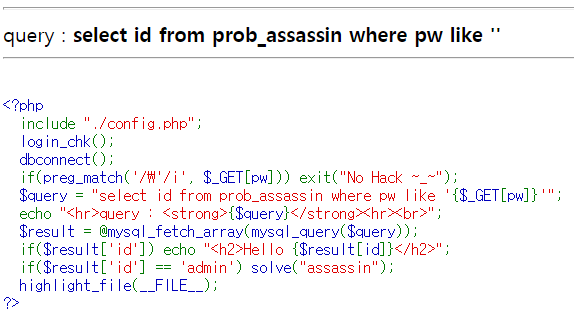
< SQL injection 워게임 풀이문서 >

허정화

문제 15번



id가 admin이면 풀리는듯 하다.

[풀이]

여러가지 넣어 보다가 도저히 안 풀려서 검색을 해보았다.

이 문제는 like based blind sql injection 문제라고 한다.

like 함수가 힌트인데 문제 풀이의 목적은 admin 행을 추출해야한다는 점에서 특정 행을 출력시켜 주는 %를 사용하면 된다고 한다.

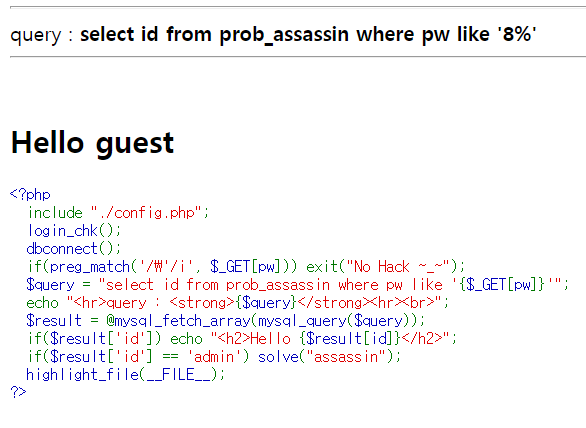
%의 사용법

like ‘가%’ : ‘가’로 시작하는 경우

like ‘%가’ : ‘가’로 끝나는 경우

like ‘%가%’ : ‘가’가 포함된 경우

처음에는 0부터 시작해서 8까지 해보니 hello guest가 나왔다.



파이썬을 이용하여 코드를 사용해 첫번째 문자가 뭔지를 알아보기위해 실행시켜보았다.

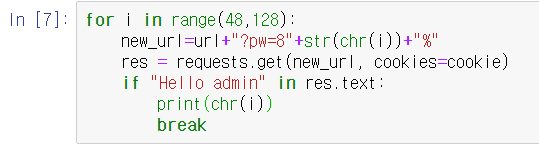
하지만 Hello admin은 나오지 않았다

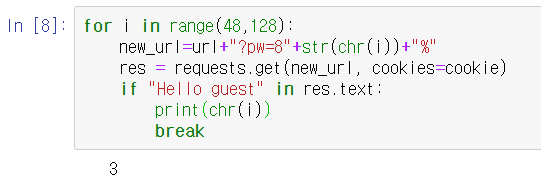
이로써 guest와 admin모두 첫 자리가 8이라고 유추할 수 있다.



두 번째 문자를 알아보자. admin으로 찾으니까 안나온다.

이번에도 guest랑 같다는 것을 알 수 있다.





guest의 두번째 문자는 3

세 번째 문자를 알아보자.



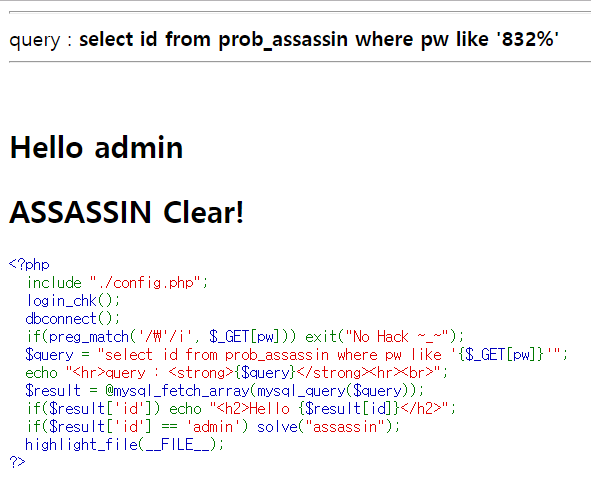
세번째 문자는 2이다.

이로써 16번을 성공할 수 있다.

?pw=832%

[flag]

성공!



번외로 계속해서 코드 이용해 찾아보니 pw값은 832edd10 이 나왔다.

