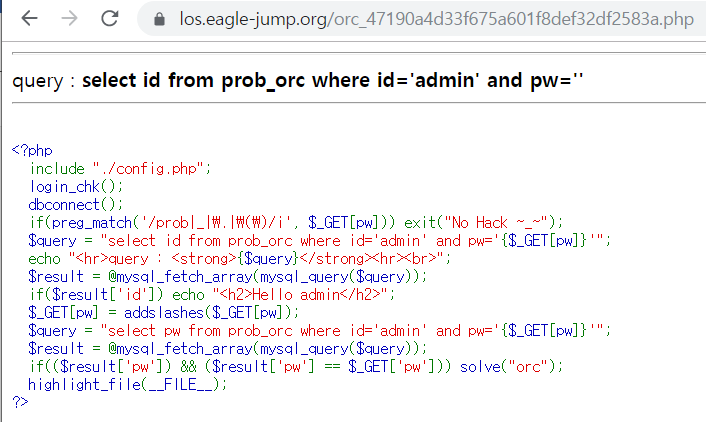
< SQL injection 워게임 풀이문서 >

허정화

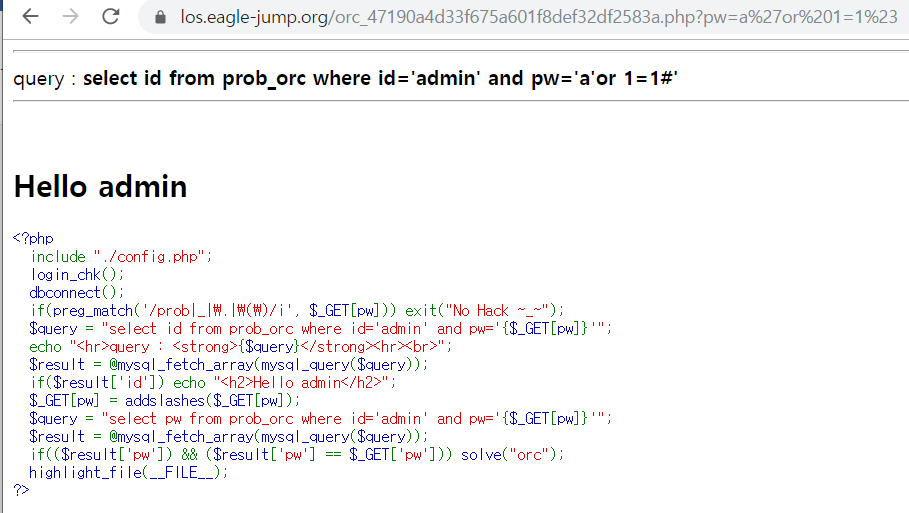
문제 4번



코드를 보면 pw값이 지정된 값과 같아야 solve되는 것 같다.

[풀이]

먼저 url뒷부분에 ?pw=a’or 1=1#을 넣어줬다.

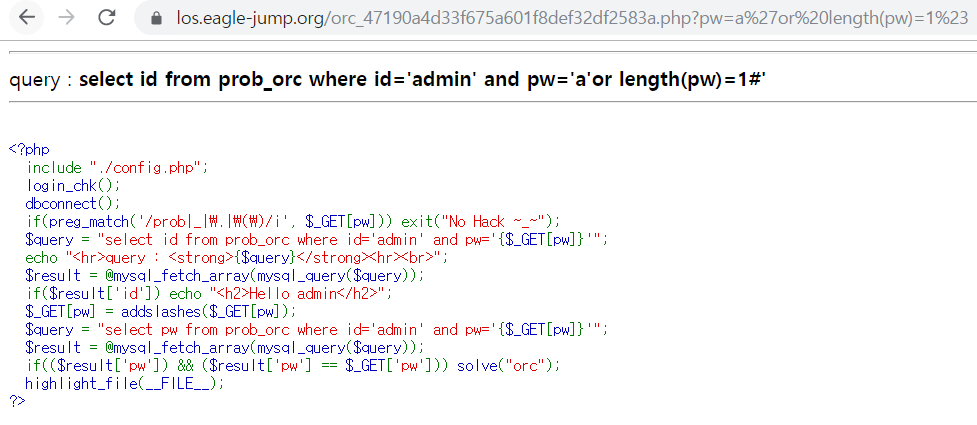


id에 admin값이 들어가서 hello admin은 출력이 되었지만 pw값은 지정된 값과 같지않아 풀리지 않았다. 어떻게 해야할지 몰라서 인터넷에 검색해보았다.

이는 blind injection문제 였으며 이에 대한 기법을 사용해보았다.

먼저 length라는 함수를 사용해 pw의 길이를 잘아보자

?pw=a’ or length(pw)=1#



1~8까지 해보았으며 결과적으로 8일 때 참으로 나왔다.



pw의 길이가 8인걸 알았으므로 코드를 작성해 pw의 값을 알아내자.

공격에는 substr연산자, asci 연산자가 필요하다.

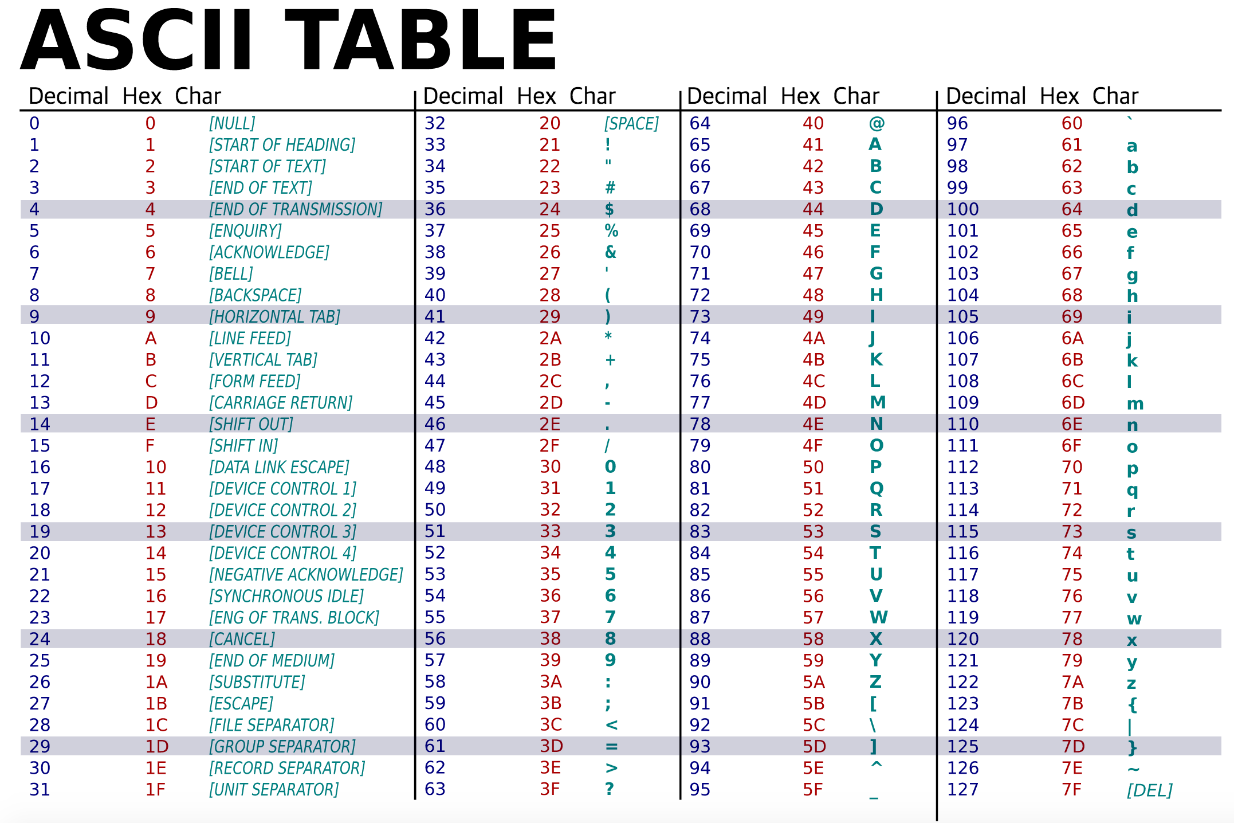
그리고 값을 참이 되도록 조작해두고 뒤에 추가로 BlindSQL 값 판단 확인 쿼리 내용추가

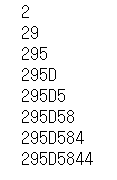


길이는 알기 때문에 8로 주고 페이지의 url과 쿠키값을 넣어주었다.

pw의 길이만큼 돌아가는 루프를 만들어주고

substing함수로 pw파라미터 문자를 하나씩 추출하여 아스키코드를 비교하여 값을 찾는다.





pw는 295d5844이다.

[flag]

성공!

