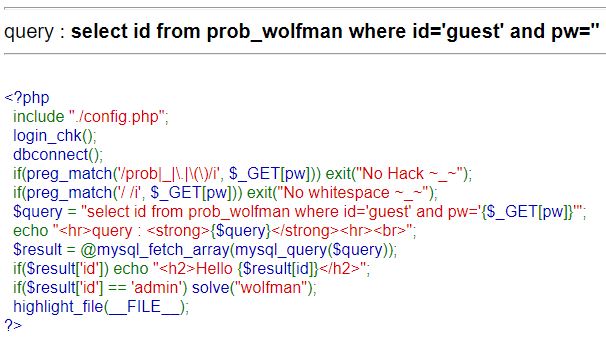
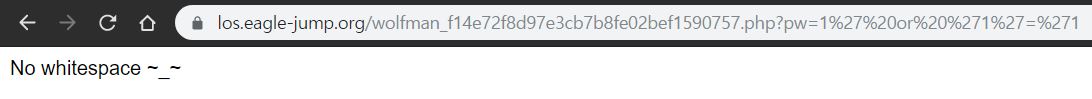
< 5번 워게임 풀이문서 >

김구민



처음에 1번을 풀었던 것과 같이 ?pw=1’ or ‘1’=’1 쿼리를 사용해 보려고 시도했으나 실패했다.



코드를 찬찬히 살펴보니 다음과 같은 코드가 있어서 공백을 사용할 수 없었다.

if(preg\_match('/ /i', $\_GET[pw])) exit("No whitespace ~\_~"); pw 유추시 공백을 사용불가.

주석을 사용하는 문제는 아닌 것 같고 or을 이용해서 푸는 방법 밖에 생각이 안 났는데 그러려면 공백을 사용해야 하는데 사용할 수 없었다.

공백을 대신해서 사용할 수 있는 대체 문자들을 찾아보니 다음과 같았다.

Tab (%09)

Line Feed (%0A)

Vertical Tab (%0B)

Form Feed (%0C)

Carriage Return (%0D)

공백 대신 Tab을 선택해서 ?pw=1’%09or%09‘1’=’1 로 대체했더니 공백 문제는 해결할 수 있었다.



if($result['id'] == 'admin') solve("wolfman");

그렇지만 문제를 풀기 위해서는 id가 admin이어야한다.

id=’guest’ 부분은 문제를 풀 때 도움이 되지 않는 부분이다.

그래서 pw부분에 아무 내용을 넣지 않고 tab과 or을 이용해서 id=’admin’ 를 추가하고

admin의 pw까지 일치시켜야 한다는 코드가 없기 때문에 그 뒤는 #(%23)으로 주석처리했다.

?pw=%27%09or%09id=%27admin%27%09%23

