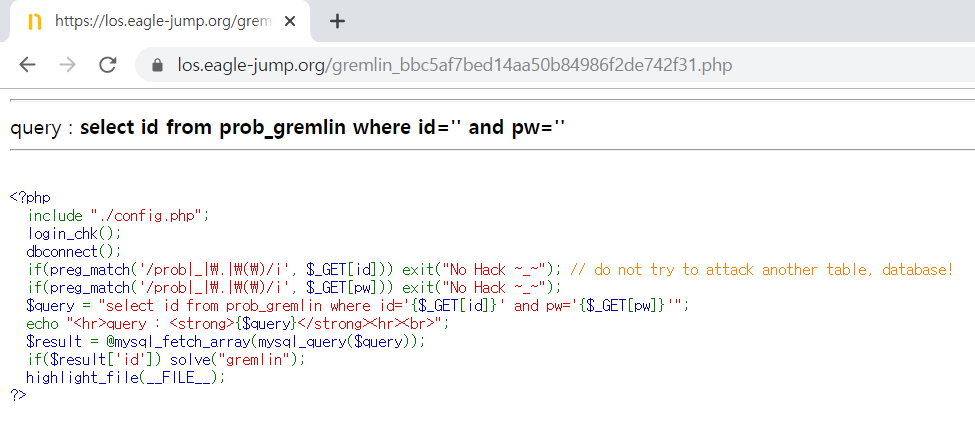
< SQL injection 워게임 풀이문서 >

허정화

문제 1번

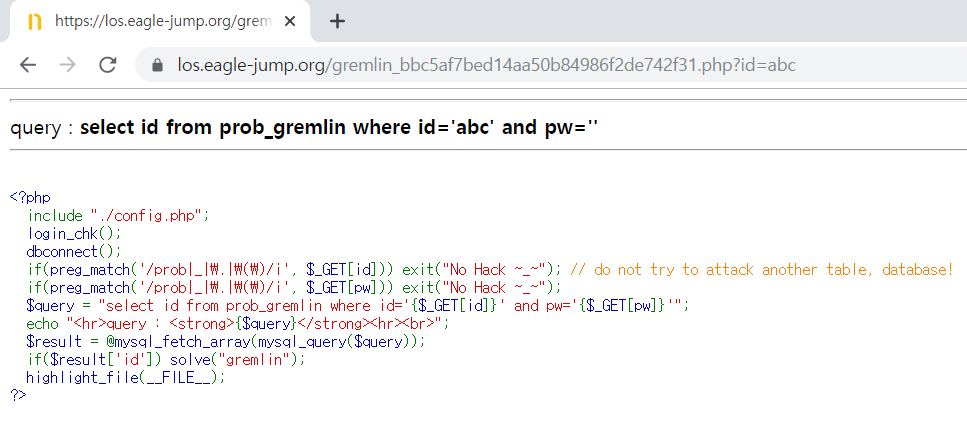


코드를 보면 id에 값이 있으면 solve(“gremlin”)이 실행되는 것을 알 수 있으며 이를 목표로 한다.

query를 통하여 id값와 pw값을 받아온다.

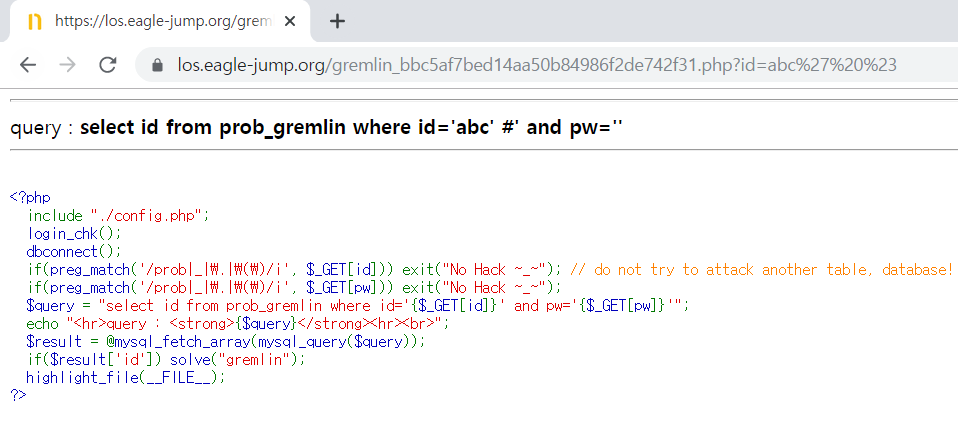
[풀이]

먼저 url뒷부분에 ?id=abc을 넣어본다. 하지만 뒤에 pw가 해결이 안돼 실패



그럼 뒤에를 주석처리 해볼까?

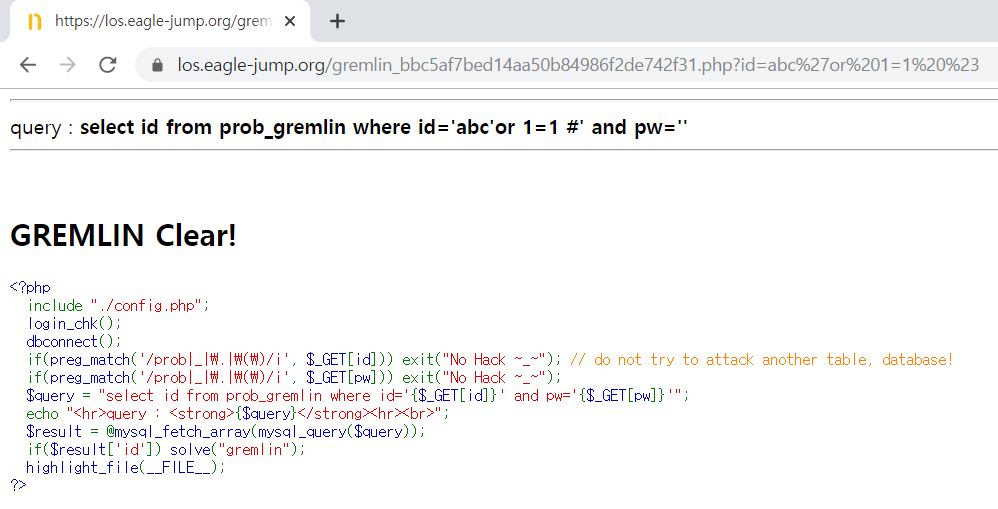
이때 띄어쓰기는 %20, # %23, ‘ %27이다.

실패

가장 많이 쓰인다는 or 1=1 # 과 or 1=1-- 를써보자



뒤에 ?id=abc%27or%201=1--%20 을 넣으니까 성공



?id=abc%27or%201=1%20%23도 성공

[flag]

성공!



