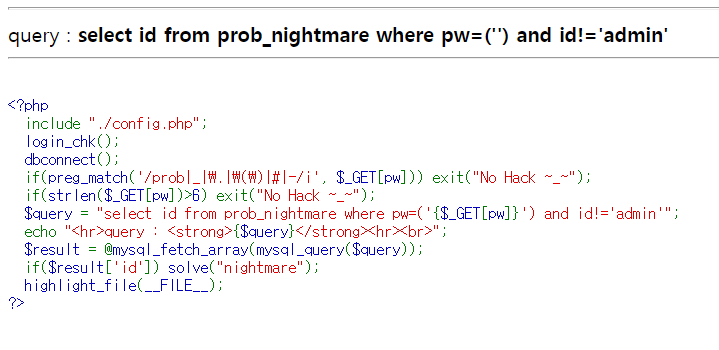
< SQL injection 워게임 풀이문서 >

허정화

문제 18번



id가 정해진 값이면 풀리는 거 같다.

[풀이]

현재 #, --,\ 등등 주석처리를 필터링하고 있으며 pw의 길이는 6자리 이하여아한다.

이는 SQL에서 임의의 문자열을 나타내는 역할인 0을 이용해야한다..

“문자열”=0은 참이 되므로 이를 사용해 쿼리를 작성해보면

?pw=‘)=0;%00

이때 %00(NULL)은 다른 주석처리하는 값들이 필터링이 되어있기 때문에 대신해서 넣어준 값이다.

[flag]

성공!

