< SQL injection 워게임 풀이문서 >

허정화

문제 14번



처음보는 유형이다.

보면 shit의 길이는 1보다 크면 안되고

shit으로부터 1234를 select한 값이 true이면 풀리는거 같다.

[풀이]

일단 shit에는 \n \r \t의 필터링이 걸려있다.

자세히 알아보면

\n : new line 활동 위치를 다음 라인의 시작으로 옮김

\r : carriage return 활성 위치를 현재 라인의 시작으로 옮김

\t : horizontal tab 활성 위치를 수평 탭의 다음 위치로 옮김

\f : form feed 활성 위치를 다음 페이지의 시작으로 옮김

\b: backspace 활성 위치를 현재 라인에서 한 스페이스 뒤로 옮김

\v : vertical tab 활성 위치를 수직 탭의 다음 위치로 옮김

그리고 검색을 해보니 from과 prob\_giant 가 붙어있어 쿼리가 실행이 안되기 때문에

공백을 넣어주면 된다고 한다.

공백우회의 방법에는  
\n : new line(Line feed) %09

\r : carriage return %0d

\t : horizontal tab %09

\f : form feed %0c

\v : vertical tab %0b

아무거나 선택해서 넣어보자

?shit=%0c

[flag]

