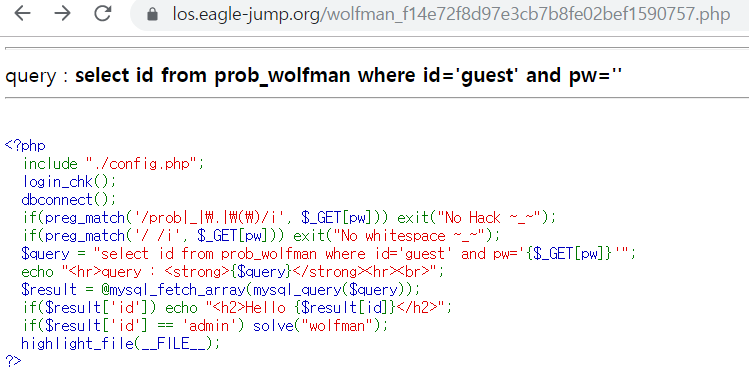
< SQL injection 워게임 풀이문서 >

허정화

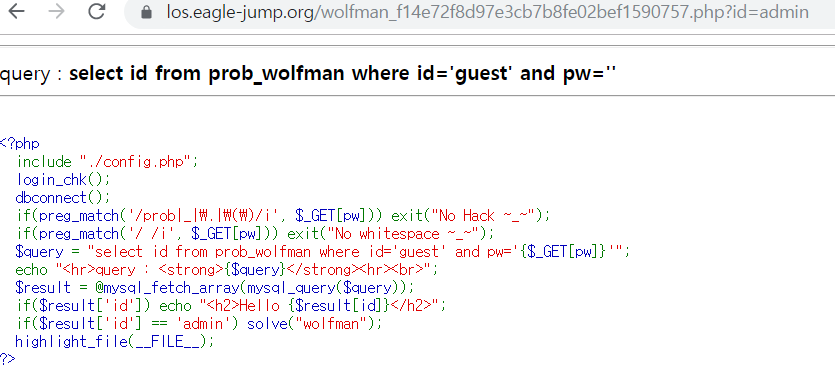
문제 5번



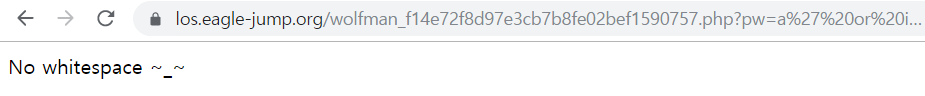
코드를 보면 id값이 admin이여야 solve되는 것 같다.

[풀이]

먼저 url뒷부분에 ?id=admin을 줬다. 역시 안된다.



?pw=1’ or id=’admin도 안된다.



보면 공백을 필터링 하고있으며 검색해보니 공백을 우회해야한다고 한다.

(%0a, %0b, %0c, %09 등 공백을 우회할 수 있는 대체 문자열을 사용)

나는 %0a를 사용해보았다.

?pw=a’%0aor%0aid=’admin

[flag]

성공!

