< 2번 워게임 풀이문서 >

김구민



1번(gremlin) 문제와 유사한 코드이다.

그러나 다른 점은 역시나 쿼리문이다. pw를 md5로 해싱 처리된 것으로 injection이 적용된다.

그리고 if($result['id'] == 'admin') solve("cobolt"); 이 부분이 핵심이다.

result의 id가 admin이어야 문제를 해결할 수 있다.

그렇기 위해서는 pw변수 부분 쿼리를 주석화해야한다.

따라서 php 뒤에 ?id=admin%27%23을 넣어주면 해결할 수 있다.(%27 = ‘ , %23 = #)

