

CVE / Billing System Project v1.0 / CVE-2022-43214(sql in printOrder.php).md

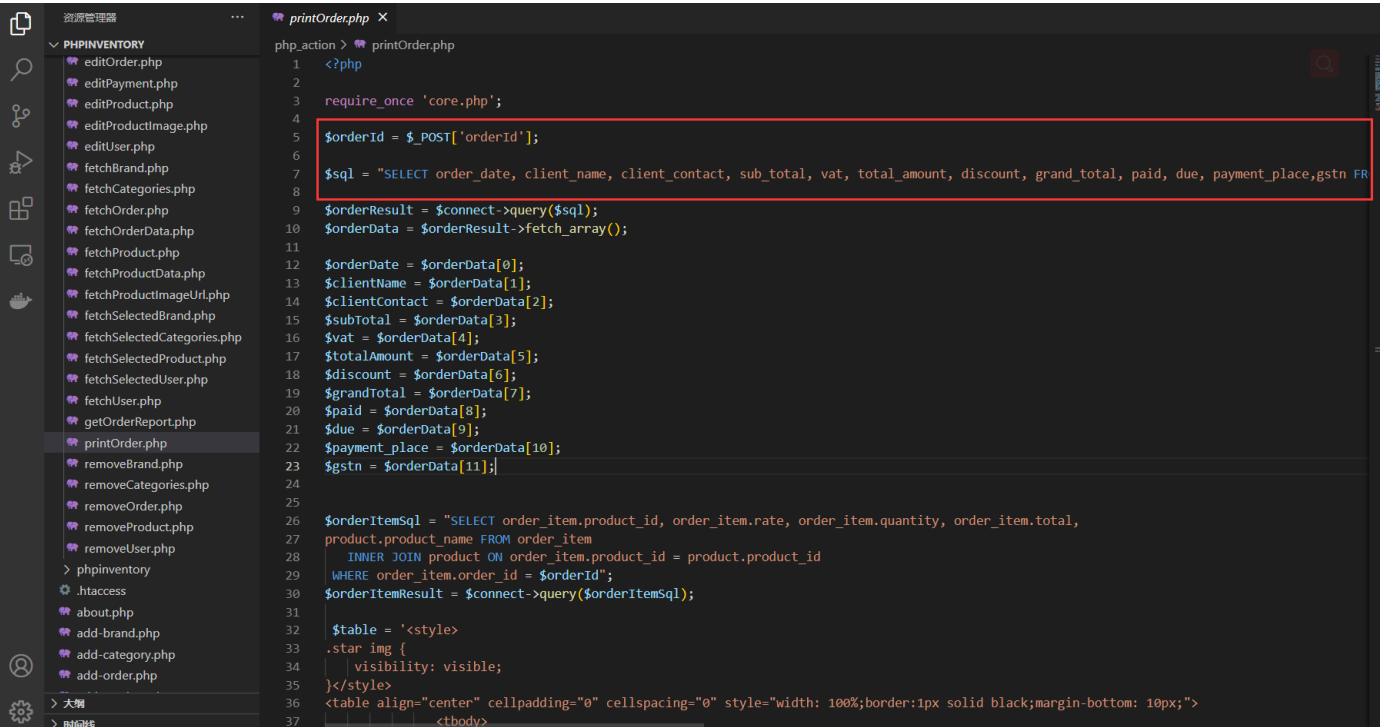
9 lines (6 sloc) 437 Bytes

vendor: <https://www.sourcecodester.com/>

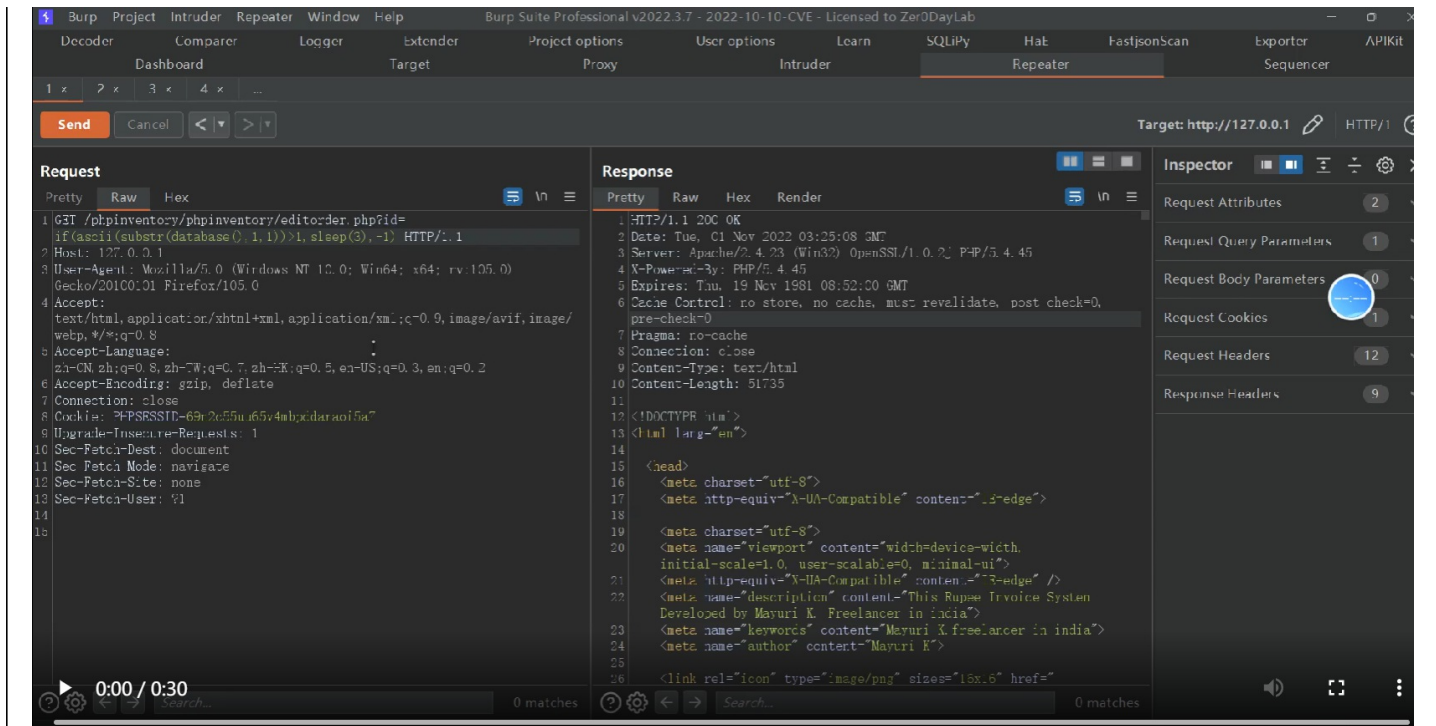
download link: <https://www.sourcecodester.com/php/14831/billing-system-project-php-source-code-free-download.html>

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 $sql = "SELECT order_date, client_name, client_contact, sub_total, vat, total_amount, discount, grand_total, paid, due, payment_place,gstn FR
8
9 $orderResult = $connect->query($sql);
10 $orderData = $orderResult->fetch_array();
11
12 $orderDate = $orderData[0];
13 $clientName = $orderData[1];
14 $clientContact = $orderData[2];
15 $subTotal = $orderData[3];
16 $vat = $orderData[4];
17 $totalAmount = $orderData[5];
18 $discount = $orderData[6];
19 $grandTotal = $orderData[7];
20 $paid = $orderData[8];
21 $due = $orderData[9];
22 $payment_place = $orderData[10];
23 $gstn = $orderData[11];
24
25
26 $orderItemSql = "SELECT order_item.product_id, order_item.rate, order_item.quantity, order_item.total,
27 product.product_name FROM order_item
28 INNER JOIN product ON order_item.product_id = product.product_id
29 WHERE order_item.order_id = $orderId";
30 $orderItemResult = $connect->query($orderItemSql);
31
32 $table = '<style>
33 .star img {
34     visibility: visible;
35 }</style>
36 <table align="center" cellpadding="0" cellspacing="0" style="width: 100%;border:1px solid black;margin-bottom: 10px;">
37 <tbody>
```



© 2022 GitHub, Inc.

- [Terms](#)
- [Privacy](#)
- [Security](#)
- [Status](#)
- [Docs](#)
- [Contact GitHub](#)
- [Pricing](#)
- [API](#)
- [Training](#)
- [Blog](#)
- [About](#)