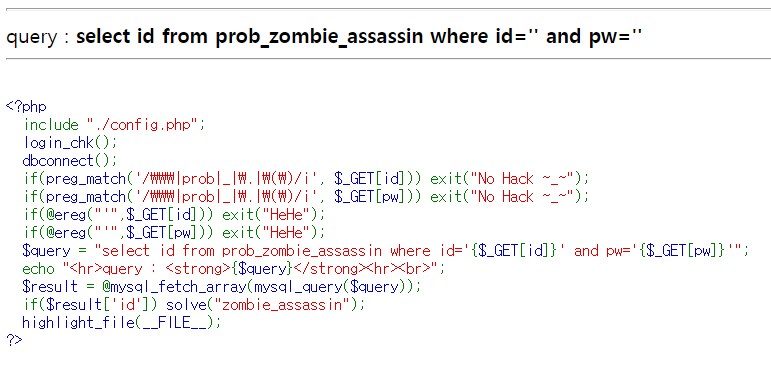
< SQL injection 워게임 풀이문서 >

허정화

문제 16번

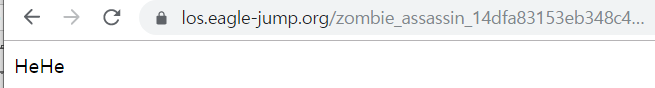


id가 정해진 값이면 풀리는 거 같다.

[풀이]

‘ or 1=1 # 공격을 하려했지만 ‘를 필터링하고있어서 안먹힌다.

?pw=’ or 1=1#



고민하다가 인터넷에 검색하니 이 문제는 싱글쿼터를 ereg로 필터링 하고있으며 이는 취약점이 있다고한다.

그 취약점 중 하나가 앞에 %00(NULL)이 있으면 탐색을 종료한다는 것이다.

그래서 해보았다.

?pw=%00’ or 1=1#

[flag]

성공!

