Lord of SQLi - troll

query : select id from prob_troll w here id=”

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

- GET방식으로 파라미터를 넘겨주고 있다.
- id파라미터의 값중에 “admin” 이 있으면 ereg를 이용하여 필터링한다.
- ereg함수와 mysql은 대소문자 구분을 하지 않는 것을 이용해서 풀면 된다.

payload

> query : select id from prob_troll w here id=‘admiN’

> URL : http://los.eagle-jump.org/troll_6d1f080fa30a07dbaf7342285ba0e158.php?id=admiN

- 위의 페이로드는 예시이고 몇번 째 글자이던 간에 대문자로 바꿔서 전송하면 풀린다.