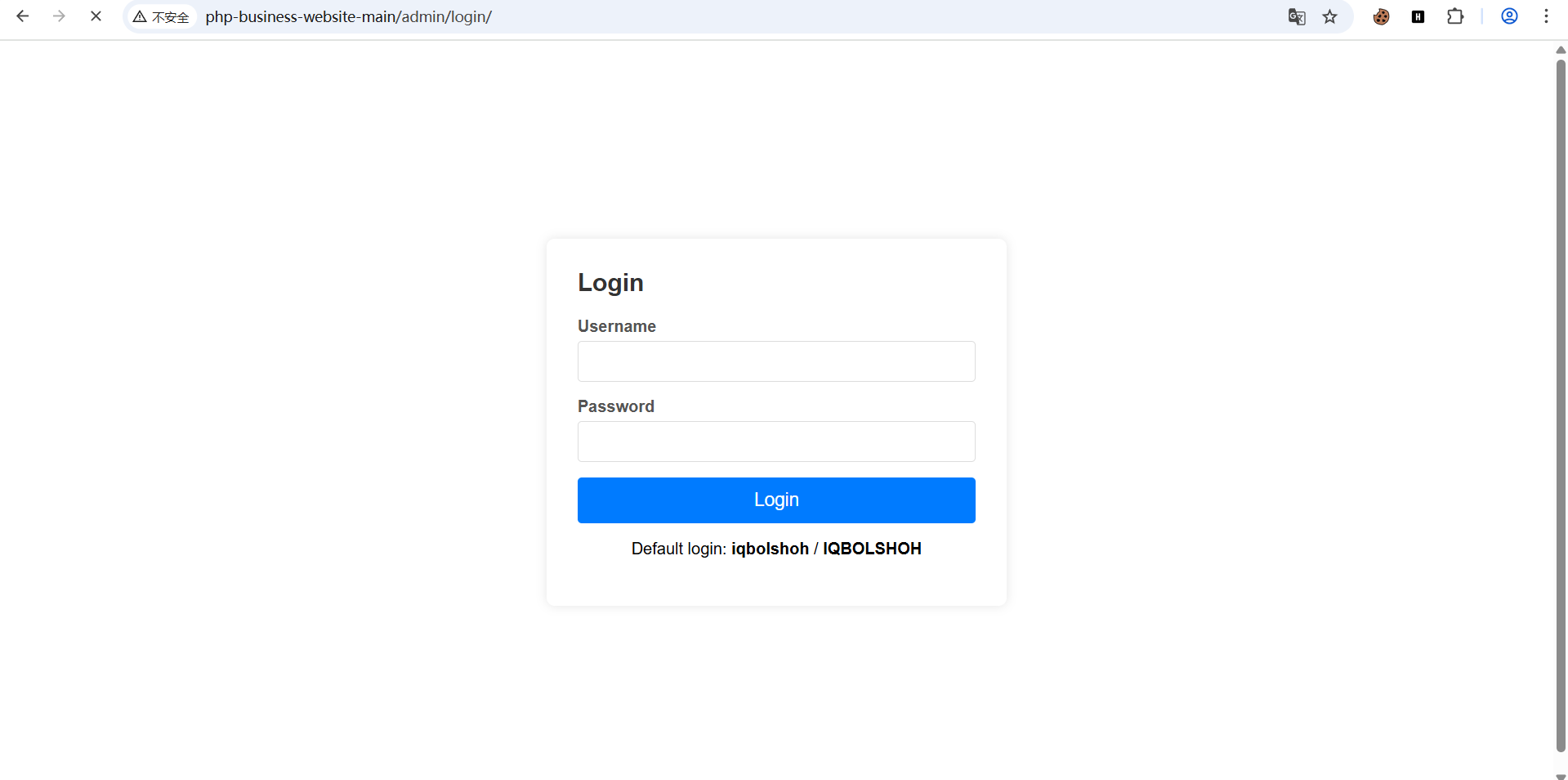
**### 6. Access and Test**

Launch the website from PHPStudy to verify access:

- **\*\*Frontend Page\*\***: Should load normally.



- **\*\*Admin Login Page\*\***: Accessible via the admin panel entry.



**### 7. Admin Login**

- Username: `iqbolshoh`

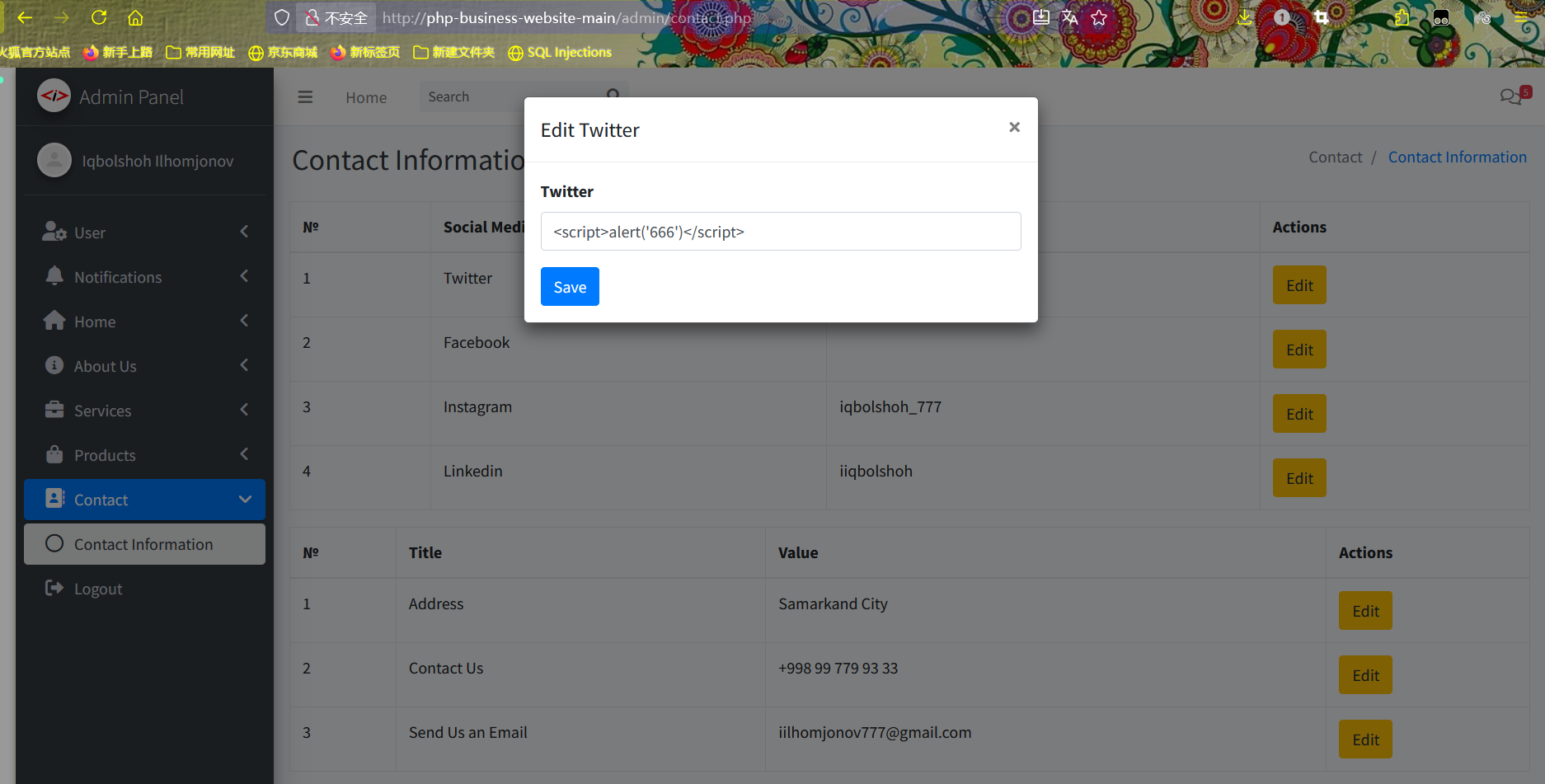
- Password: `IQBOLSHOH`

**## Vulnerability Reproduction Steps**

1. Navigate to `http://php-business-website-main/admin/contact.php`.

2. Locate the Twitter entry and click "Edit".

3. Enter `<script>alert('666')</script>` in the input field.



This will trigger a **\*\*stored XSS\*\*** attack.

