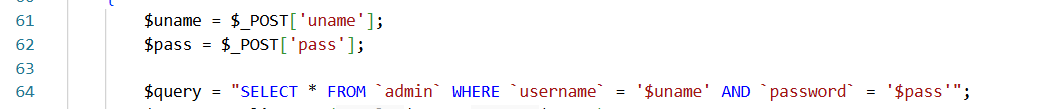
# SQL Injection Vulnerability in the Online-Food-Ordering-System

## Brief Demonstration

The `admin/admindash.php` file contains code that has a \*\*high-risk SQL injection vulnerability\*\*. The core issue is that the user inputs `$uname` (username) and `$pass` (password) are directly concatenated into the SQL query statement without any security processing.



An attacker can enter `' OR '1'='1` in the \*\*username (uname)\*\* field of the login form, and enter any value in the password field.

At this point, the concatenated SQL statement becomes:

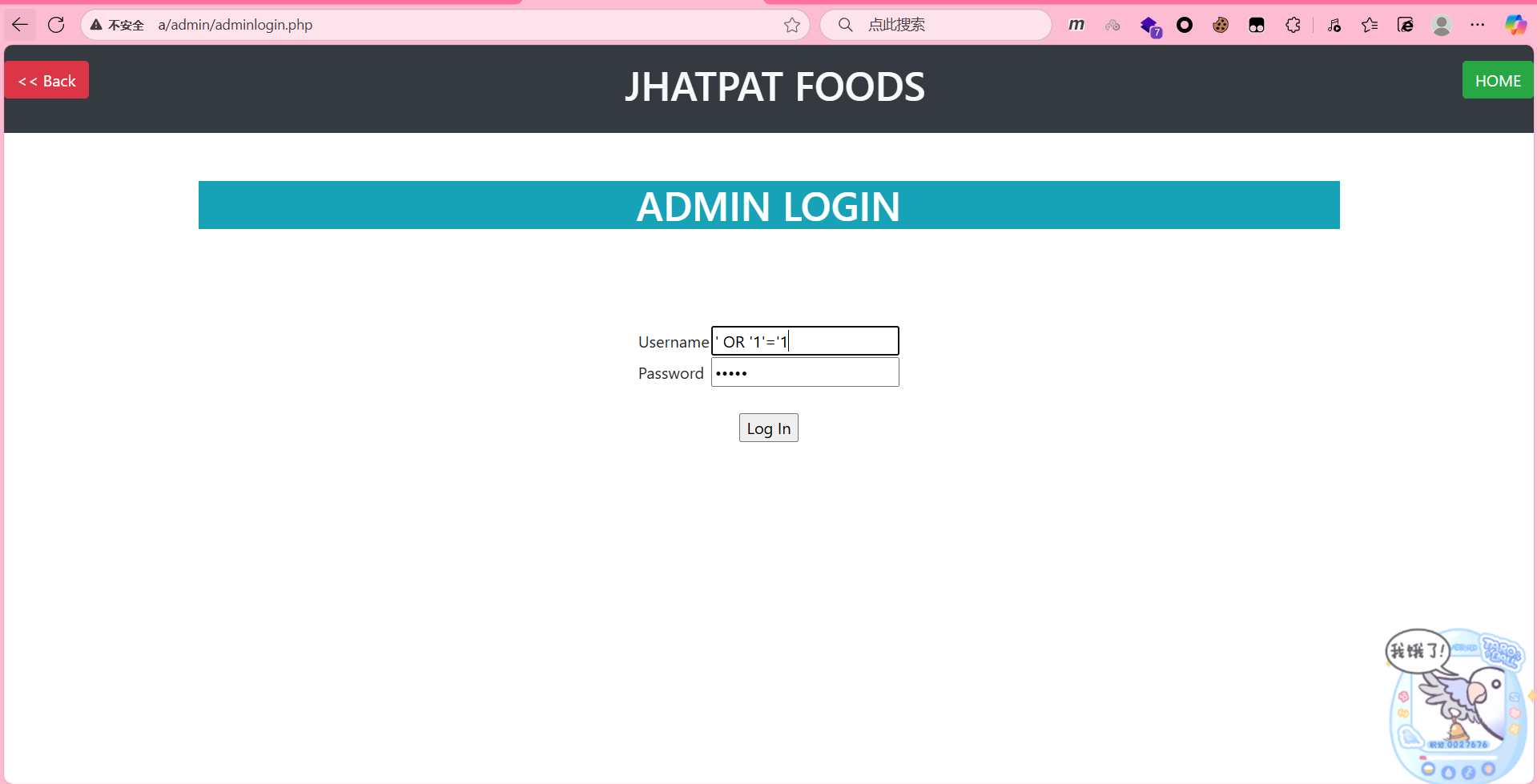
```sql

SELECT \* FROM `admin` WHERE `username` = '' OR '1'='1' AND `password` = 'any\_value'

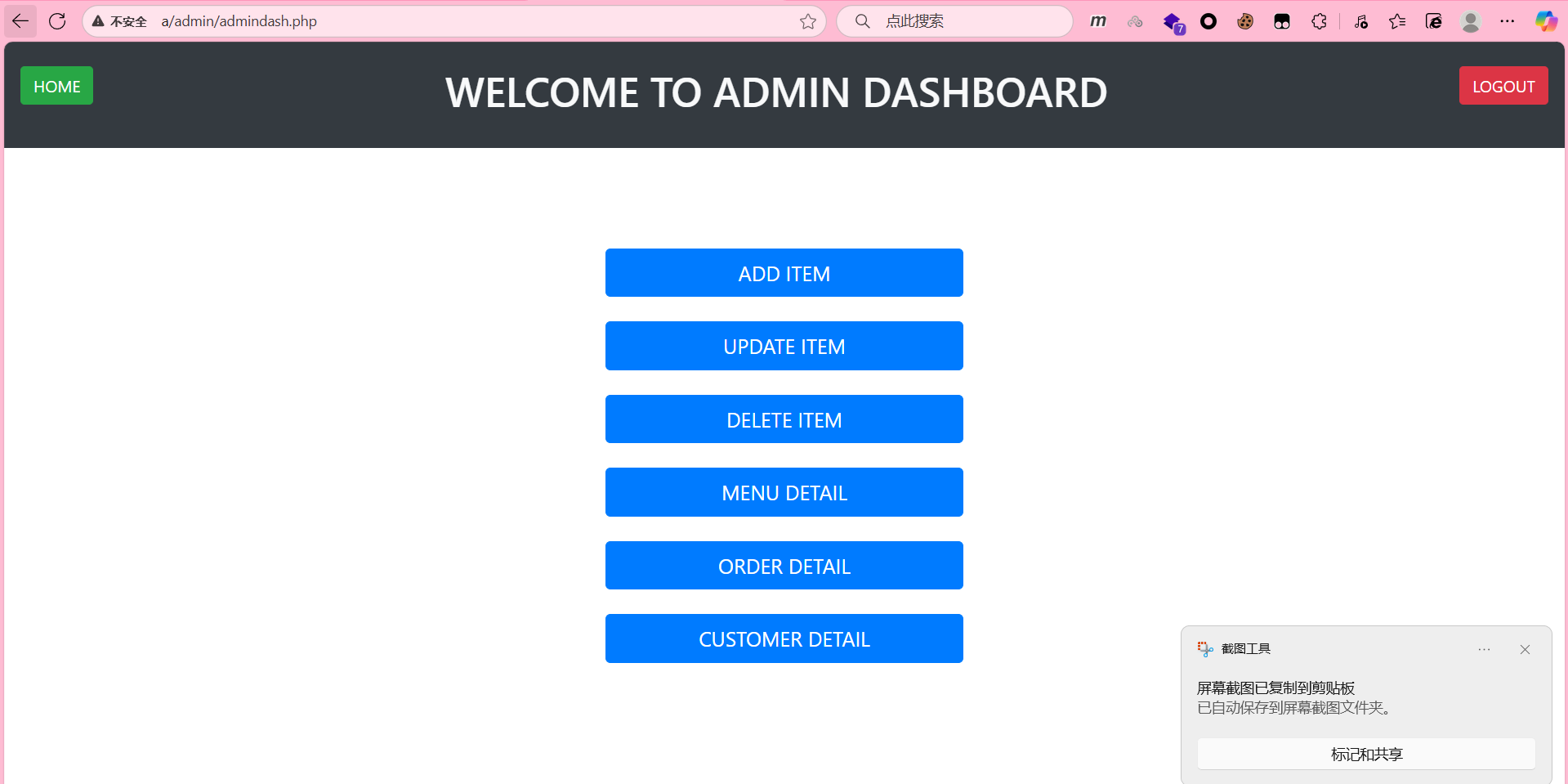
```

This allows login with any password.

Example:



Successful login:

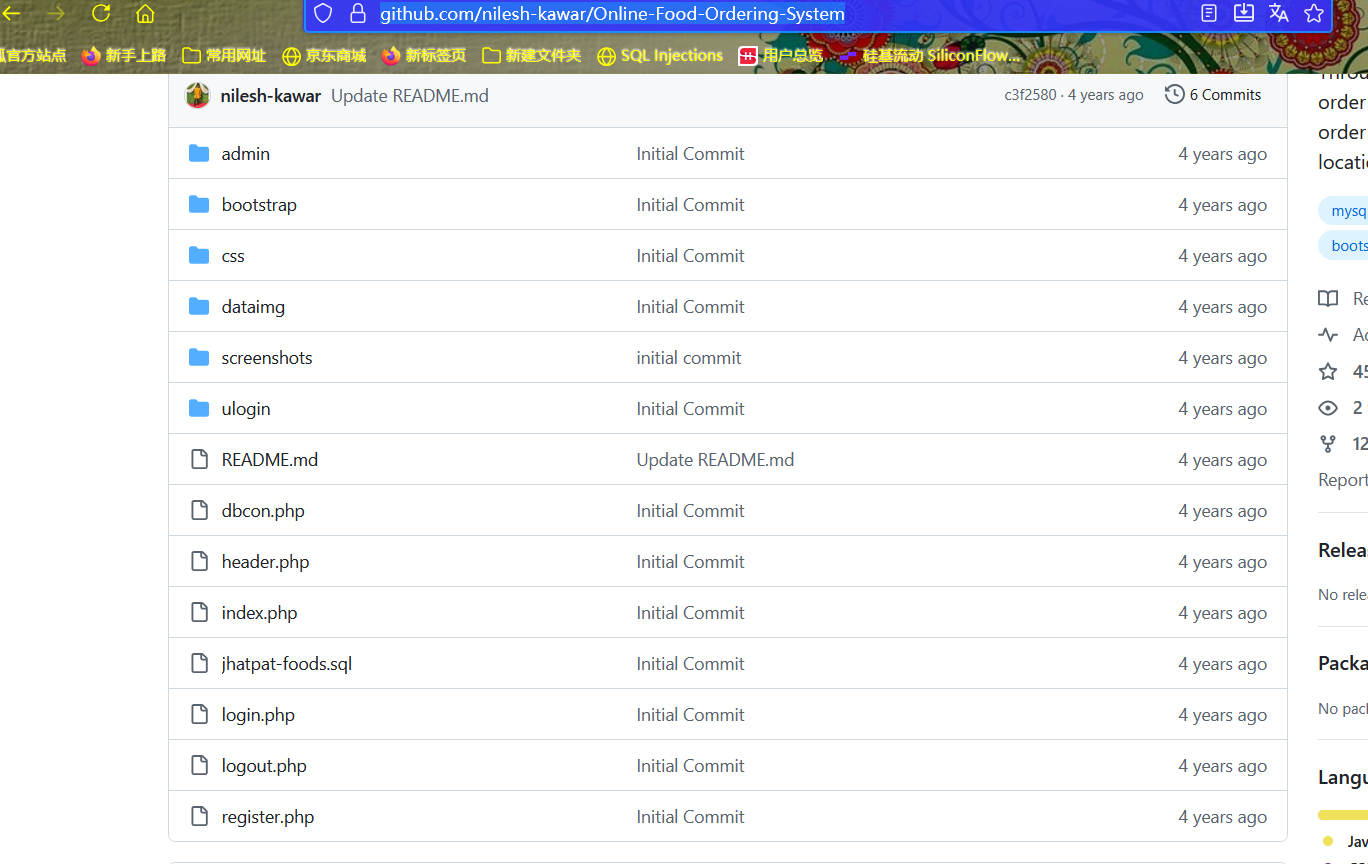


# Project Setup and Vulnerability Reproduction

## Download Link

https://github.com/nilesh-kawar/Online-Food-Ordering-System

## Directory Structure



## Setup Steps

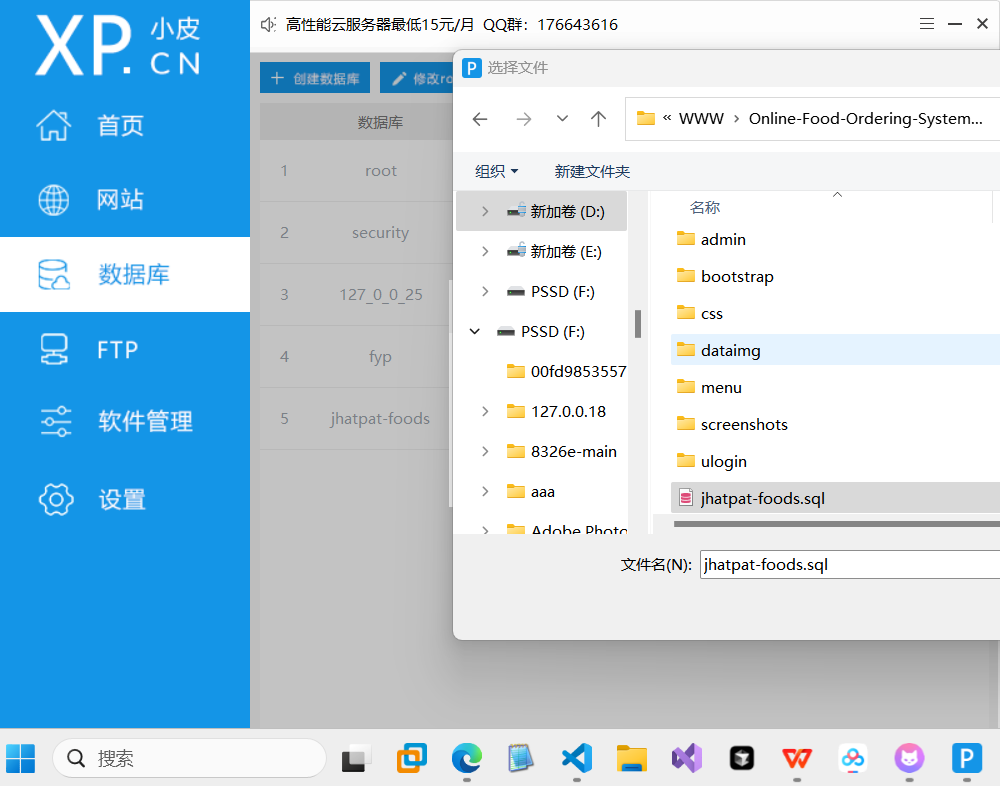
1. Launch phpstudy (with Apache + MySQL).

1. Place the project files into the \*\*Web root directory\*\* (`www`) of phpstudy.



3. Import the database

Create a new database named `jhatpat-food` and import the downloaded `jhatpat-foods.sql` file.



4. Modify the database configuration file (`dbcon.php`) to match your database settings.

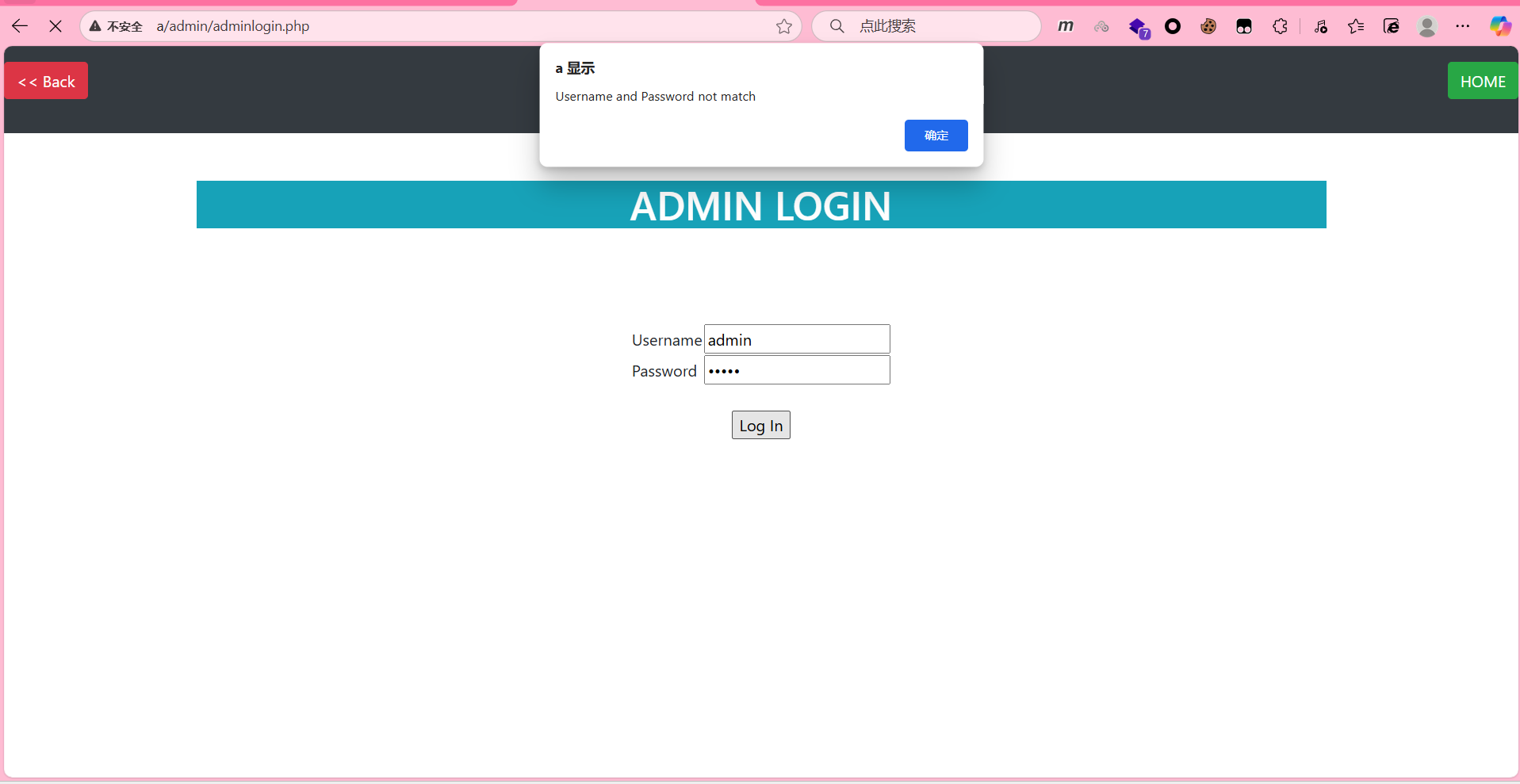


5. Successfully set up! Access the webpage via phpstudy, e.g.:

http://a/admin/adminlogin.php

# Normal Function Demonstration

- Entering an incorrect username prevents login:



- However, entering `' OR '1'='1` (in the username field):

