

main

...

## CVE / Billing System Project v1.0 / CVE-2022-43213(sql in editororder.php).md

Qratty Update CVE-2022-43213(sql in editororder.php).md

History

1 contributor

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:

The screenshot displays the code editor for the file `editororder.php`. The code is a PHP script that handles the editing of an order. It includes a database connection, a query to fetch order details based on the `$orderId` parameter, and a form to update the order. The code is as follows:

```
68 <?php
69 // PHP, CodeIgnitor or Laravel work visit www.mayurix.com ->
70
71
72 <div class="row">
73 <div class="col-lg-8" style=" margin-left: 10%;>
74 <div class="card">
75 <div class="card-title">
76
77 </div>
78 <div id="add-brand-messages"></div>
79 <div class="card-body">
80 <div class="input-states">
81 <form class="form-horizontal" method="POST" action="php_action/editororder.php" id="editOrderform">
82
83 <?php $orderId = $_GET['id'];
84
85 $sql = "SELECT orders.order_id, orders.order_date, orders.client_name, orders.client_contact, orders.sub_total, orders.vat, orders.total as
86 WHERE orders.order_id = ($orderId)";
87
88 $result = $connect->query($sql);
89 $data = $result->fetch_row();
90 echo 1;
91 </div>
92
93 <div class="form-group">
94 <div class="row">
95 <label class="col-sm-3 control-label">Order Date</label>
96 <div class="col-sm-9">
97 <input type="text" class="form-control" id="orderDate" name="orderDate" autocomplete="off" value="<?php echo $data[1] ?>" />
98 </div>
99 </div>
100 </div>
101 <div class="form-group">
102 <div class="row">
103 <label class="col-sm-3 control-label">Client Name</label>
104 <div class="col-sm-9">
```

The second screenshot shows the response of a GET request to the `editororder.php` endpoint. The response is an HTML document with a status of 200 OK. The response body contains the following HTML structure:

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <meta charset="utf-8">
5 <meta http-equiv="X-UA-Compatible" content="IE=edge">
6 <meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=0">
7 <meta http-equiv="X-UA-Compatible" content="IE=edge" />
8 <meta name="description" content="This is a Billing System Developed by Mayuri K. Freelancer in India">
9 <meta name="keywords" content="Mayuri K Freelancer in India">
10 <meta name="author" content="Mayuri K">
11 </head>
12 <body>
13 <div class="row">
14 <div class="col-lg-8" style=" margin-left: 10%;>
15 <div class="card">
16 <div class="card-title">
17
18 </div>
19 <div id="add-brand-messages"></div>
20 <div class="card-body">
21 <div class="input-states">
22 <form class="form-horizontal" method="POST" action="php_action/editororder.php" id="editOrderform">
23
24 <?php $orderId = $_GET['id'];
25
26 $sql = "SELECT orders.order_id, orders.order_date, orders.client_name, orders.client_contact, orders.sub_total, orders.vat, orders.total as
```