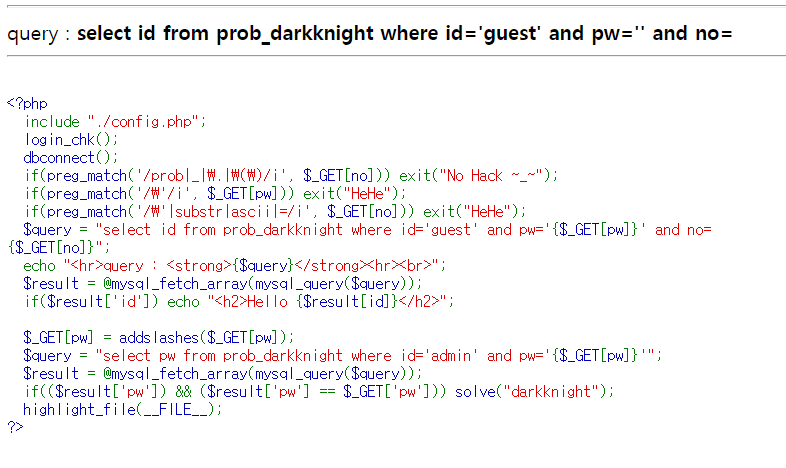
< SQL injection 워게임 풀이문서 >

허정화

문제 12번

코드를 보면 id가 admin이고 pw값이 지정된 값이어야 solve되는 것 같다.

[풀이]

현재 여러가지 필터링이 걸려있으며 SQL블라인드 문제라고 보여진다.

pw에서 싱글쿼터(‘)를 사용할 수 없으며 no에서는 싱글쿼터(‘), ascii, substr함수를 못쓴다.

일단 pw의 길이를 알아보자.

?pw=1&no=1 or length(pw) like 8#



다른 여느 문제와 똑같이 8자리이다. 파이썬 코드를 고쳐보자.

‘ -> “ (%22)

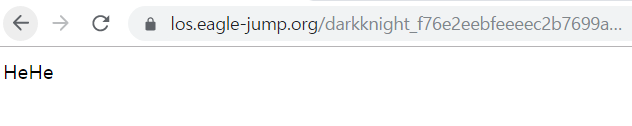
= -> like

어차피 나는 substr함수를 안쓴다. 근데 오류가 난다.. 왜일까 ?



혹시나 해서 url에 직접 입력해보았다.

?no=1 or substring(pw,1,1) like “1”

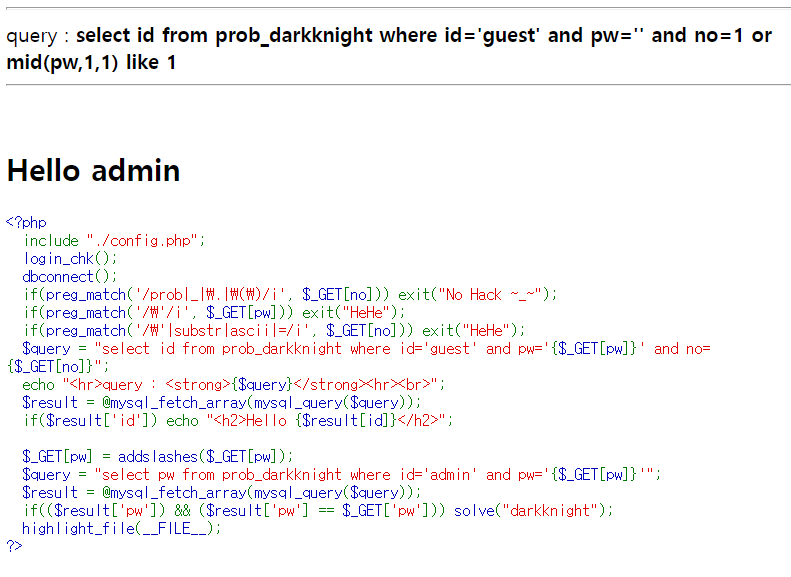


필터에 걸렸다. substring함수도 안되나 보다.

검색해보니 사람들은 mid함수를 대체해서 사용하였다.

mid는 mid(문자열, 위치, 길이) 이므로 substr과 동일하게 사용할 수 있다.

그리고 마지막 like ‘문자열’로 필터에 걸리기 때문에 like “문자열”로 대체해줬다.



mid 로 대체해주니 우연히 1이 맞았다.

파이썬 코드를 돌려보자 !



[flag]

1c62ba6f



**성공!**