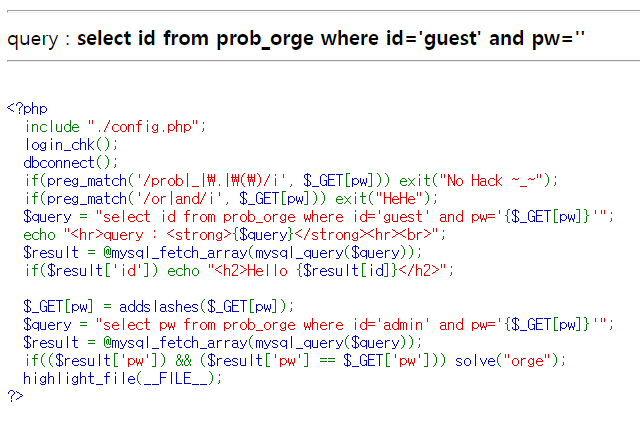
< SQL injection 워게임 풀이문서 >

허정화

문제 7번



코드를 보면 pw값이 정해진 값이어야 solve되는 것 같다.

[풀이]

블라인드 SQL이라고 생각을 하여서 일단 pw의 길이를 구해주었다.

현재 or와 and에 필터링이 걸려있기 때문에 or은 ||로 바꿔준다.

여러 숫자들을 해본결과 length는 8이다

?pw=1’ || length(pw)=8#



문제 4에서 만들었던 파이썬 코드를 사용하여 pw를 구해보자.

여기서 유의해야할 점은 or은 ||그리고 and는 &&로 바꿔줘야하는데 이때 url에서 인식을 하기위해서는 &은 %26으로 써야한다.



[flag]

pw 값은 6c864dec

성공!

