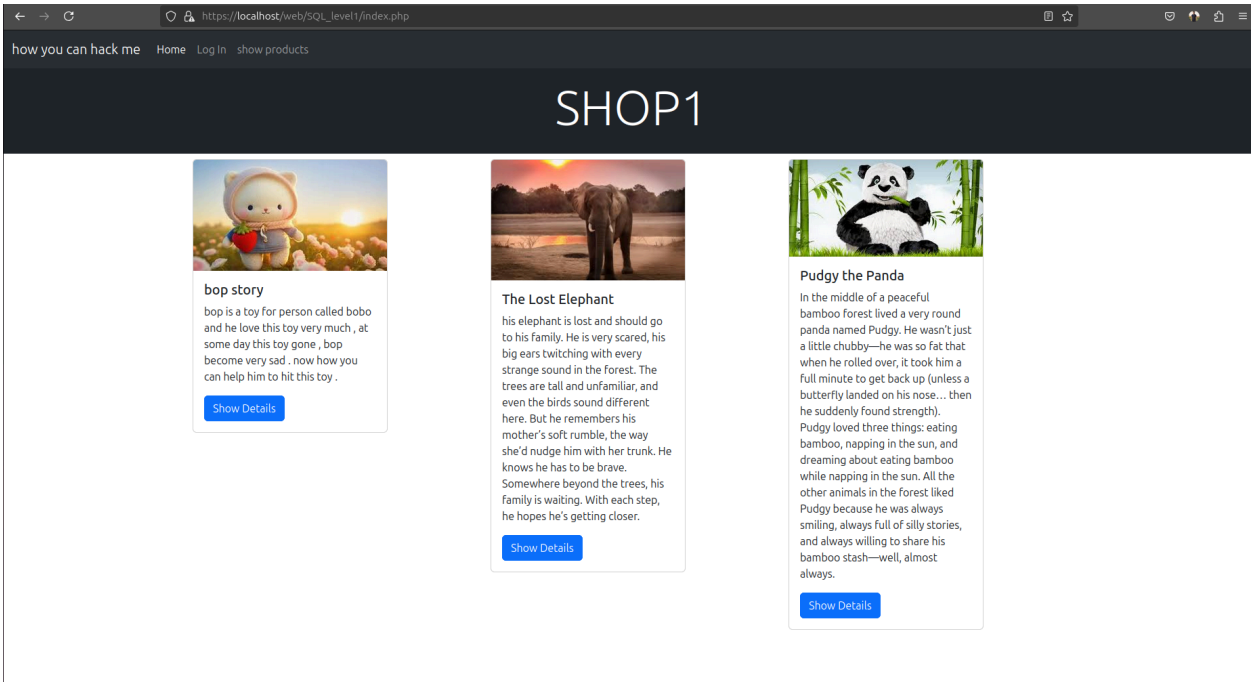
SQL_LEVEL3

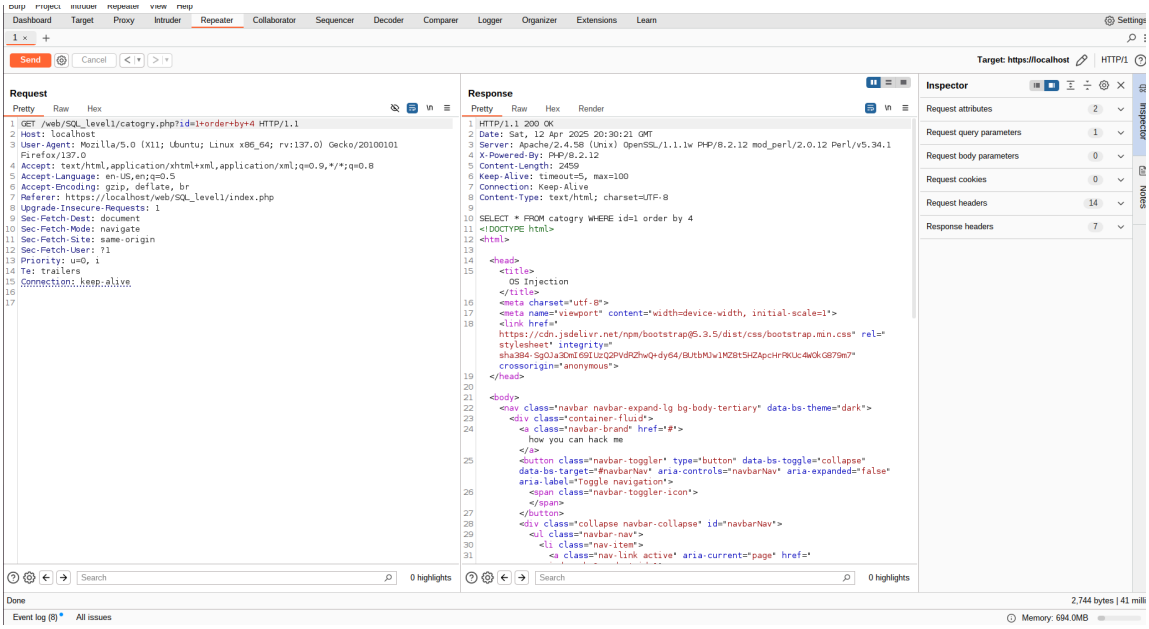
lets add new idea in our program, i want you log in without now any information .

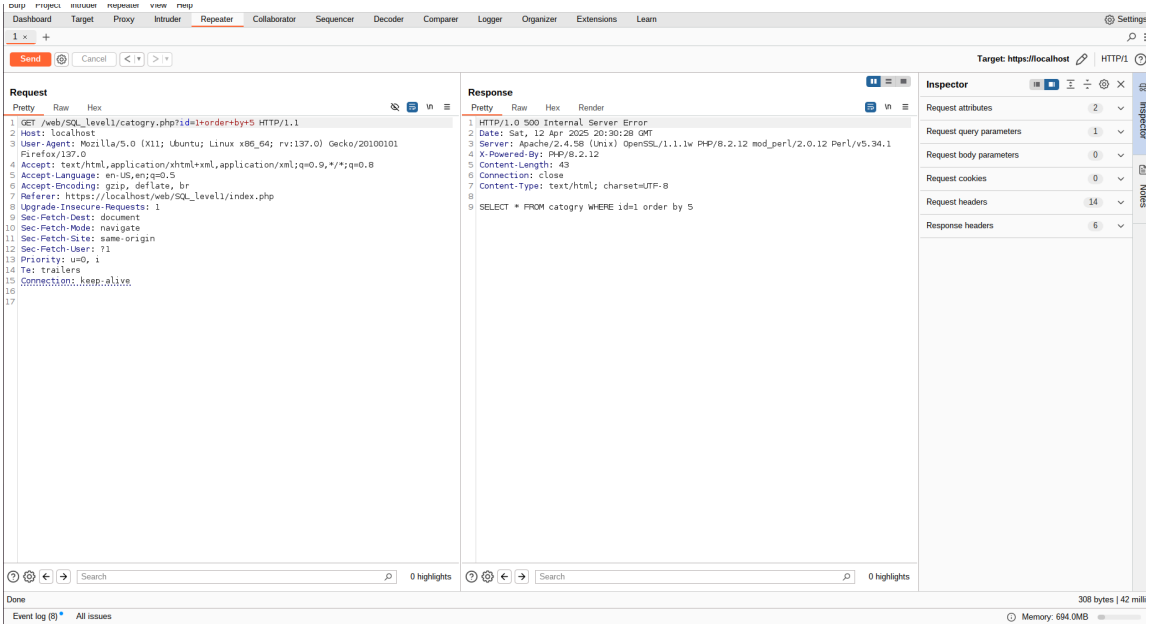


▼ use sample payload using Burp Suite

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

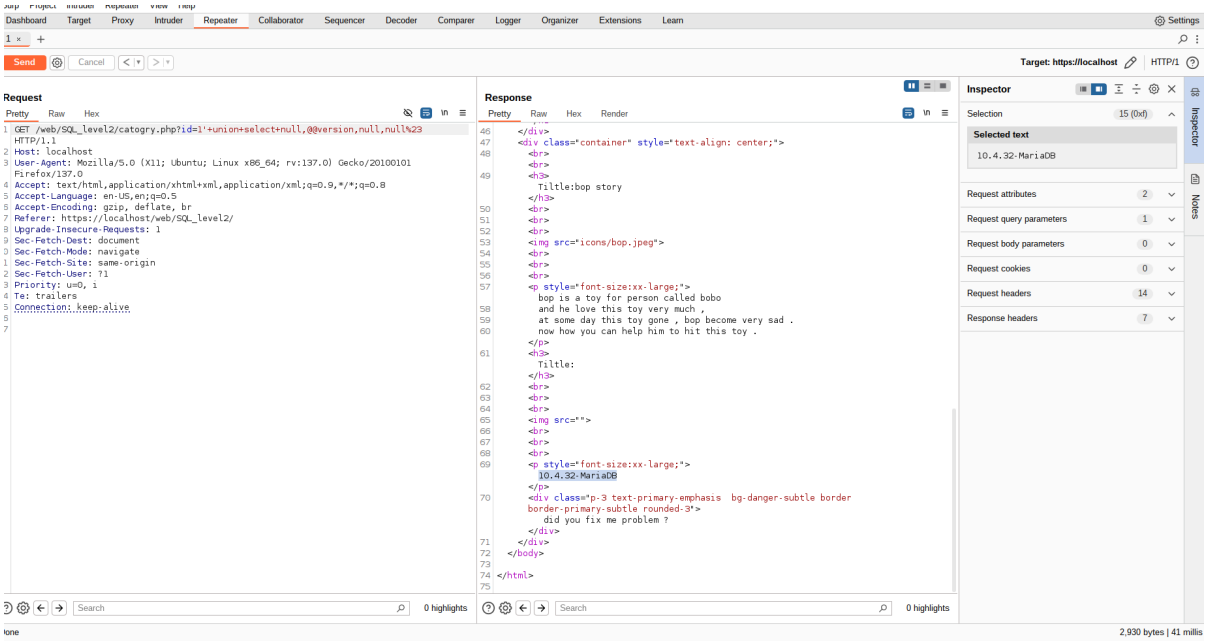
  you still increment the number of the [order by 2] until error happen then you should know now the number of columns in the table of database .





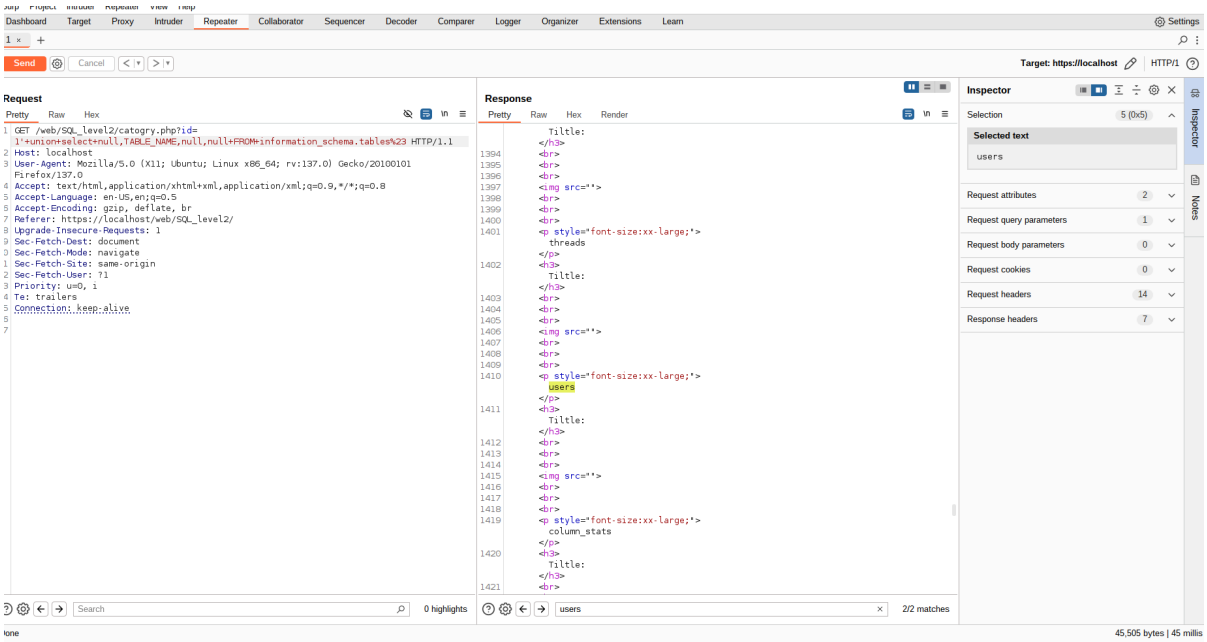
- so the number here is 4
    - now lets use our payload

- UNION ⇒ to know the database type .

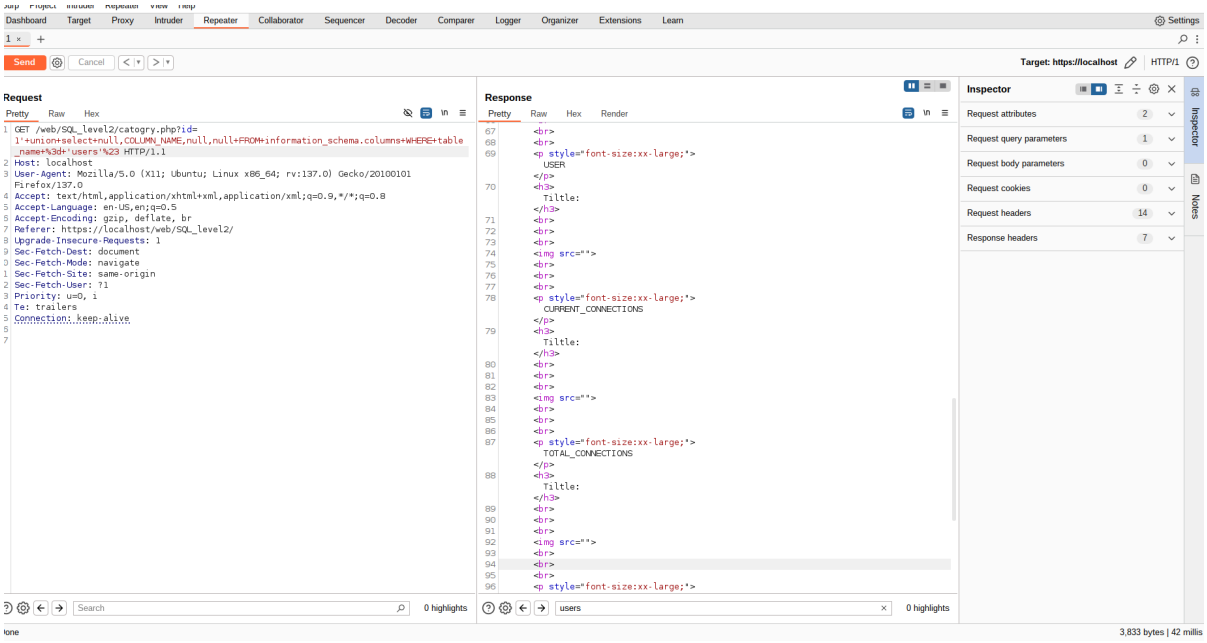


now we know that the data base type is mysql

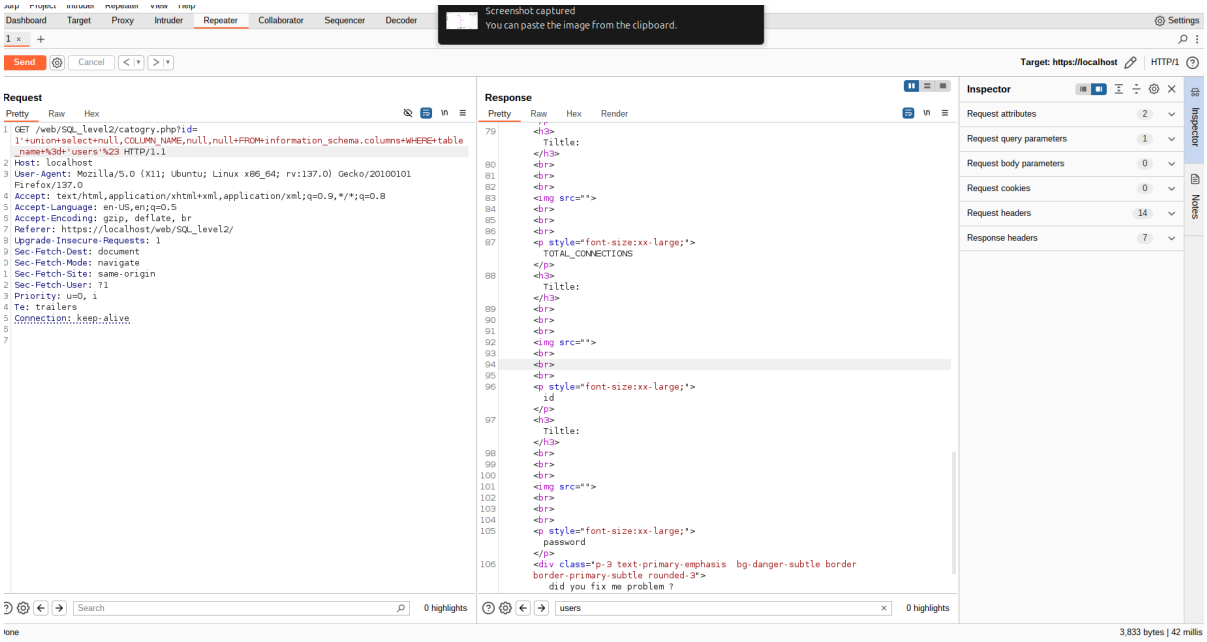
-lets know the tables name and columns name



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

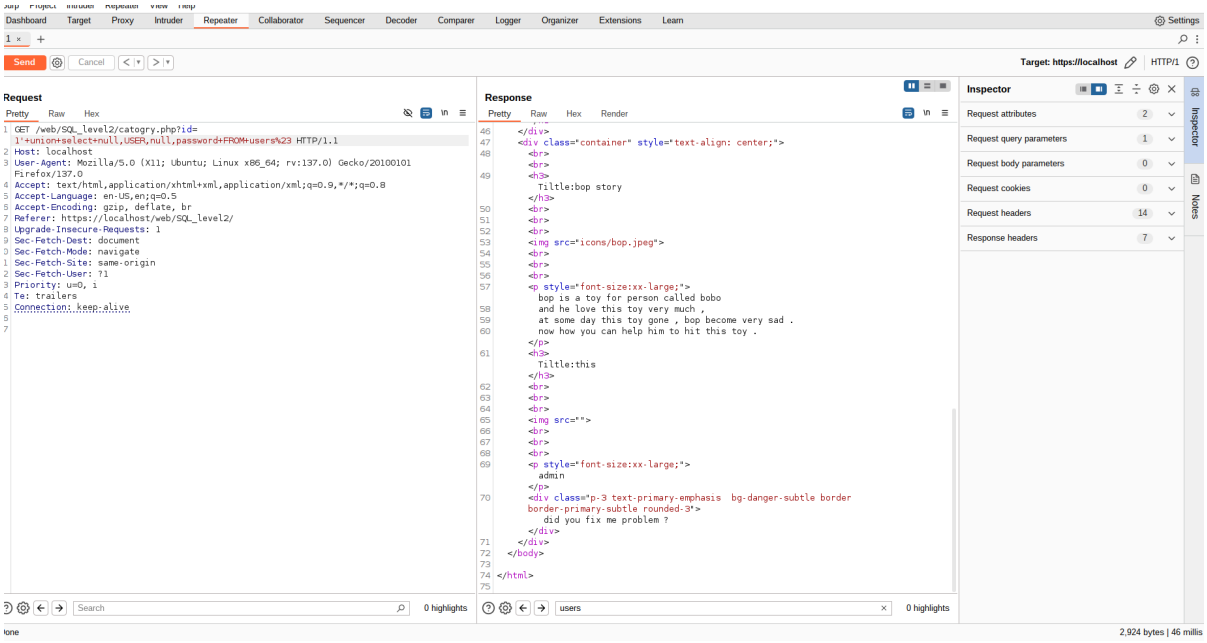


USER is the first column in the table

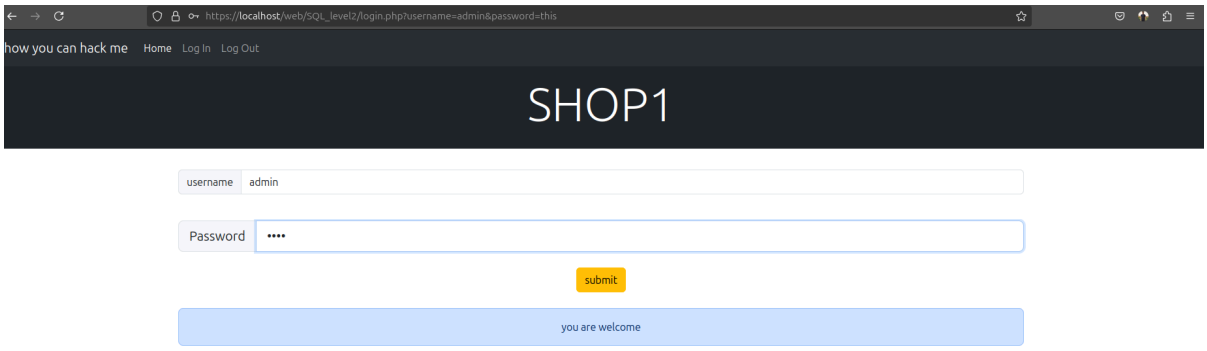


password is the second column in the table

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

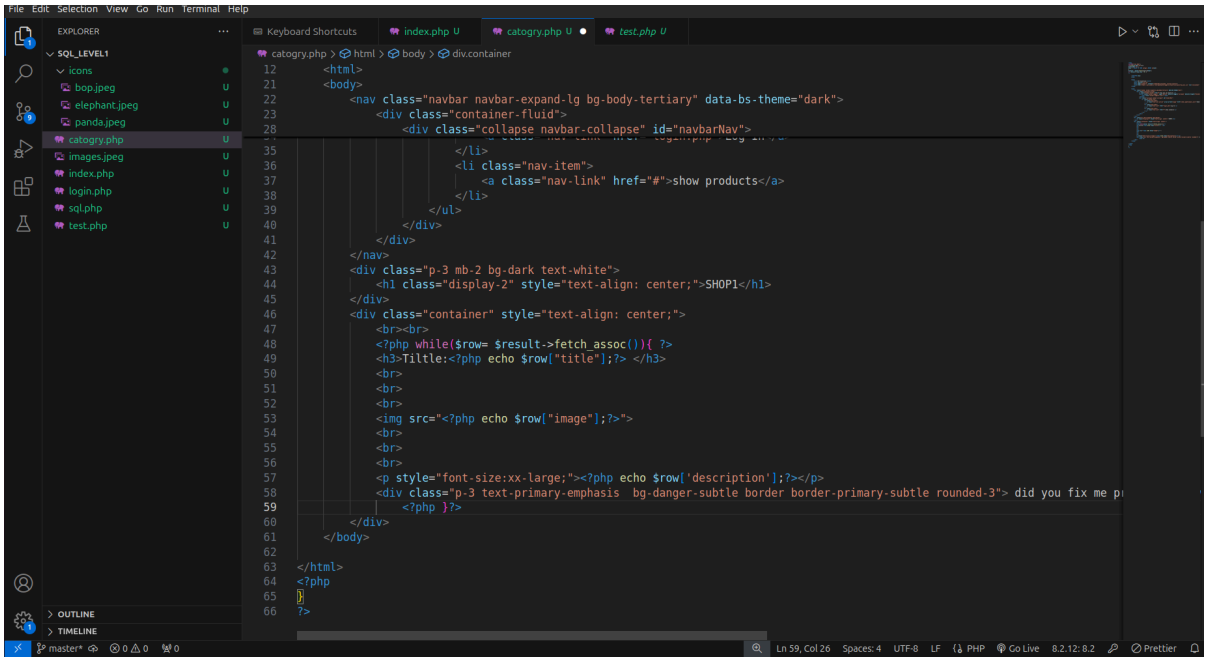


know we sea [this admin] lets try it in log in page



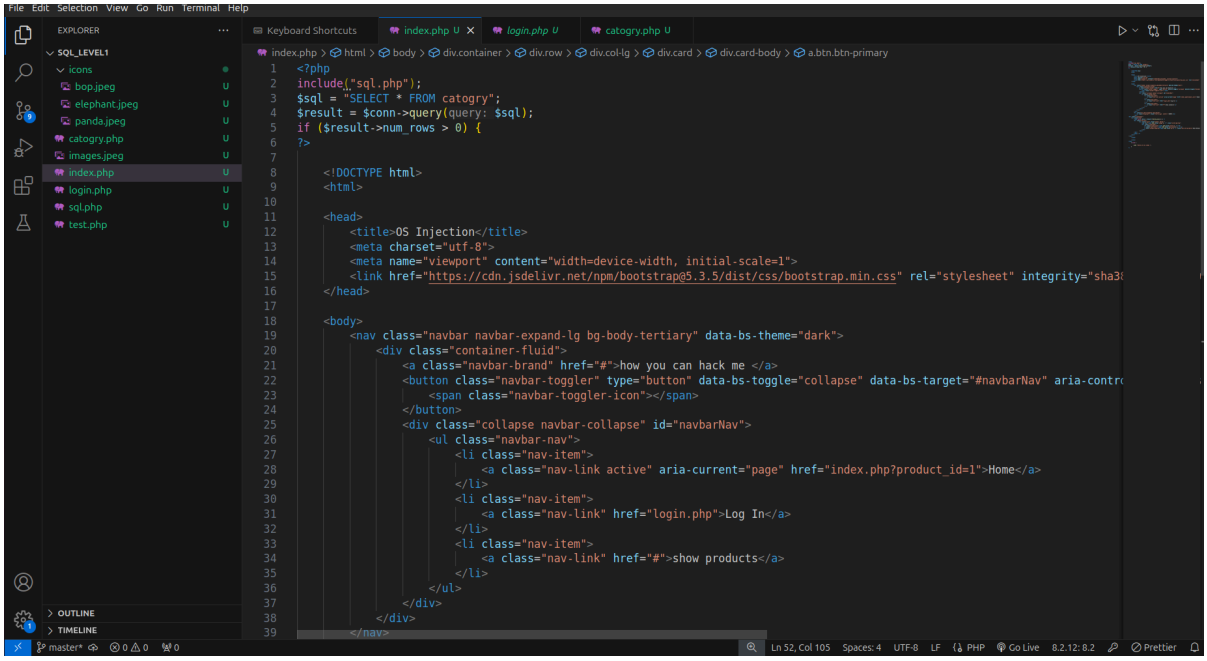
▼ stop payload by sample function

-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 .

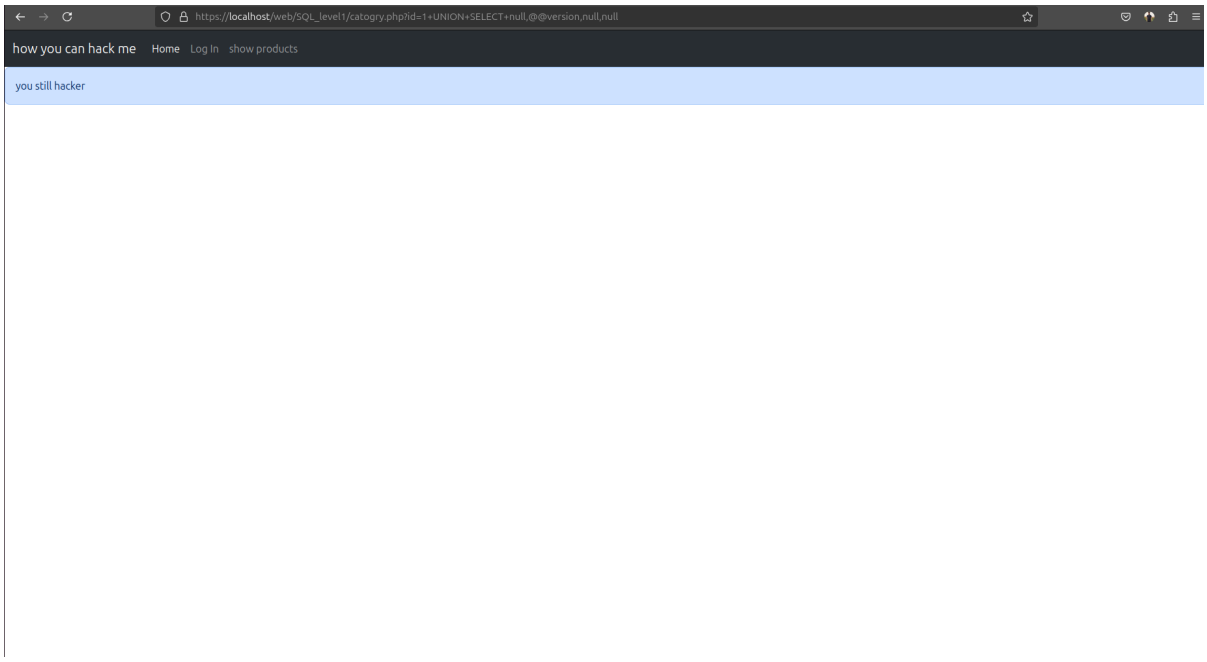
-i can make it show only the first row by that ⇒



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.