Lord of SQL Injection - orc Writeup

query : **select id from prob_orc where id='admin' and pw=''**

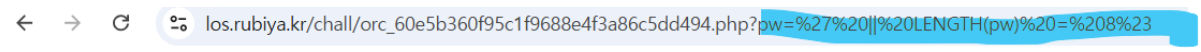
```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_orc where id='admin' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));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

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

먼저 쿼리문을 확인해보면 아이디는 admin으로 고정되어 있고, 패스워드를 파라미터로 입력받고 있다. 즉 pw를 맞춰야 문제가 풀릴 것으로 보인다.

이때 $_GET['pw'] 값에 특정한 패턴 (prob, _, ., ())이 포함되어 있으면 종료되므로 이것들을 사용하지 않고 공격을 해야 한다.

이 코드는 pw 파라미터의 값을 쿼리로 전달한 후 응답 결과에 따라 참(true) 또는 거짓(false)을 확인할 수 있으므로 Boolean-based Blind SQL Injection이 가능하다고 할 수 있다.

먼저 admin 계정의 비밀번호 길이를 알아내야 한다. 이를 위해 'pw=' || LENGTH(pw) = <숫자>%23 이라는 쿼리를 구성하여 참/거짓 결과에 따라 비밀번호의 길이를 추측할 수 있다. 이때 <숫자> 부분에 숫자를 1부터 시작하여 차례로 증가시키며 시도해야 한다.



query : **select id from prob_orc where id='admin' and pw='' || LENGTH(pw) = 8#'**

Hello admin

넣은 숫자가 8일 때 hello admin이 출력되는 것을 볼 때 pw의 길이는 8이라고 할 수 있겠다.

이제 실제 pw의 값을 알아내야 한다. 먼저 pw의 길이를 알아낸 것처럼 각 문자를 하나씩 대입하여 'hello admin'이 출력되는 값을 알아내고, 이를 8번 반복하는 방법이 있으나 너무 시간이 오래

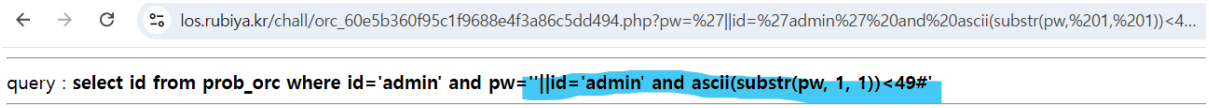
걸릴 것 같았다. 다른 라이트업들을 찾아보니 파이썬 코드를 구성해 pw를 알아내는 방법이 있었으나 실제로 코드를 실행해 봤을 때 자꾸 에러가 발생해서 결국 라이트업들을 참고하여 직접 대입하는 방법을 사용하기로 했다.

각 문자 위치별로 알파벳을 하나씩 추측해 나가는 이런 방법에서는 SQL의 SUBSTRING 함수를 사용한다.

예를 들어, 비밀번호의 첫 번째 문자가 '0' 인지 확인하려면 이러한 쿼리를 사용한다.

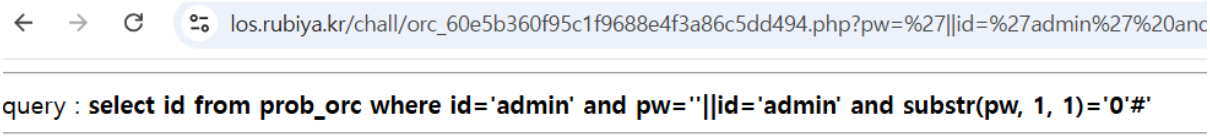
pw='||id='admin' and ascii(substr(pw, 1, 1))<49%23

id는 admin으로 고정시켜 둔다. Substring 함수를 사용한 substr(pw, 1, 1)라는 이 구조는 pw 문자열을 첫 번째부터 1개 문자열을 가져온다. 그리고 문자를 ascii코드로 변환하기 위해 ascii 함수를 사용한다. 첫 번째 글자가 ascii 코드 49번보다 작을 때 참이 반환되므로 ascii 코드 48번인 0이라 볼 수 있다.



Hello admin

확인하려면 쿼리문을 이렇게 수정한다.



Hello admin

<?php

이렇게 hello admin이 반환되면 맞는 값이라는 뜻이다. 즉 pw의 첫 글자는 0이다. 이런 과정들을 반복하여 참 즉 hello admin이 출력되는 값들을 8개 구하면 된다.

Hello admin

두 번째 글자를 구하려면 substr(pw, 2, 1)로 수정해야 한다. 이런 방법들을 반복하면 된다.

이 과정들을 반복하면 다음과 같이 글자들을 구할 수 있다.

두번째 pw ascii 57 -> 9

세번째 pw ascii 53 -> 5

네번째 pw ascii 97 -> a

다섯 번째 pw ascii 57 -> 9

여섯 번째 pw ascii 56 -> 8

일곱 번째 pw ascii 53 -> 5

여덟 번째 pw ascii 50 -> 2

이제 url 뒤에 **?pw=095a9852**를 입력하면 된다.