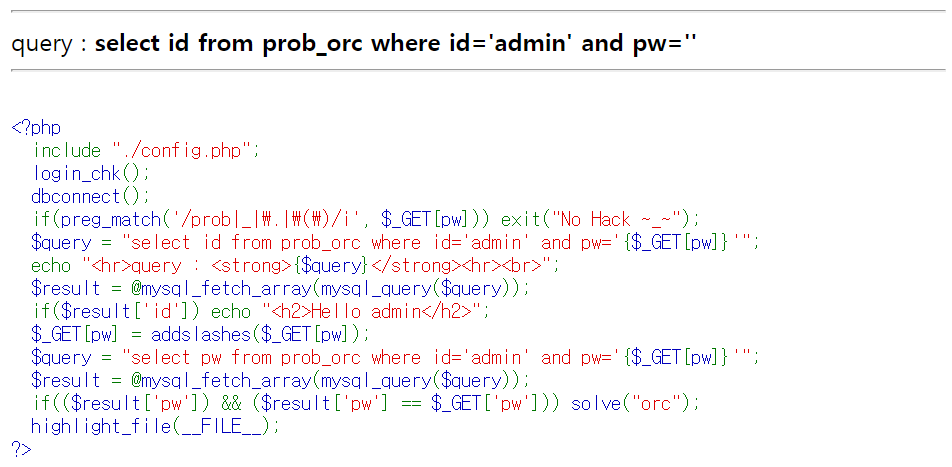
<워게임 풀이문서>

4번(orc) 풀이

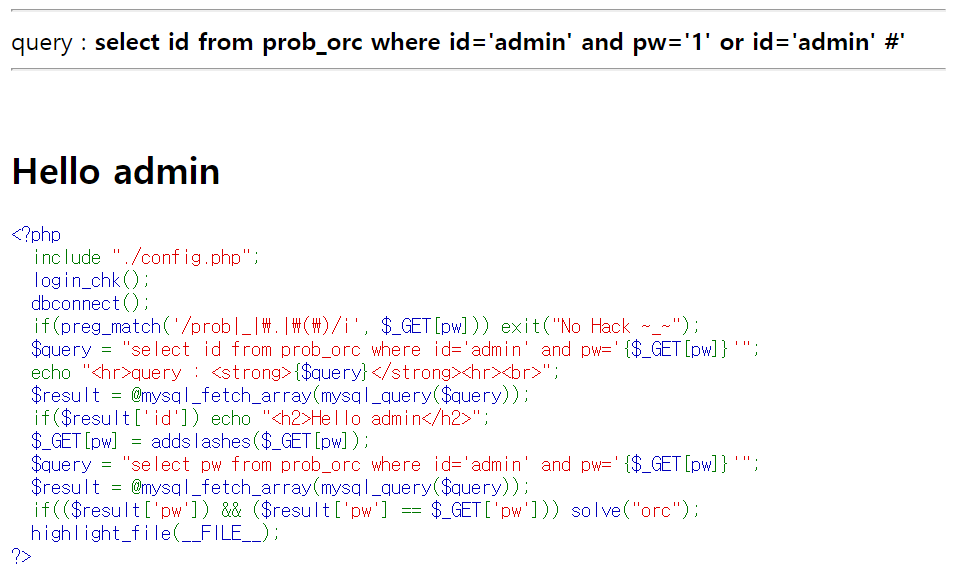
이안나



orc의 문제 화면이다.

preg\_match로 질의문에 \_와 . 그리고 ()사용을 제한하고 있다.

if($result['id']) echo "<h2>Hello admin</h2>"; 에서 쿼리가 참이면 페이지에 Hello admin을 출력한다.



그리고

$\_GET[pw] = addslashes($\_GET[pw]); 로 사용자가 작성한 질의문에 addslashes() 함수를 사용해 한번 더 질의를 수행한다.

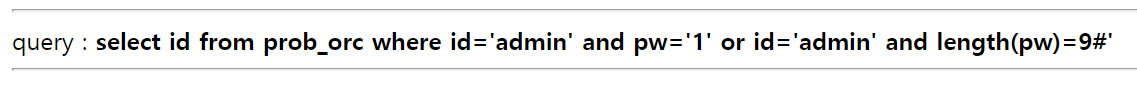
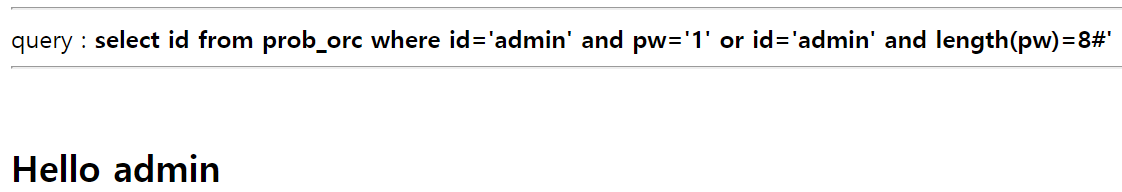
if(($result['pw']) && ($result['pw'] == $\_GET['pw'])) solve("orc");

그리고 if문에서 쿼리로 출력된 pw와 사용자가 입력한 값이 같아야 solve("orc")가 수행되어 문제를 해결할 수 있다.

addslashes함수는 특정 문자(', “ 등)에 \를 추가해 이스케이프 문자로 바꾸어 주는 함수이다. 쿼리문을 사용할 경우 ‘’에 \가 추가되기 때문에 입력 값과 result가 일치하지 않게 된다. 따라서 pw=’’에는 ’등이 사용되는 쿼리 문이 아닌 정확한 admin의 password을 입력해야 두번째 if문이 작동된다는 것을 알 수 있다.

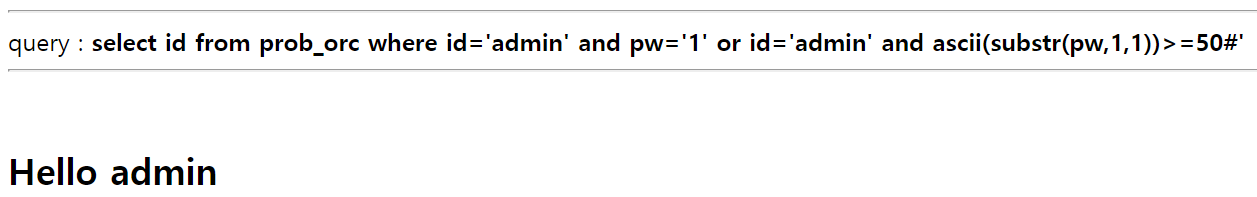
비밀번호를 알아내기 위해선 우선 length()함수를 사용해 비밀번호의 길이를 알아내고, substr()로 문자를 비교해 유추할 수 있다.

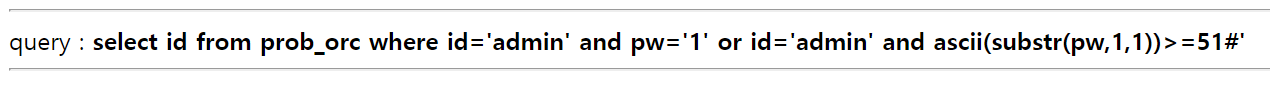


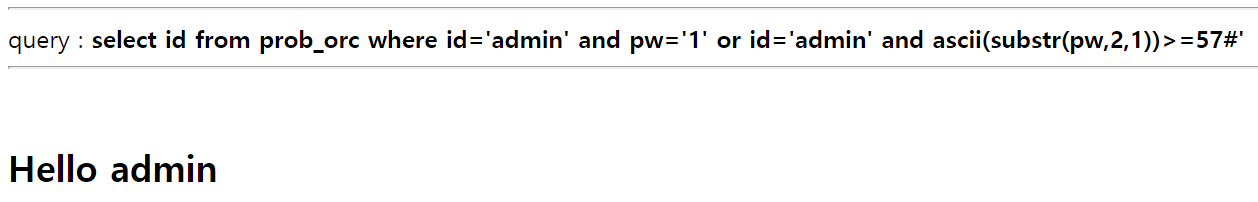
id가 admin이고 비밀번호의 길이가 8일 때 참이므로 admin의 비밀번호는 8개의 문자로 이루어져 있다.

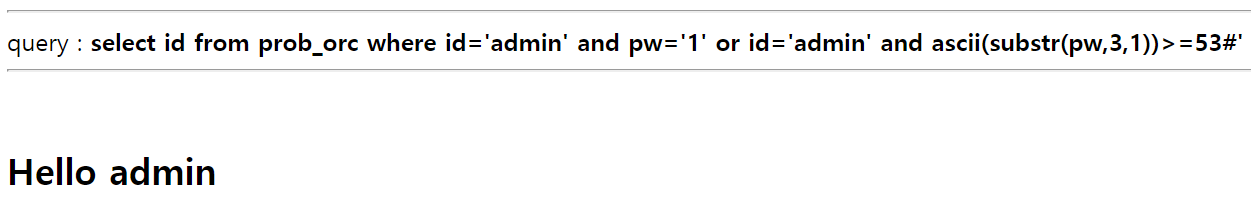
substr(문자열, 시작할 문자의 순서, 가져올 문자 수)로 pw에서 한 문자 씩 꺼내고, 비교연산자로 문자를 알아낼 수 있도록 ascii()함수를 이용해 문자를 아스키코드로 변환한다.

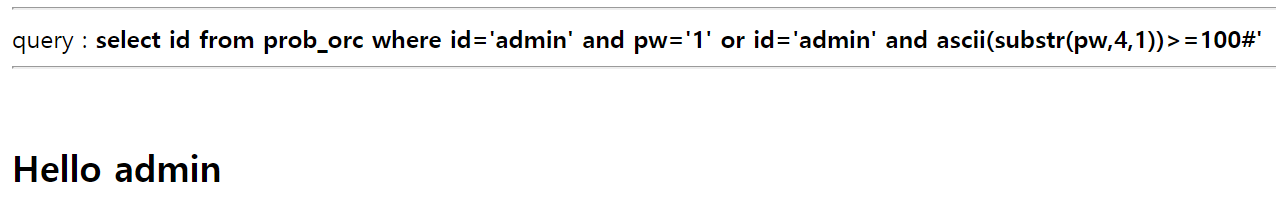
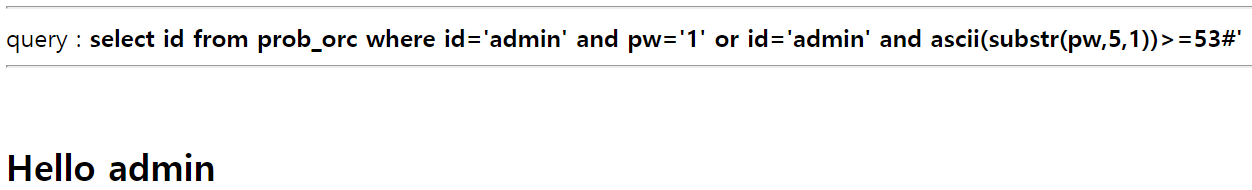


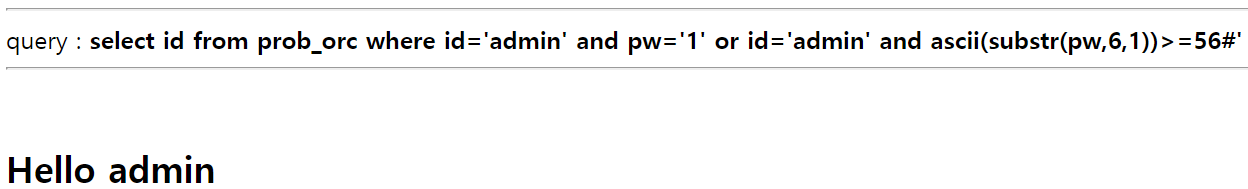
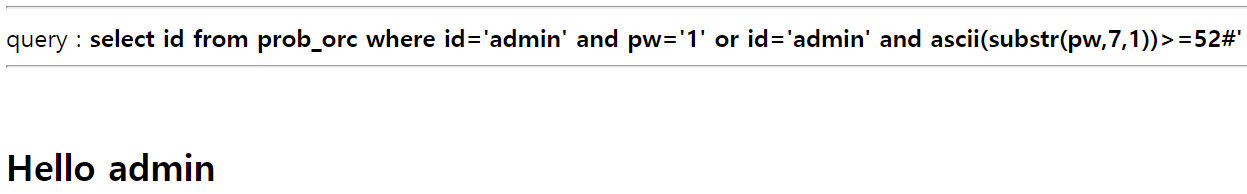
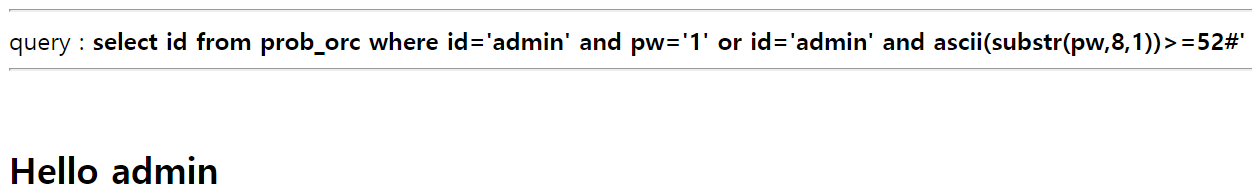


1번째 글자는 >=50일 때 true이고 51일 때 false이므로 아스키 50인 문자인 것을 알 수 있다.





1부터 8자리 까지 비밀번호는 아스키코드로 50 57 53 100 53 56 52 52 알아냈다.

아스키코드를 아스키코드표와 비교하여 원래의 문자인 ‘295d5844’를 찾아내고 pw값으로‘295d5844’를 입력하여 문제를 해결하였다.

