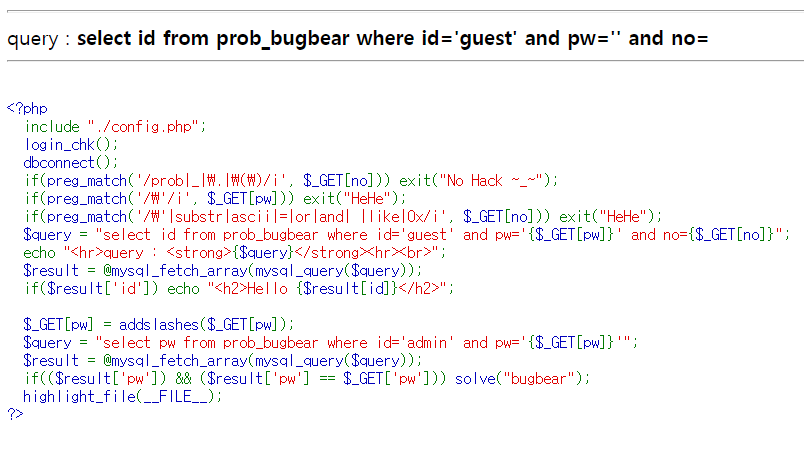
< SQL injection 워게임 풀이문서 >

허정화

문제 13번

코드를 보면 id가 admin이고 pw값이 지정된 값이어야 solve되는 것 같다.

[풀이]

현재 이 문제도 12번과 비슷하게 여러가지 필터링이 걸려있으며 SQL블라인드 문제라고 보여진다.

pw에서 싱글쿼터(‘)를 사용할 수 없으며 no에서는 싱글쿼터(‘), ascii, substr함수,or, and 심지어

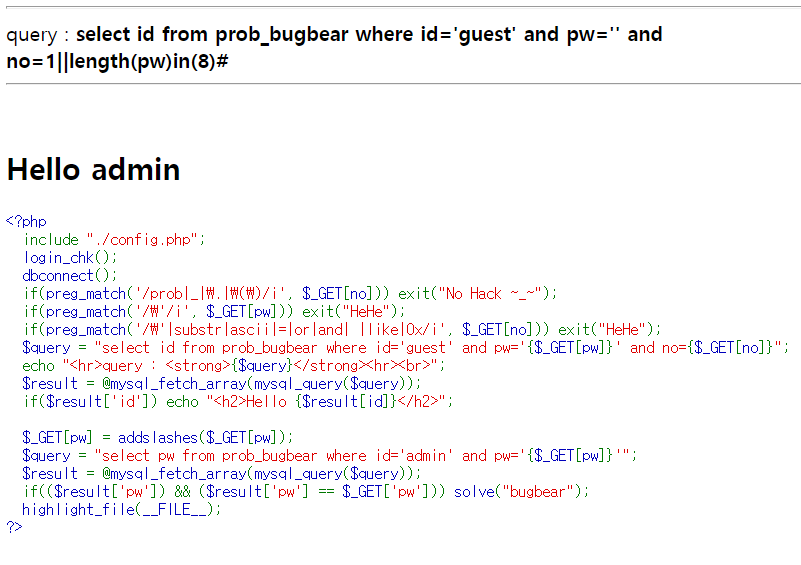
like, 0x 도 못쓴다. 공백도 못씀..

or -> ||

like -> in()으로 대체해서 쓸수있다.

일단 pw의 길이를 알아보자. 일부러 공백없이 썼다.

?no=1||length(pw)in(8)#

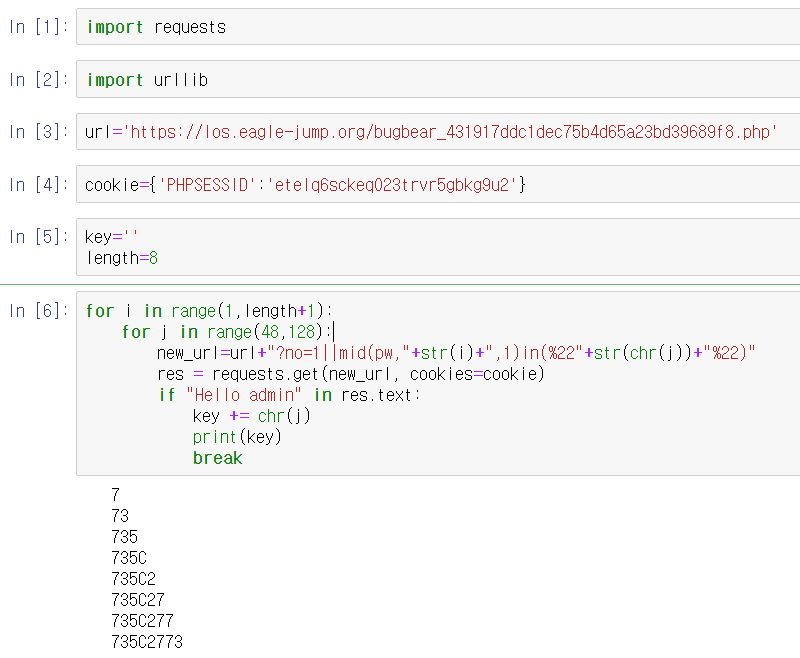


다른 여느 문제와 똑같이 8자리이다. 파이썬 코드를 고쳐보자.

or -> ||

subst 함수 -> mid

=, like -> in(문자) 이때 안에 문자는 싱글쿼터’말고 더블쿼터”



[flag]

735c2773

