< SQL injection 워게임 풀이문서 >

허정화

문제 3번

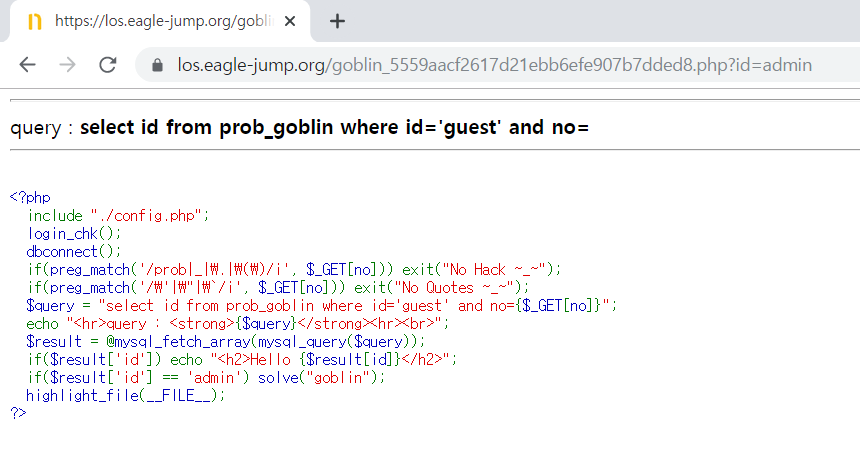


코드를 보면 id값이 admin이면 solve(“cobolt”)가 실행되는 것을 알 수 있으며 이를 목표로 한다.

query를 통하여 id값와 pw값을 받아온다.

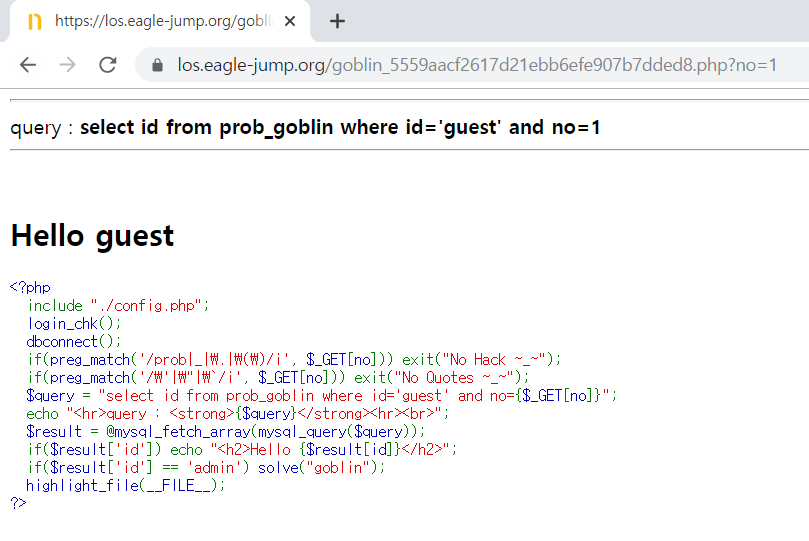
[풀이]

먼저 url뒷부분에 ?id=admin을 넣어본다. id에 admin이 들어가지 않았다.



?no=0 을 뒤에 붙여보니 no에 들어가긴했으나 별다른 변화가없음, 1을 넣어보자



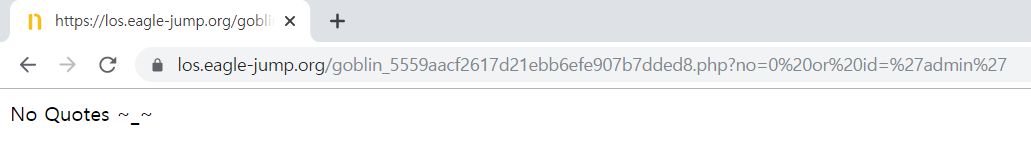


1을 넣어주니 Hello guest가 나옴, no 1이면 id에 값이 들어가 guest 출력되는 것을 알 수 있음

그렇다는건 0을 넣을 때는 id에 값이 안 들어갔다는 걸 알 수 있다.

따라서 no에는 0 id에는 admin을 넣어주면 성공할 수 있다는 건데

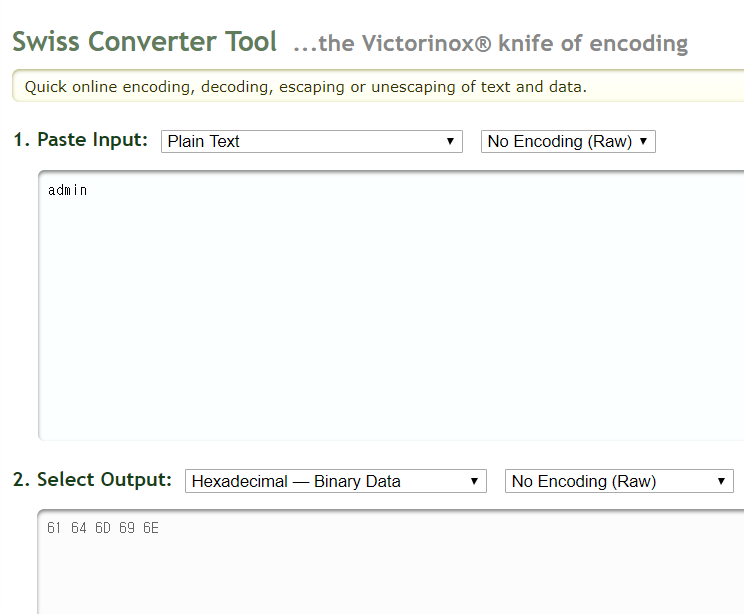
?no=0 or id=’admin’



위에 if문에서 ‘ ’때문에 걸려버린다.

검색해보니 이런 경우 문자열을 16진수로 나타내라고 한다.

<https://www.percederberg.net/tools/text_converter.html> 에서 변환을 하였다.



php에서 hex형태를 인식 시키키위해 앞에 0x를 붙여준다

?no=0 or id=0x61646D696E 넣어줌.

[flag]

성공!

