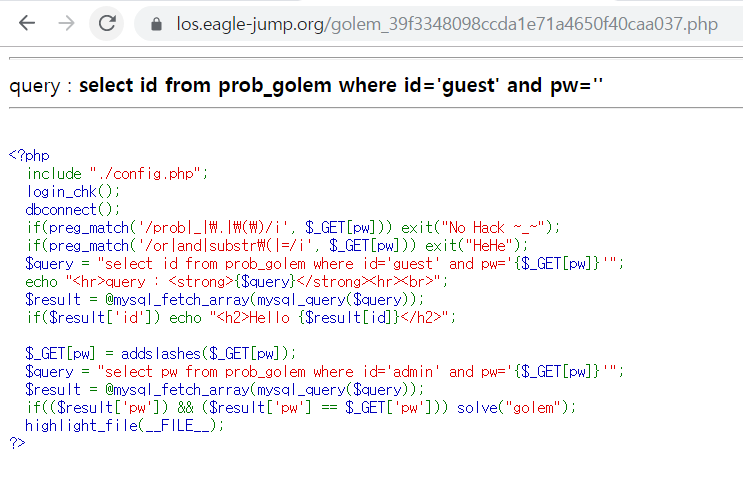
< SQL injection 워게임 풀이문서 >

허정화

문제 11번

코드를 보면 pw값이 지정된 값이어야 solve되는 것 같다.

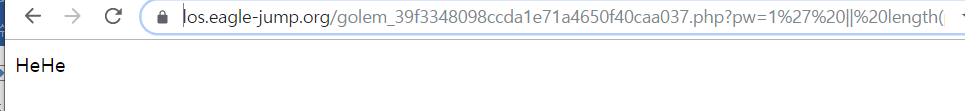
[풀이]

SQL블라인드 문제라고 보여진다.

보면 or and substr함수를 필터링 하기 때문에 코드를 손봐야 할 것으로 보인다.

일단 pw의 길이를 알아보자.

?pw=1’ || length(pw)=8#



왜죠… 자세히 보니 =도 필터링을 하고있다..ㅎ;;;ㅎㅎㅎ

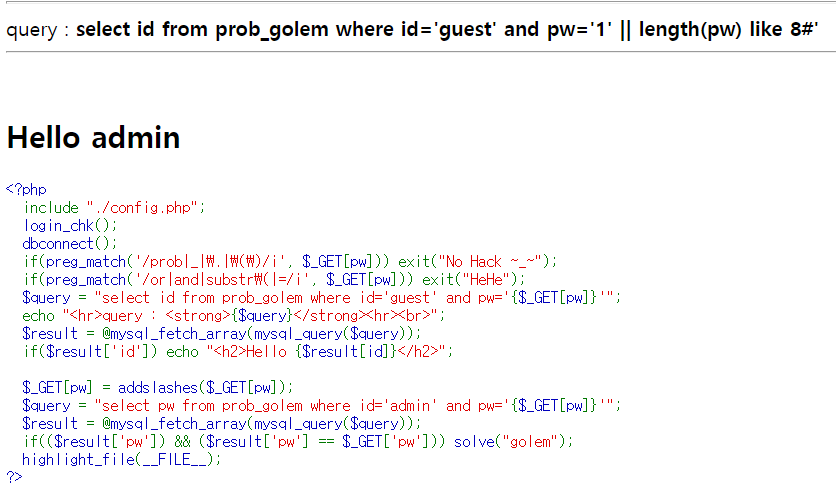
대체가능한 문자열을 알아보자

or = ||

and = &&

= = (like)

어차피 나는 substr함수를 안쓴다.



길이는 8

짜뒀던 파이썬 코드를 수정하여 실행시켜 보자.



[flag]

88e3137f

