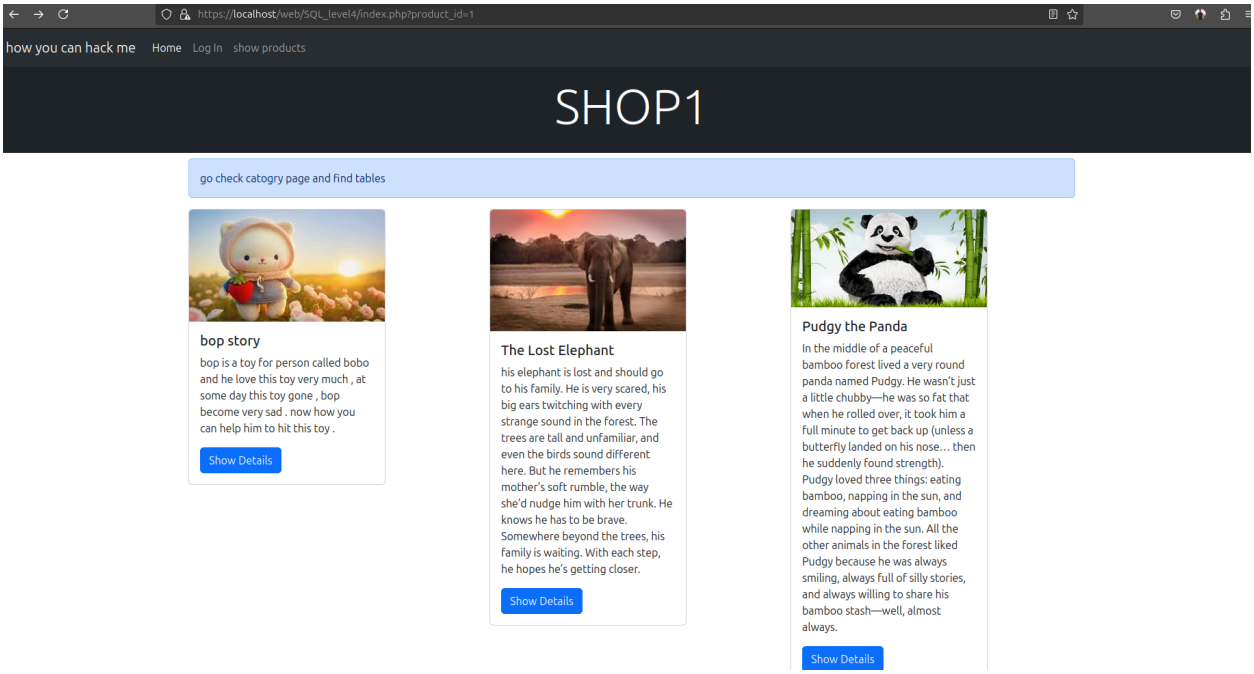
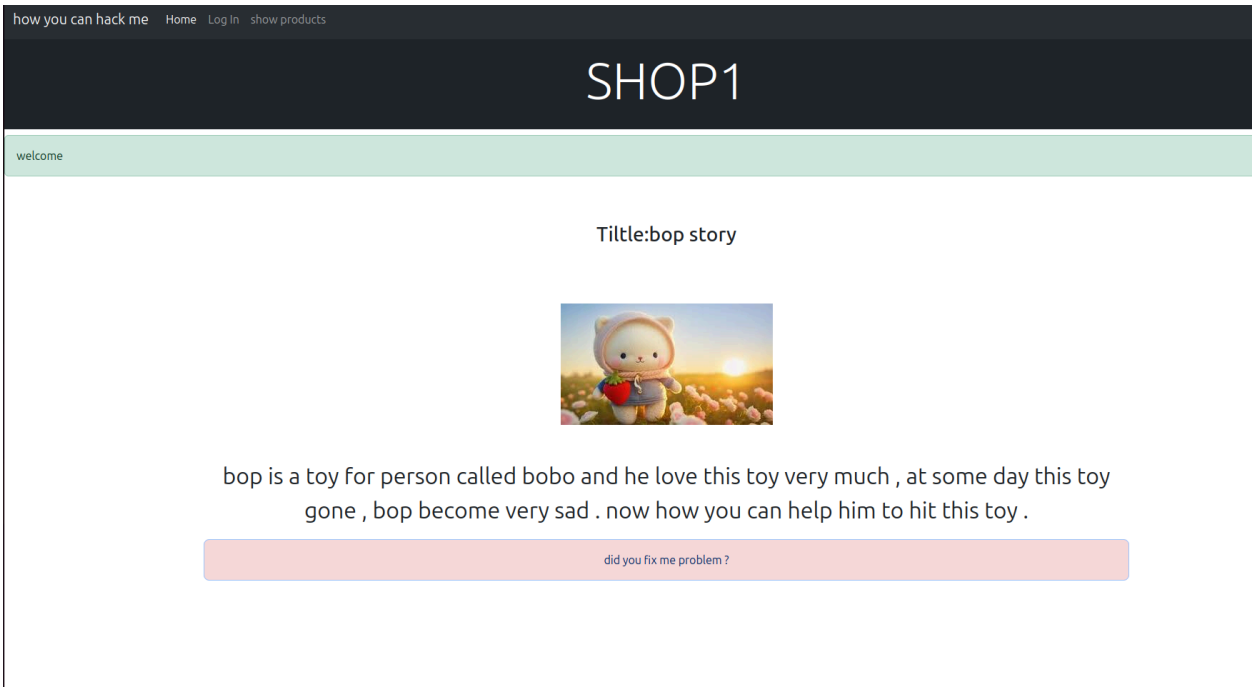
SQL_LEVEL5

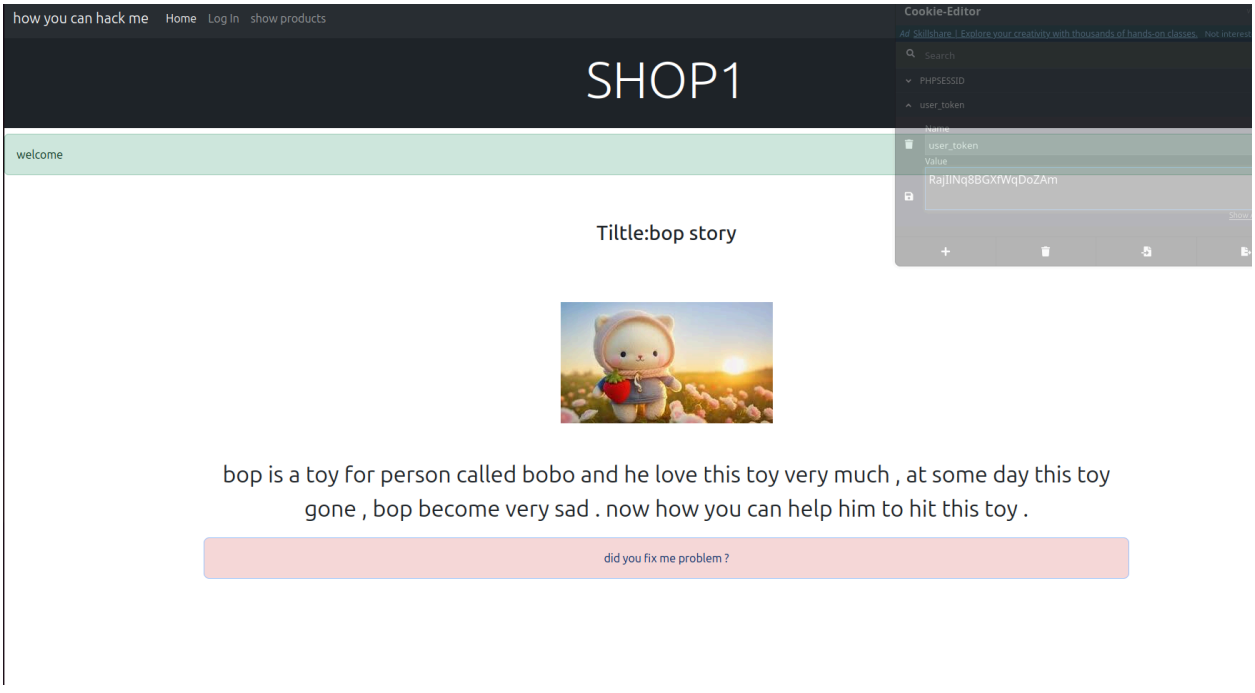
lets add new idea in our program, now the user git a token ⇒ message is appear:

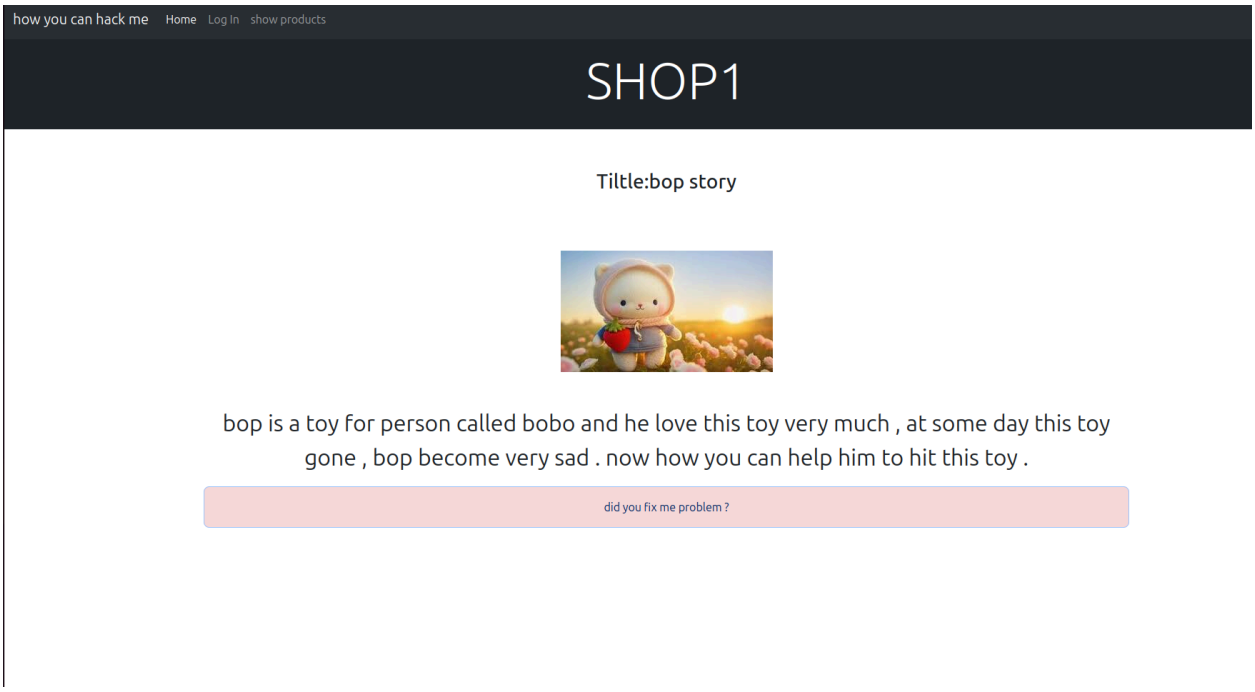
- use table users and columns is user [admin]& password ⇒ to git user password





we sea welcome message ⇒ lets change the token value



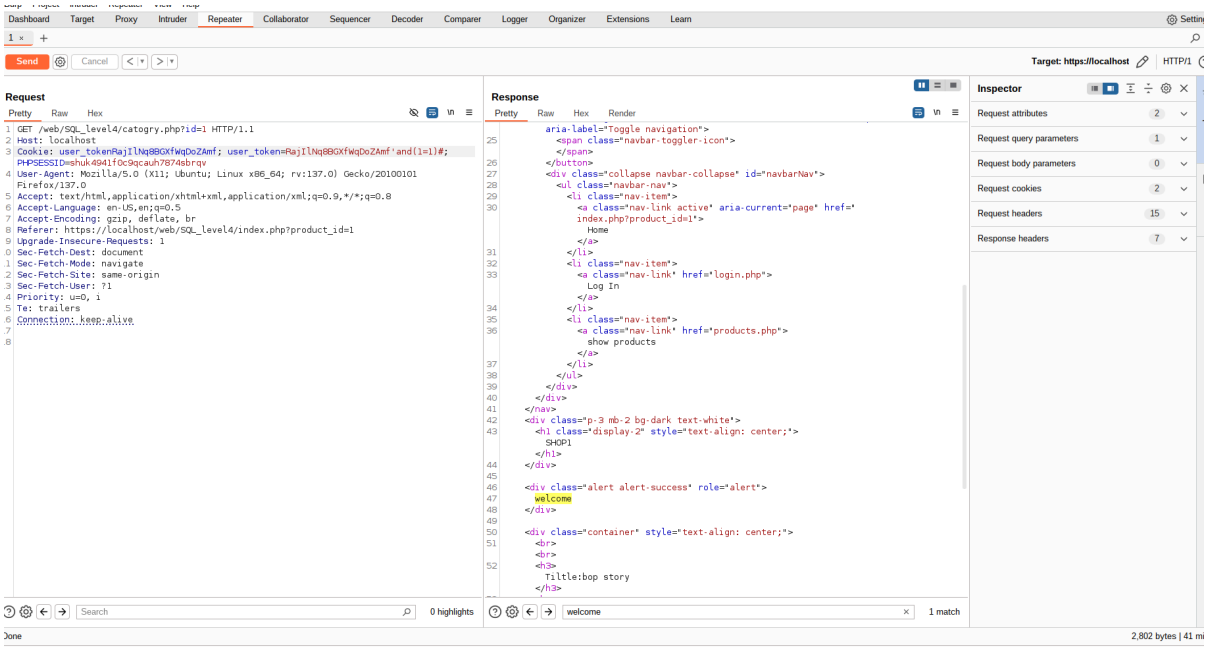


the message after change is disappear

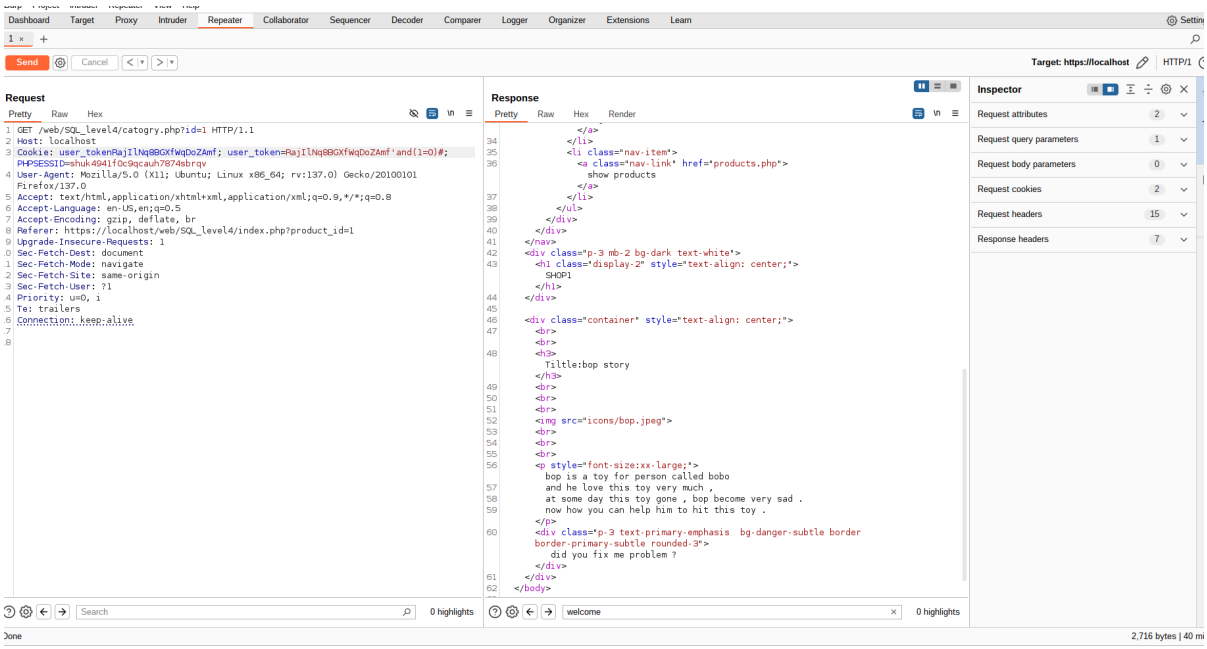
⇒now let’s use payloads to work with it .

▼ use sample payload using Burp Suite

i user first payload and 1=1 ⇒ this return true and i check the welcome is found in response or not .

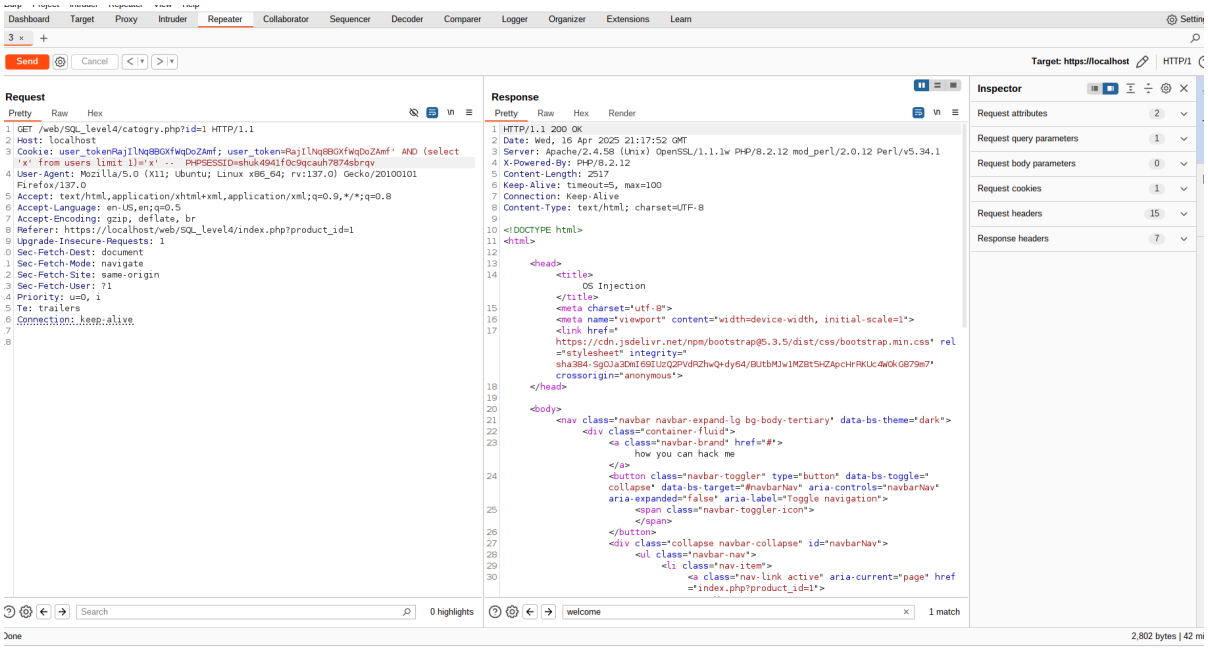


lets make and 1=0 ⇒ false , the token false should return no thing =

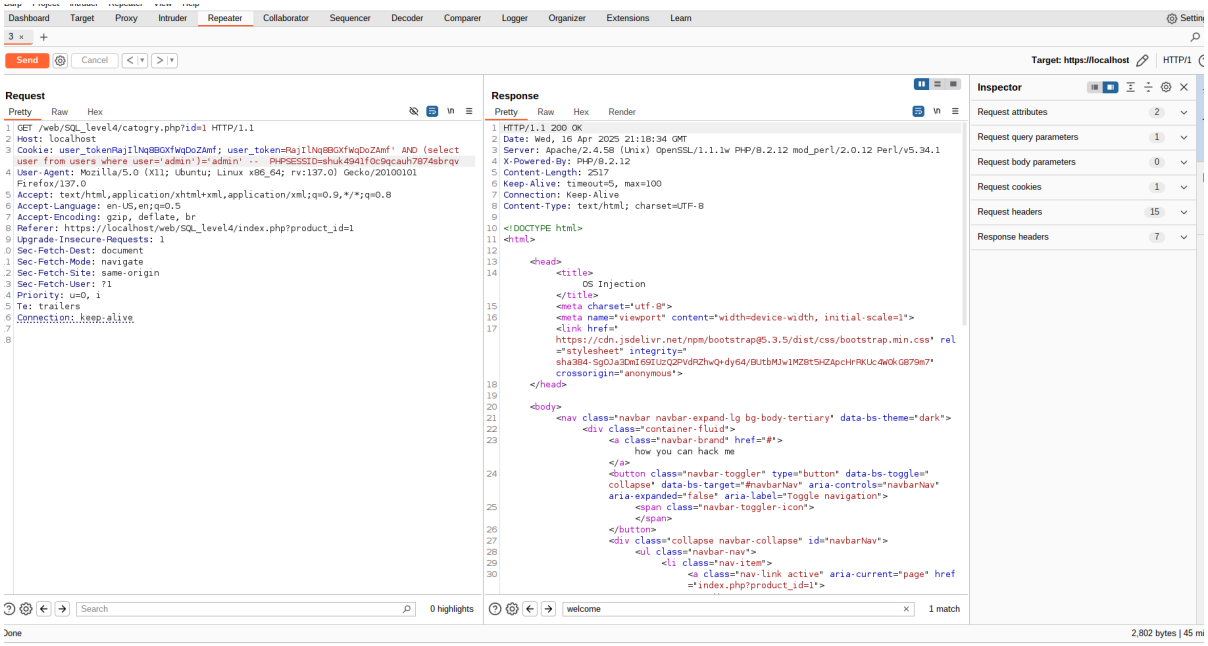


lets use payloads to git user password

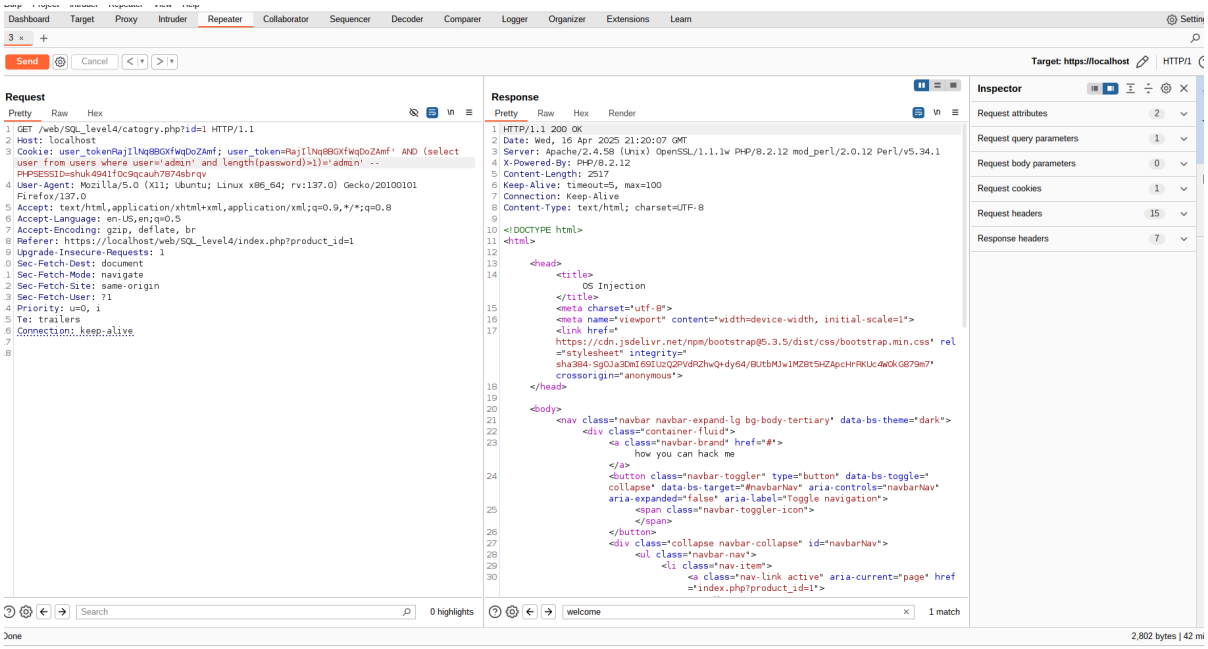
- first payload i use for check if table exist or not [limit 1]⇒ to git first row in data base only and to avoid error



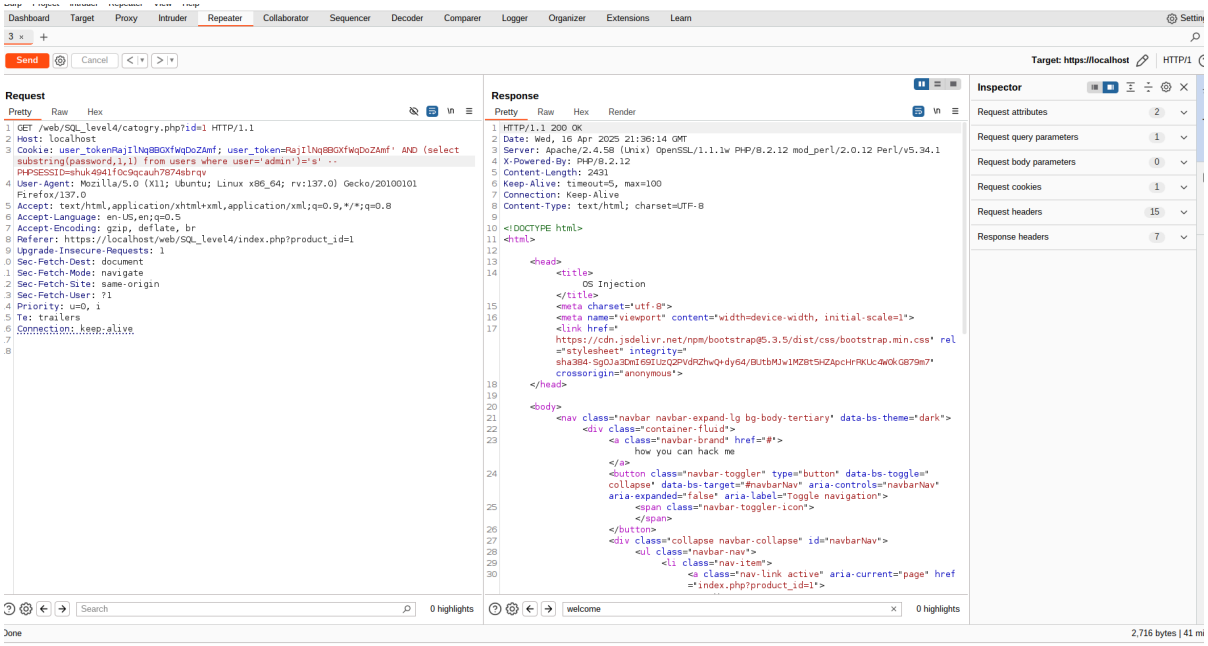
- lets test if user ='admin' exist or not , (select..)⇒return 'admin' so i make 'admin'='admin'⇒true



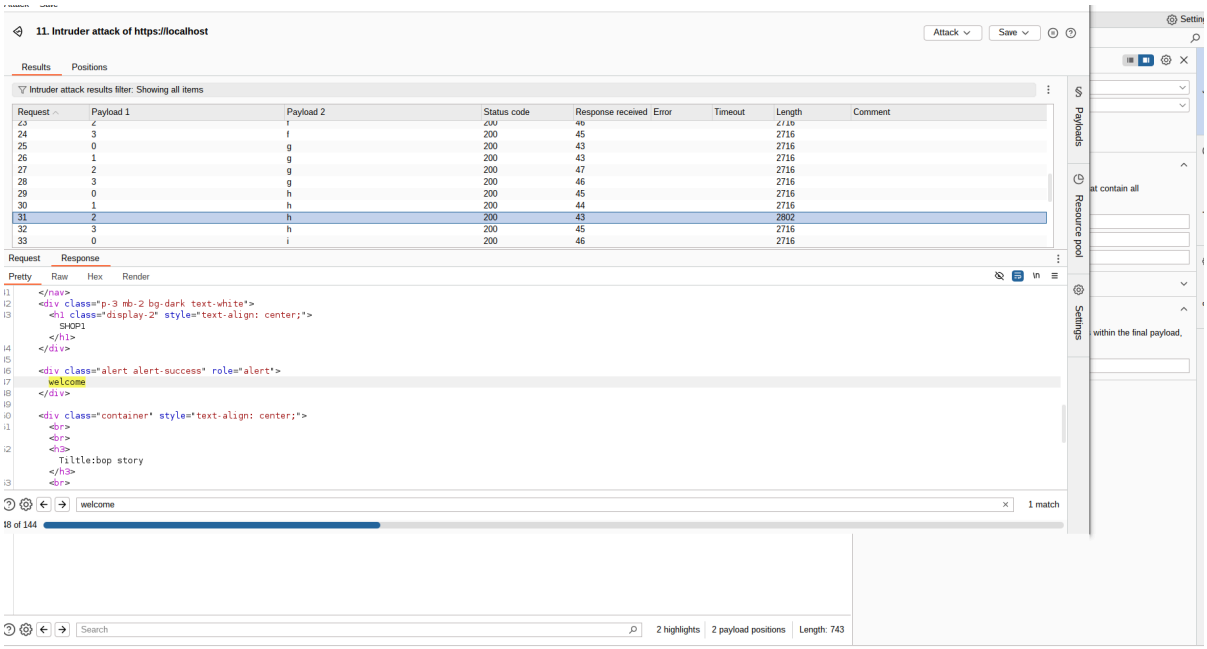
- i determine here the password length



- let’s use substring(password,position,step)⇒ to git the character one by one and compare it with character i put it .



- now we should intruder to make multi request

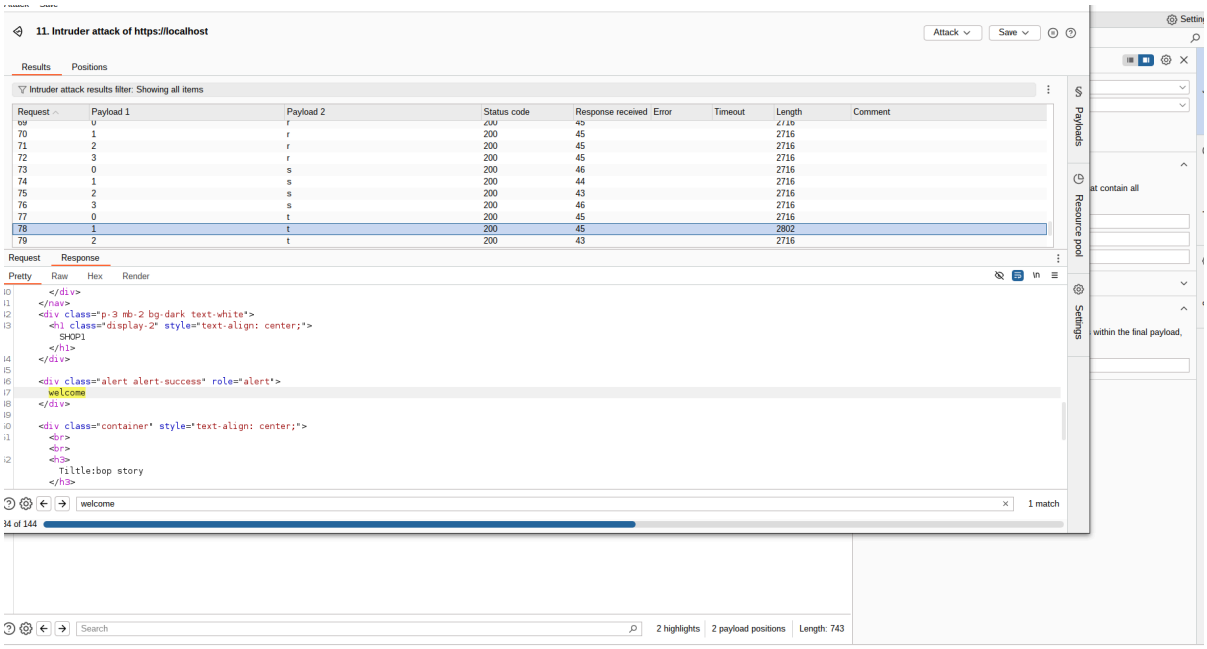

11. Intruder attack of https://localhost
Attack
Save
Results
Positions
Intruder attack results filter: Showing all items
Request
Payload 1
Payload 2
Status code
Response received
Error
Timeout
Length
Comment
24 3 f 200 45 2716
25 0 g 200 43 2716
26 1 g 200 43 2716
27 2 g 200 47 2716
28 3 g 200 46 2716
29 0 h 200 45 2716
30 1 h 200 44 2716
31 2 h 200 43 2802
32 3 h 200 45 2716
33 0 i 200 46 2716
Request
Response
Pretty
Raw
Hex
Render
</nav>

<h1 class="display-2" style="text-align: center;">
SHOP1
</h1>

welcome

<h3>
Tiltle:bop story
</h3>

welcome
1 match
18 of 144
Search
2 highlights
2 payload positions
Length: 743
Payloads
Resource pool
Settings

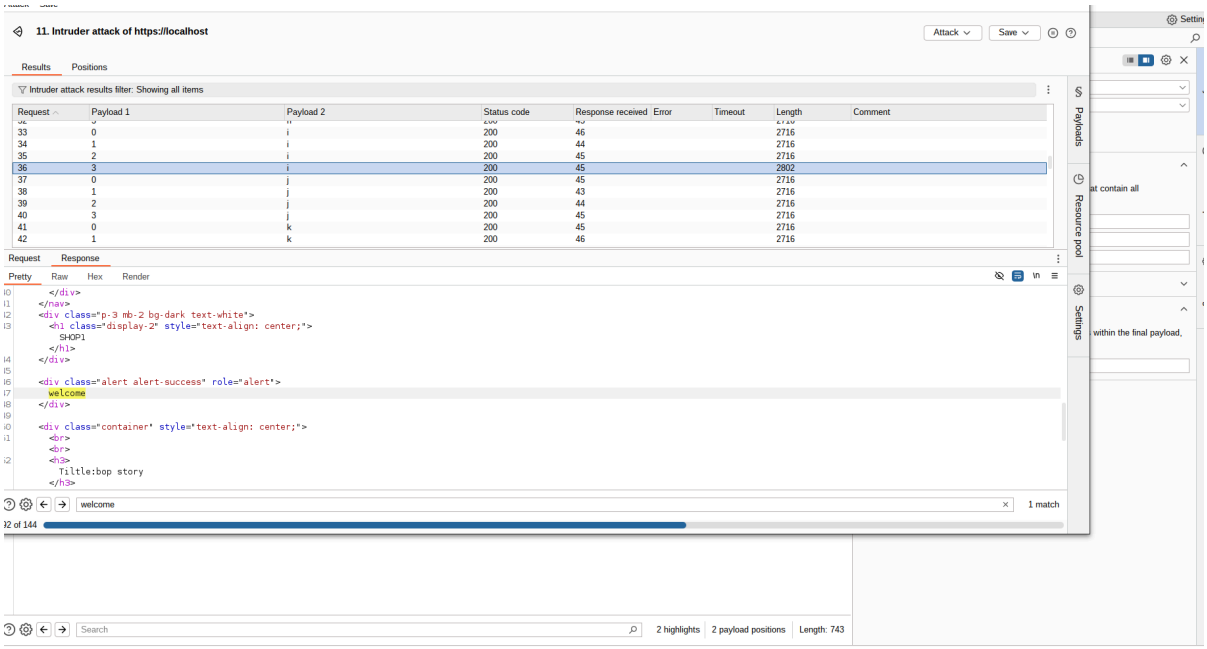

11. Intruder attack of https://localhost
Attack
Save
Results
Positions
Intruder attack results filter: Showing all items
Request
Payload 1
Payload 2
Status code
Response received
Error
Timeout
Length
Comment
70 1 r 200 45 2716
71 2 r 200 45 2716
72 3 r 200 45 2716
73 0 s 200 46 2716
74 1 s 200 44 2716
75 2 s 200 43 2716
76 3 s 200 46 2716
77 0 t 200 45 2716
78 1 t 200 45 2802
79 2 t 200 43 2716
Request
Response
Pretty
Raw
Hex
Render

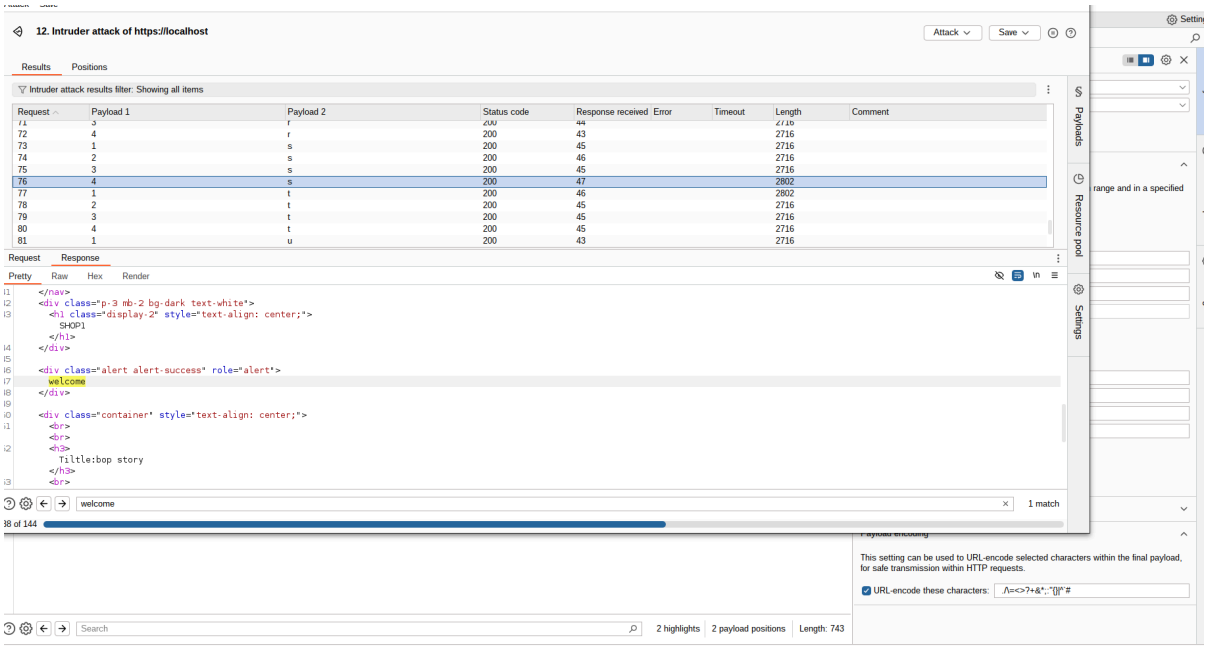
</nav>

<h1 class="display-2" style="text-align: center;">
SHOP1
</h1>

welcome

<h3>
Tiltle:bop story
</h3>
welcome
1 match
34 of 144
Search
2 highlights
2 payload positions
Length: 743
Payloads
Resource pool
Settings

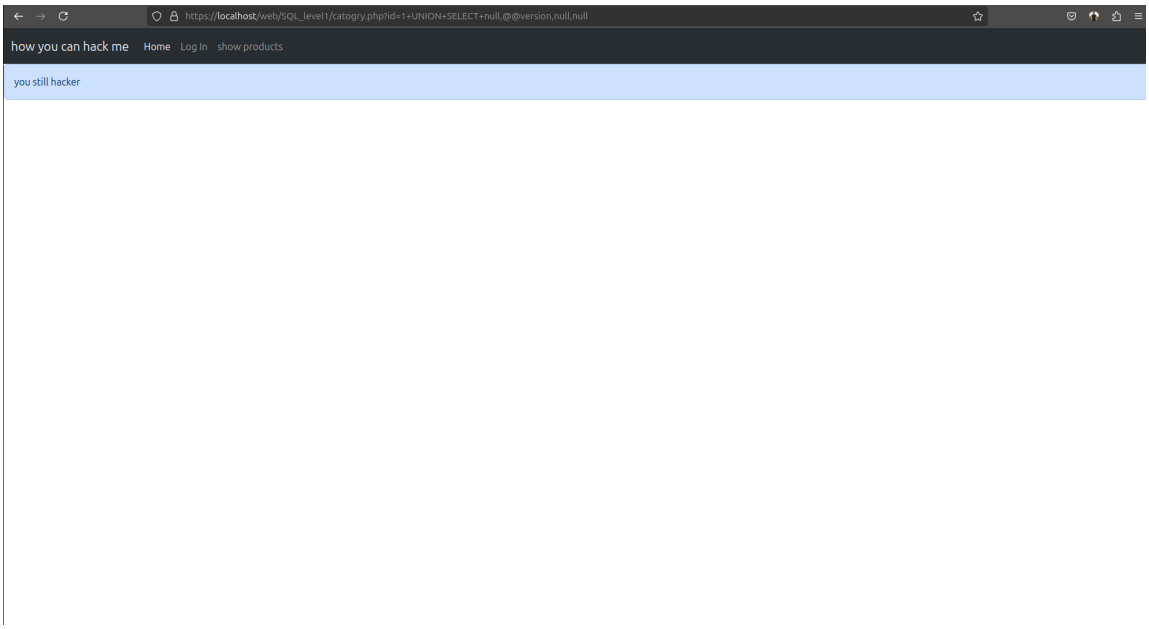




⇒ now we know the password is ‘this’

▼ stop payload by sample function

- 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_LEVEL6.