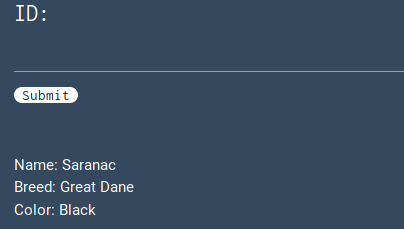
INJ3CTION TIME

I stumbled upon this website: http://web.ctflearn.com/web8/ and I think they have the flag in their somewhere. UNION might be a helpful command

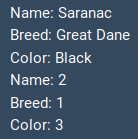
I must say this was a pretty hard challenge but basics of UNION command will solve it.



After opening the website it looked like this with an input box.

First I tried to find the number of id’s available by typing 1,2,3,4 in the above input box. At 4 it showed error, means there are id available up to 3.

Then I typed (1 UNION SELECT 1,2,3,4) and it gave me following results:



This gave me some information about the table and column position.

Then I typed (1 UNION SELECT 1, table\_name, 3, 4 FROM information\_schema.tables) and it gave following results:

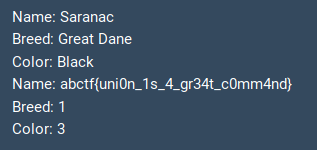


After this I searched for (1 UNION SELECT 1, column\_name, 3, 4 FROM information\_schema.columns) and got following results(deep down):



I got the table\_name as “w0w\_y0u\_f0und\_m3” and column\_name as “f0und\_m3”. Now the query was simple :-

(1 UNION SELECT 1, f0und\_m3, 3, 4 FROM w0w\_y0u\_f0und\_m3) and the flag came:



The flag is : abctf{uni0n\_1s\_gr34t\_c0mm4nd}