< SQL injection 워게임 풀이문서 >

허정화

문제 8번



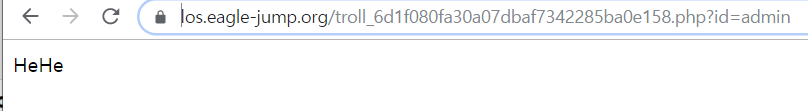
코드를 보면 id값이 admin이어야 solve되는 것 같다.

[풀이]

?id=’admin 을 넣어줬더니 필터링이 걸려있어 안된다.



?id=admin도 안된다.



헥사코드로 넣어줘야할까?

?id=0x61646D696E



아마 헥사코드는 ‘’안에 들어가면 안되는데 들어가서 인식을 못하는 듯하다.

모르겠어서 찾아보니 SQL쿼리문에서는 대소문자를 구분하지 않는다는 점을 이용하여 admin이든 Admin이든 ADMIN이든 모두 admin의 결과를 반환한다.

이 점을 이용해 적절히 변환해주면 된다고 한다.

?id=ADMIN

[flag]

성공!

