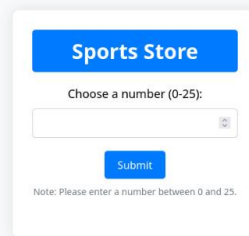


Challenge Name : Sp0rts_St0r3

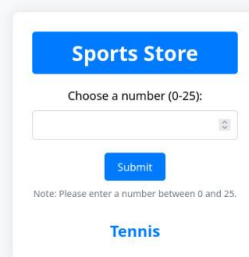
Author : Samarth & Siddharth

Solution :

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

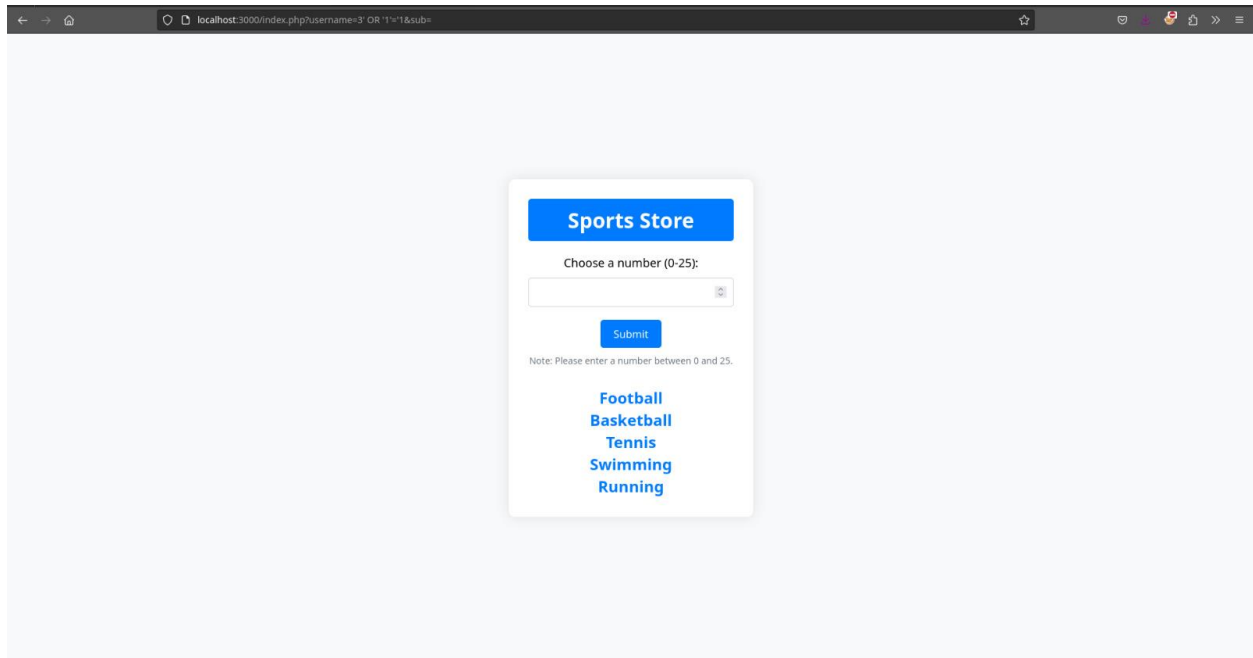


The screenshot shows a web application titled "Sports Store". Below the title, there is a prompt "Choose a number (0-25):" followed by a text input field. A "Submit" button is located below the input field. At the bottom of the form, a note reads: "Note: Please enter a number between 0 and 25."

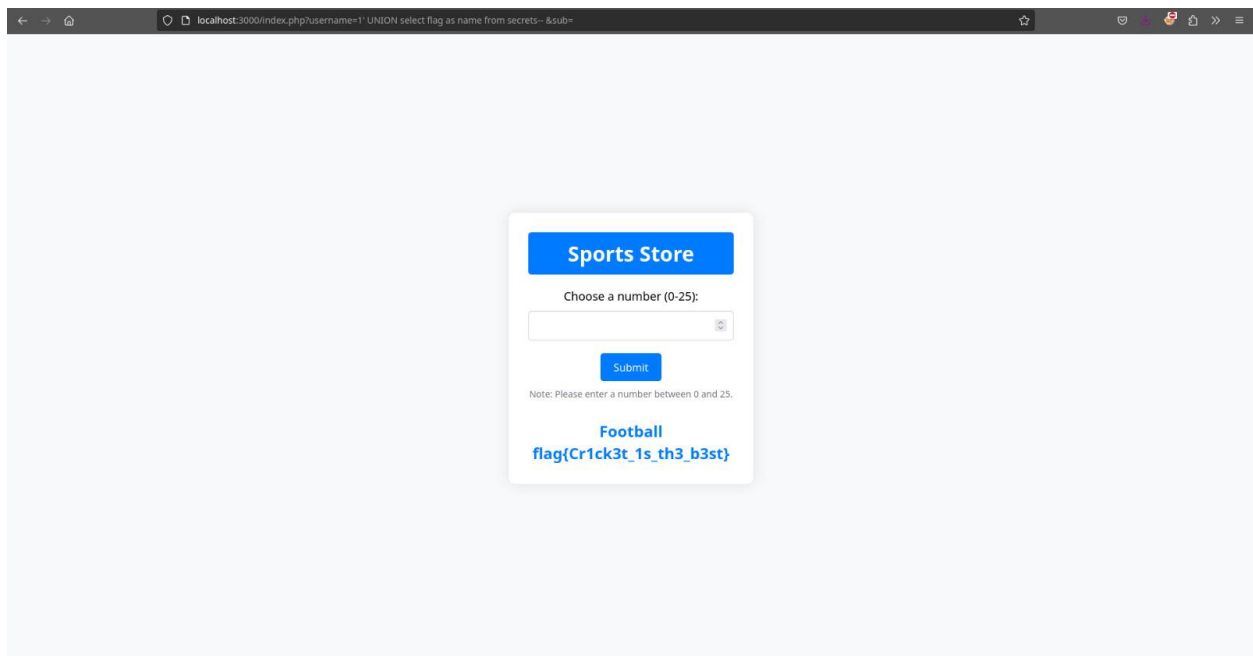


This screenshot shows the same "Sports Store" application after a successful SQLi attack. The input field now contains the payload "1' OR '1'='1". The "Submit" button is still present. Below the note, the word "Tennis" is displayed in blue text, indicating that the application has returned a result based on the injected payload.

We are now performing a simple sql injection



Payload : ' OR '1'='1



flag{Cr1ck3t_1s_th3_b3st}