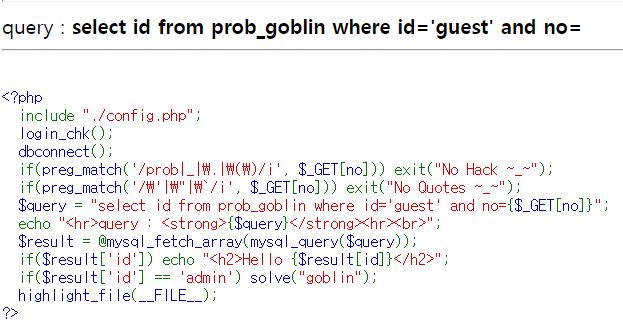
< 3번 워게임 풀이문서 >

김구민



이번 문제의 쿼리는 id를 guest라는 문자열로 가정하고 시작한다.

if($result['id'] == 'admin') solve("goblin"); 를 보아 id가 admin이어야 한다.

그리고 if(preg\_match('/\'|\"|\`/i', $\_GET[no])) exit("No Quotes ~\_~"); 문장이 추가되었는데

작은 따옴표(‘) 혹은 큰 따옴표(“)로 쿼리를 설정하는 것이 불가능하다.

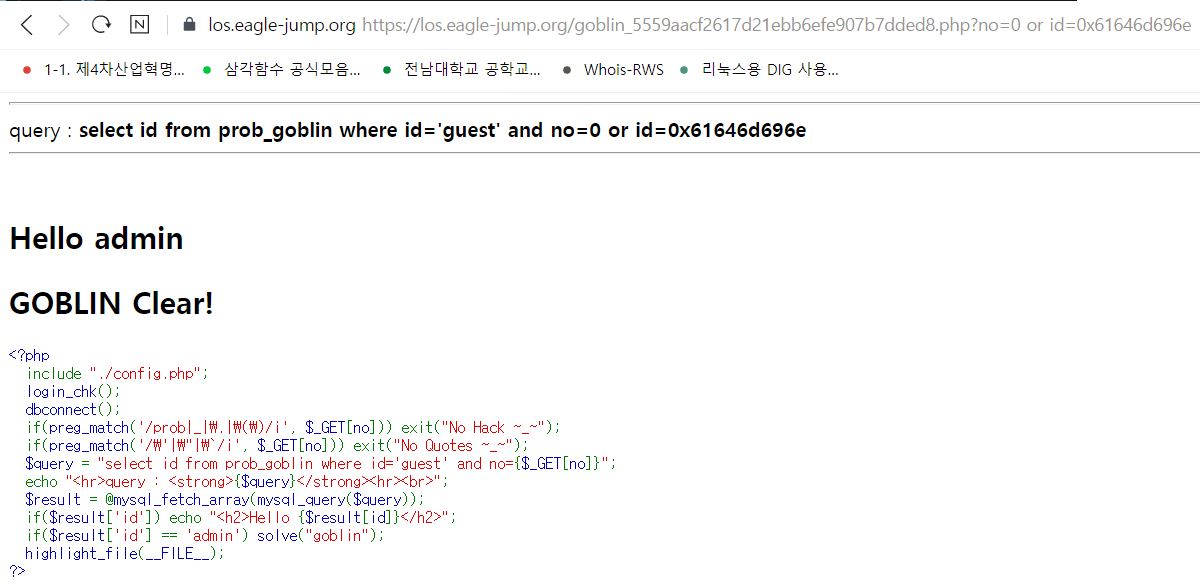
그렇기 때문에 예를 들어 no = 1 or id = ‘admin’ 식의 쿼리로는 풀 수 없다.

또한 쿼리를 no값을 설정하는 것부터 시작해야 한다.

따라서 쿼리에서 id를 설정할 때 다른 방식으로 접근해야 하는데 여기서 이용한 것 중 하나가 hex(16진수)이다. <https://www.browserling.com/tools/text-to-hex> 사이트를 이용해서 admin을 hex로 바꾸면 61/64/6d/69/6e이다.

그리고 일단 admin의 no가 뭔지 몰라서 0으로 설정하고 시작했다.

따라서 ?no=0 or id=0x61646d696e라는 문장으로 쿼리를 설정했다.



일단 문제가 풀렸다. 여기서 no값을 0으로 설정했었는데 다른 값으로 바꿔도 될까라는 의문점이 생겼다. 그래서 no를 1로 바꾸어보았다.



그렇게 하니까 위 사진과 같이 Clear라는 문구는 뜨지 않고 Hello guest라는 문구만 뜬 화면을 볼 수 있었다. 아마 guest의 no가 1로 설정되어 있는 것으로 해석된다.