LOS 풀이 문서

이진하

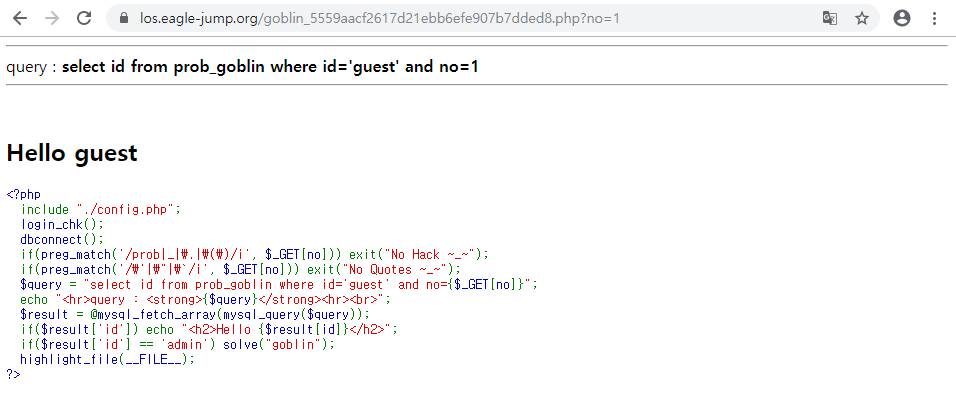
문제 3번



올바른 id, pw 값을 입력하면 문제를 해결할 수 있다.

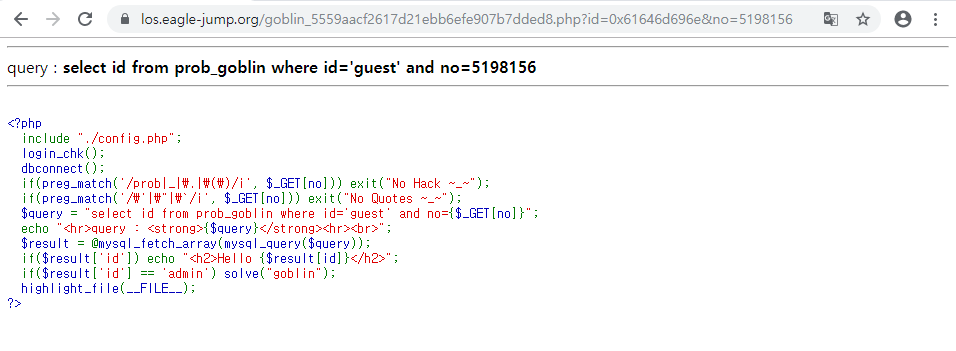
[풀이]

if($result['id'] == 'admin') solve("goblin"); 부분을 보면 이 문제의 id가 admin이라는 것을 확인할 수 있지만, 쿼리문에는 id가 ‘guest’라고 나와 있다. 따라서 id가 admin이 되게 하면서, id=guest 값을 무력화시켜야 한다. 따라서 no 변수에 값을 찾기 위해 먼저 1을 넣어 보았다.



Hello guest 가 뜬 것을 보아 guest의 no가 1이라는 걸 알게 됐고, 따라서 no에 1이 아닌 값을 넣으면 코드를 무력화시킬 수 있을 것이다.

또한 if(preg\_match('/\'|\"|\`/i', $\_GET[no])) exit("No Quotes ~\_~"); 를 보면 따옴표 문자들을 쓸 수 없다는 것을 알 수 있다. id 변수에 String 값을 넣기 위해서는 따옴표가 필요했는데 싱글 쿼터를 사용하면 값을 필터링 하기 때문에 admin을 16진수로 바꿔 넣어보았다.



id=guest를 무력화시키기 위해 no에 임의의 값을 넣었으나, 이렇게 되면 no 조건이 맞지 않기 때문에 쿼리문을 이용해 ?id=0x61646D696E&no=5198156 or id=0x61646D696E를 url에 넣어 보았다.



GOBLIN Clear!