< SQL injection 워게임 풀이문서 >

허정화

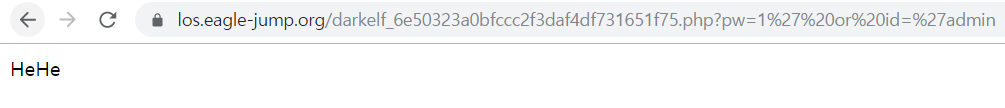
문제 6번



코드를 보면 id값이 admin이여야 solve되는 것 같다.

[풀이]

먼저 url뒷부분에 ?pw=1’ or id=’admin을 줬다. 역시 안된다.



현재 or 과 and에 필터링이 걸려있다.

검색해보니 이것도 공백을 우회했던것과 같이 우회하면 된다고 한다.

or은 || , and 는 &&

?pw=1’ || id=’admin

[flag]

성공!

