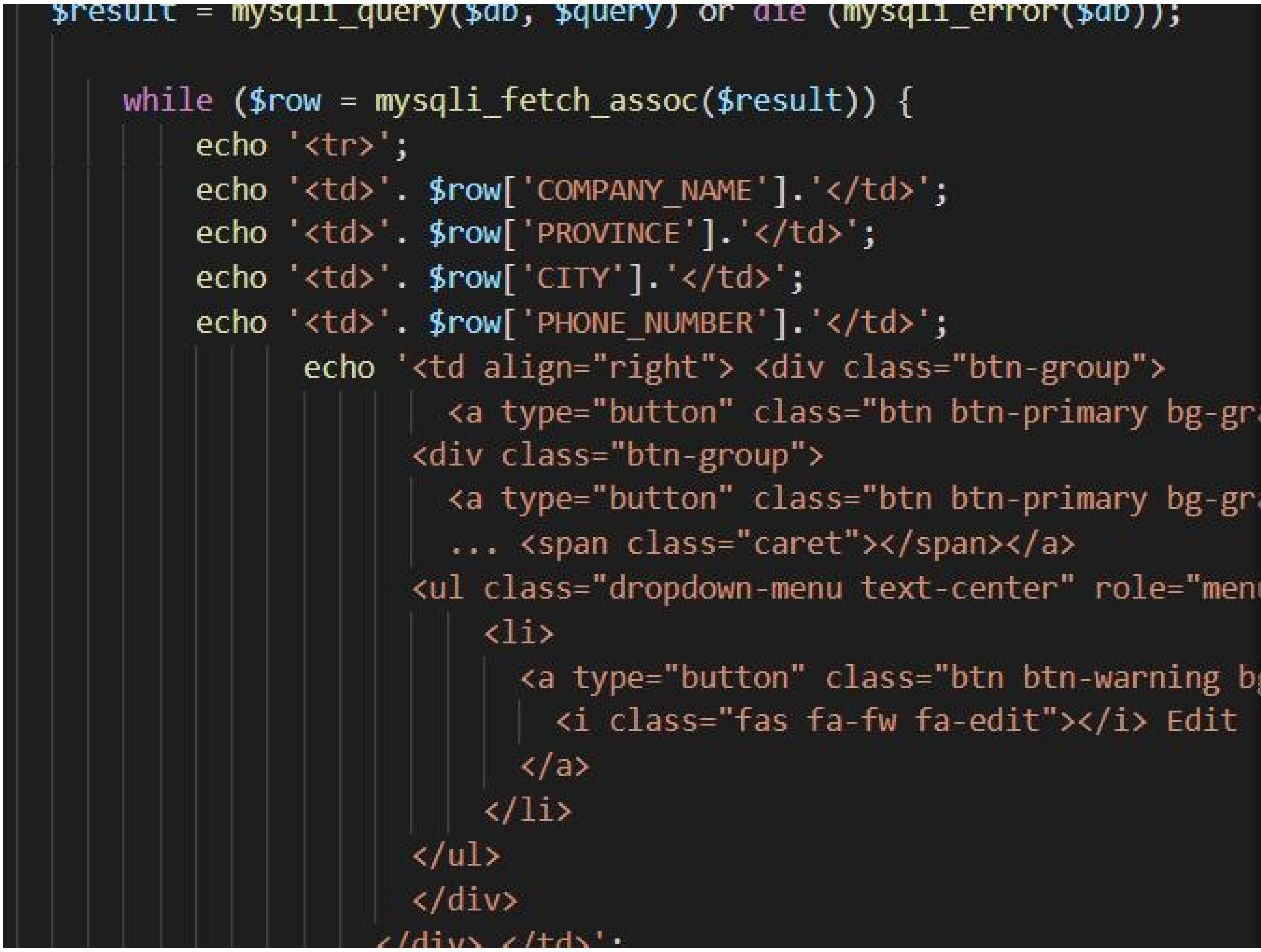
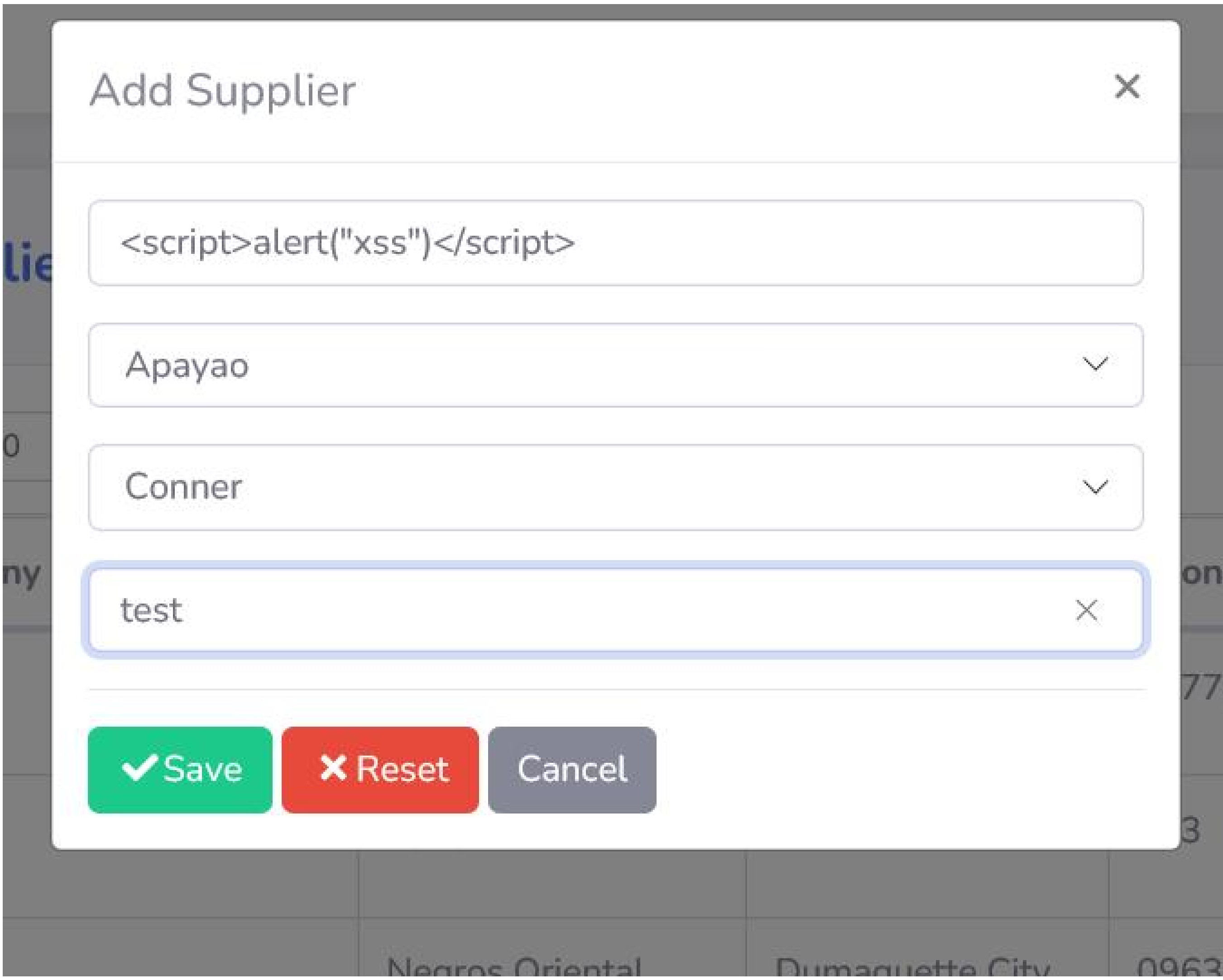
The Cross-Site Scriptin vulnerability exists in the supplier file of the computer parts sales and inventory system system, which is caused by the insufficient filtering of user input by the Web application. Attackers take advantage of website vulnerabilities to inject malicious script code (usually including HTML code and client-side Javascript script) into web pages. When other users browse these pages, the malicious code will be executed, and the victim may take Cookie data theft, session hijacking, phishing, and other attacks.

复现过程



```
  $result = mysqli_query($db, $query) or die (mysqli_error($db));

    while ($row = mysqli_fetch_assoc($result)) {
        echo '<tr>';
        echo '<td>'. $row['COMPANY_NAME'].'</td>';
        echo '<td>'. $row['PROVINCE'].'</td>';
        echo '<td>'. $row['CITY'].'</td>';
        echo '<td>'. $row['PHONE_NUMBER'].'</td>';
              echo '<td align="right"> <div class="btn-group">
                      <a type="button" class="btn btn-primary bg-gr
                    <div class="btn-group">
                      <a type="button" class="btn btn-primary bg-gr
                      ... <span class="caret"></span></a>
                    <ul class="dropdown-menu text-center" role="menu
                        <li>
                          <a type="button" class="btn btn-warning b
                            <i class="fas fa-fw fa-edit"></i> Edit
                          </a>
                        </li>
                    </ul>
                    </div>
                  </div> </td>';
```



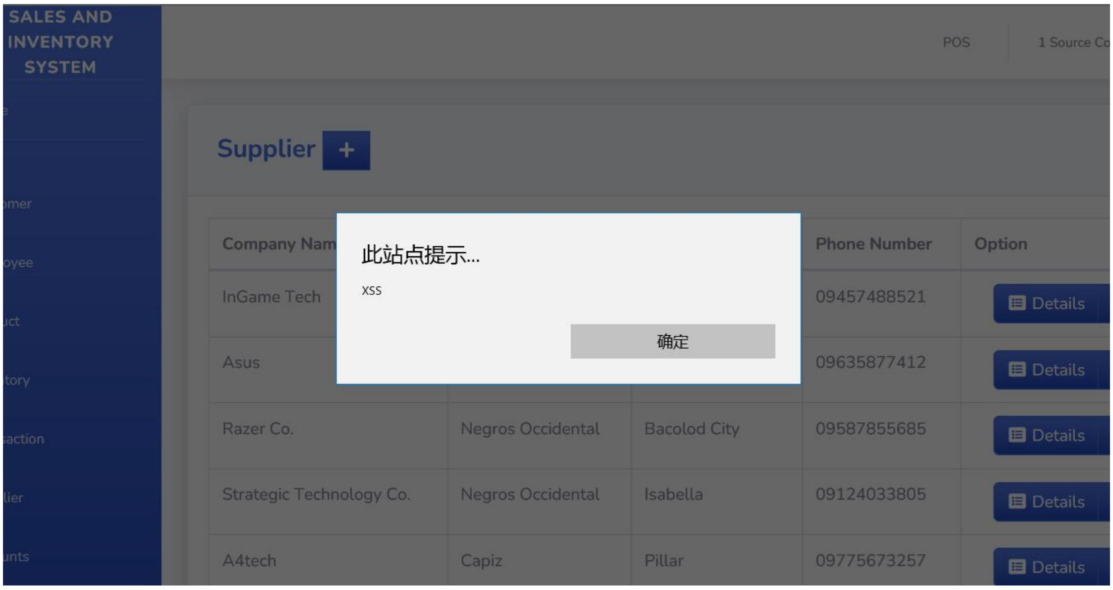
Add Supplier

<script>alert("xss")</script>

Apayao

Conner

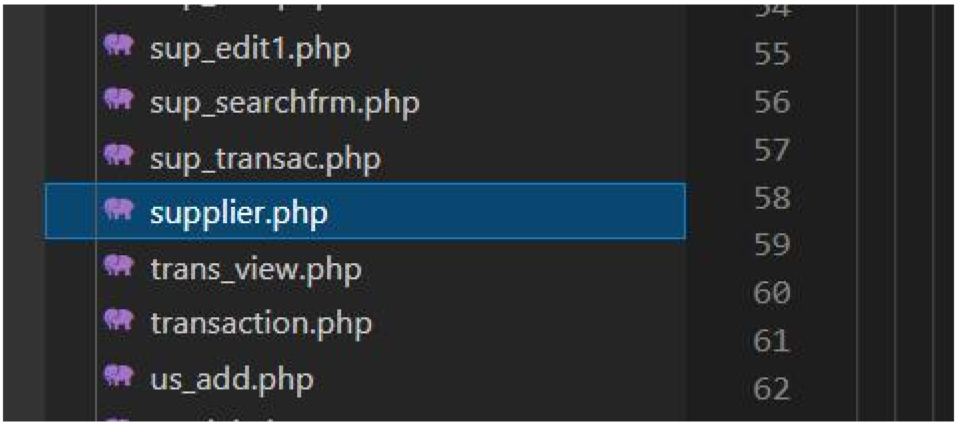
test



此站点提示...

xss

Company Nam			Phone Number	Option
InGame Tech			09457488521	Details
Asus			09635877412	Details
Razer Co.	Negros Occidental	Bacolod City	09587855685	Details
Strategic Technology Co.	Negros Occidental	Isabella	09124033805	Details
A4tech	Capiz	Pillar	09775673257	Details



sup_edit1.php
sup_searchfrm.php
sup_transac.php
supplier.php
trans_view.php
transaction.php
us_add.php