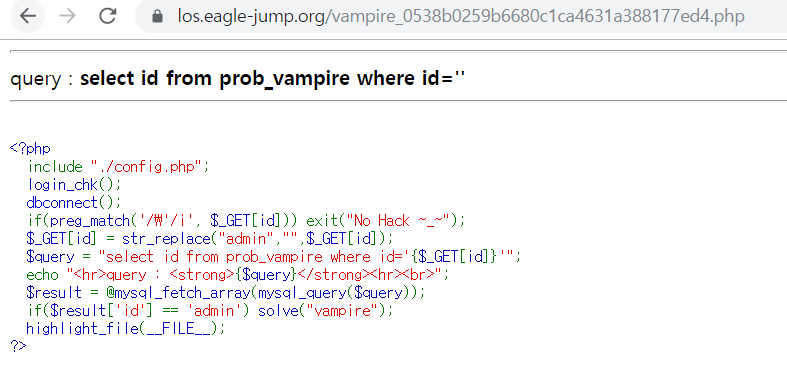
< SQL injection 워게임 풀이문서 >

허정화

문제 9번



코드를 보면 id값이 admin이어야 solve되는 것 같다.

[풀이]

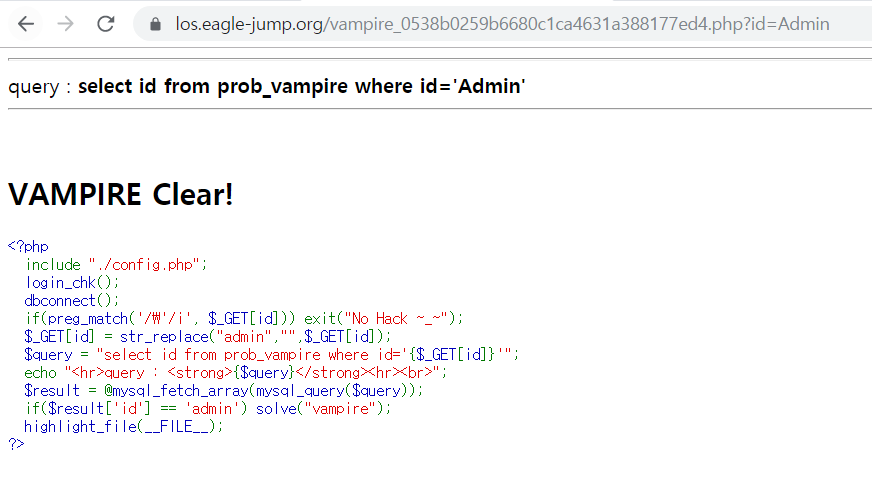
str\_replace함수를 보면 admin을 공백으로 치환해주는 역할을 하는 것을 알 수 있다.

그렇다면 대문자로 쓰면되지 않나..

?id=Admin

[flag]

성공!



너무 쉽게 성공한거 같아 출제의 의도를 파악하기 위해 검색을 해보았다.

원래는 strtolower이라는 함수가 존재해 대문자를 소문자로 바꾸어주는 함수가 있다.

그래서 출제자의 의도는 str\_replace함수가 1번만 실행이 되기 때문에

admin을 2번쓰는것이다.

근데 보면 현재 strtolower이라는 함수가 없다.

문제의 오류라고 생각한다.