Moctf 新春欢乐赛 WriteUp

签到题

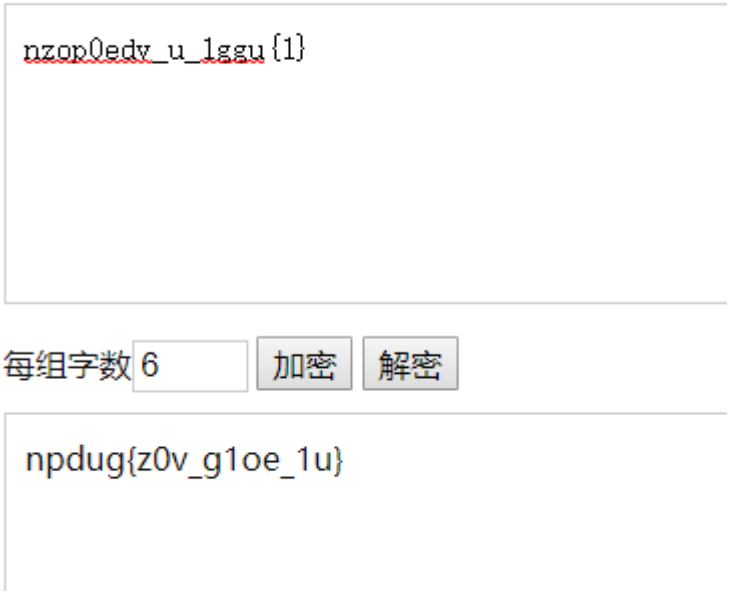
百度出来个 5 亿
Flag:moctf{500000000}

MISC

1:颜文字
直接把给的东西拉到 http://www.bm8.com.cn/jsConfusion/里格式化一下然后再 f12 里用控制台运行一下得到
Falg: moctf{Yan_Wen_Zi}

2:流量分析
用 wireshark 打开后拉到后面随便选一个可以追踪 TCP 流的,追踪一下就可以发现 flag
Flag: moctf{c@N_y0U_4lnd_m8}

3: 栅栏你都过不了,就不要进来了
看题目就知道要先用解密栅栏, http://www.qqxiuzi.cn/bianma/zhalanmima.php
将给的密文用栅栏解密,每组字数从 1 开始尝试,每尝试一次就将得到的东西用凯撒解密一次
http://www.zjslove.com/3.decode/kaisa/index.html
最终知道的每组字数为 6
Flag: moctf{y0u_f1nd_1t}



4:base 全家桶

百度了一下 base 全家桶,发现有 base16,base32,base64 这几个,所以用 python 写了一个脚本把给的密文通过 base16->base32->base64 解一下

Py:

```
import base64
s="4D4A4C545332544549354E444F554C4E495A35465556525A4B4A53464F5254564C4159
484134435A4B5934564B595253475658474D554A3548553D3D3D3D3D3D"
a = base64.b16decode(s)
b = base64.b32decode(a)
c = base64.b64decode(b)
print c
```

运行后即可得到 flag

Flag:moctf{Base_Quan_Jia_Tong}

5:奇怪的 16 进制

给了一串的 16 进制数字,尝试着把 16 进制转为 10 进制用 c++写了个脚本…

```
#include <iostream>
#include <string>
#include <ctype.h>
using namespace std;
int power(int a, int b)
{
    int ans=1,i;
    for(i=0;i<b;i++)
        ans *= a;
    return ans;
}
int main()
{
    int sum = 0, cnt = 0;
    string s;
    string x[]={"5a","45","64","6f","63","45","35","57","4f","48",'
    for(int i = 0; i < 24; i++)
    {
        s = x[i];
        cnt = 0;
        sum = 0;
        for(int j=1;j>=0;j--)
        {
            if(s[j] >= 'a' && s[j] <= 'z')
            {
                switch(s[j])
                {
                    case 'a':sum += 10 * power(16,cnt);break;
                    case 'b':sum += 11 * power(16,cnt);break;
                    case 'c':sum += 12 * power(16,cnt);break;
                    case 'd':sum += 13 * power(16,cnt);break;
                    case 'e':sum += 14 * power(16,cnt);break;
                    case 'f':sum += 15 * power(16,cnt);break;
                }
            }
            else
                sum += (s[j] - '0') * power(16,cnt);
            cnt++;
        }
        printf("%c",sum);
    }
    cout << endl;
}
```

运行后得到 ZEdocE5WOHhjMTltYkdFNQ==看着像 base64 编码的字符串,用 python 试了一下得到 dGhpNV8xc19mbGE5,一开始以为是 md5 试了一下发现不行，就又试着用 base64 解

了一次，出现了 thi5_1s_fla9,加上 moctf{}后就过了
Flag:moctf{thi5_1s_fla9}

6:空 word
好像是之前把隐藏字符打开了所以打开后发现并不是应该空 word,
里面有'->'和' ',感觉像是摩斯密码于是试着把'->'替换为'-',' '替换为'.',，解密后得到 6D6F6374667B426C346E6B5F30725F7461623F7D 发现和第 5 题有点像就该了一下第 5 题的代码，运行得到 flag
Flag: moctf{Bl4nk_0r_tab?}

7:一万年的爱有多久
下载下来一个 zip,解压了几次都还没解压出来,百度了一下发现可能是嵌套压缩,所以又百度了一个可以解压嵌套压缩的脚本
Py:

```
import zipfile
import os

for i in range(10000):

    file_list = os.listdir(r'.')
    for file_name in file_list:
        if os.path.splitext(file_name)[1] == '.zip':

            file_zip = zipfile.ZipFile(file_name, 'r')
            for file in file_zip.namelist():
                file_zip.extract(file, r'.')
            file_zip.close()
            os.remove(file_name)
```

把压缩包和 py 脚本放的统一路径下运行脚本就好了,得到一个 falg 文件用 notepa++打开后得到 falg
Flag: moctf{Just_a_few_minutes}

8:Hacker!!!
下载下来一个数据包,一开始打开看了一下里面好多 sql 注入语句,还给会长博客的地址,以为真的要 sql 注入,可是并不会 sql 注入就把这个题放一边,后面又仔细看了一下那些 sql 语句,发现了规律,包的名字是 http,于是过滤掉了其他的协议只看 http 发现每条语句都有 ascii 这个字符串,后面的数字也会改变，1,1））='109，109 对应的刚好是'm'于是就把每组最后一个数字保存下来
109 111 99 116 102 123 72 116 116 112 95 49 115 95 100 52 110 103 51 114 73 48 117 53 125
输出对应的字符即可
Flag: moctf{Http_1s_d4ng3rl0u5}

```
),1,1))='93 HT
),1,1))='94 HT
),1,1))='95 HT
),1,1))='96 HT
),1,1))='97 HT
),1,1))='98 HT
),1,1))='99 HT
),1,1))='100 H
),1,1))='101 H
),1,1))='102 H
),1,1))='103 H
),1,1))='104 H
),1,1))='105 H
),1,1))='106 H
),1,1))='107 H
),1,1))='108 H
),1,1))='109 H
),2,1))='32 HT
),2,1))='33 HT
),2,1))='34 HT
),2,1))='35 HT
),2,1))='36 HT
),2,1))='37 HT
),2,1))='38 HT
),2,1))='39 HT
),2,1))='40 HT
),2,1))='41 HT
```

9:李华的疑惑

下载下来后有一个加密压缩包和一个 txt 文件，打开 txt 文件发现里面全都是数字，

每一行都是由 3 个数字组成,几乎都是 255,255,255,总共有 22500 行，百度了一下 255,255,255 ,第一条就是关于 255,255,255 是什么颜色，就想到这个可能是一张图，总共 22500 行（150*150），于是就百度了一个可以把这些数字转为图片的 py 脚本，
http://www.wangchao.net.cn/it/detail_352026.html
Py:

```
#-*- coding:utf-8 -*-
from PIL import Image
x = 150
y = 150
Image = Image.new("RGB",(x,y))
f = open('password.txt')
for i in range(0,x):
    for j in range(0,y):
        l = f.readline()
        r = l.split(",")
        Image.putpixel((i,j),(int(r[0]),int(r[1]),int(r[2])))
```

Image.save('password.jpg')得到一张有 key 的图为 PPPPPPass_word,打开压缩包的 txt 发现一个有点像 base64 编码的密文，可是 base64 解码没用，没办法只能到这些解密网站一个一个的试不同的解密方法，终于试出来是 aes 加密得到 flag
Flag: moctf{D0_You_1ik3_tO_pAinH_wi4h_pi8e1}

WEB

1:是时候让你手指锻炼一下了
F 发现要点击 108000 次才可能会个 falg,于是用鼠标自带鼠标宏试了一下,发现点击 108000 次还是可以的但是点击完 108000 次后页面并没有提示而是回到的 0/108000,,f12 看了下源码发现 falg
Flag:moctf{Here_Is_Your_Surprise}

REVERSE

1:easyre
下载下来一个没有后缀的文件,试着用 ida 打开,发现可以查看源码,直接选择主函数 f5 查看伪代码

IDA View-A | Pseudocode-A | Hex View-1

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char v4; // [sp+0h] [bp-70h]@1
  int v5; // [sp+6Ch] [bp-4h]@1

  v5 = 0;
  printf("input your flag:  ", argv, envp);
  __isoc99_scanf("%s", &v4);
  v5 = getflag(&v4);
  if ( !v5 )
    puts("The flag has been told you");
  return 0;
}
```

发现了一个 getflag 函数

```
signed __int64 __fastcall getflag(char *a1)
{
  signed __int64 result; // rax@2
  char *s1; // [sp+8h] [bp-78h]@1
  char dest[8]; // [sp+10h] [bp-70h]@1
  char v4; // [sp+18h] [bp-68h]@1
  int v5; // [sp+70h] [bp-10h]@1

  s1 = a1;
  *(_QWORD *)dest = 135679969554285LL;
  memset(&v4, 0, 0x58uLL);
  v5 = 0;
  strcat(dest, acc);
  strcat(dest, add);
  *(_WORD *)&dest[strlen(dest)] = 45;
  strcat(dest, abb);
  *(_WORD *)&dest[strlen(dest)] = 125;
  if ( !strcmp(s1, dest) )
  {
    printf("great~", dest);
    result = 1LL;
  }
  else
  {
    result = 0LL;
  }
  return result;
}
```

发现了几个可疑的数字尝试用了一下 r 键得到了“{ftcom” “-” “}”
分析了一下代码 falg 还要拼接上 acc,add,abb,但是提交了还是不对,用 shift+f12 查看了一下字符串,发现了 3 个还没看过的字符串

```
Sign-in
desk
english?
```

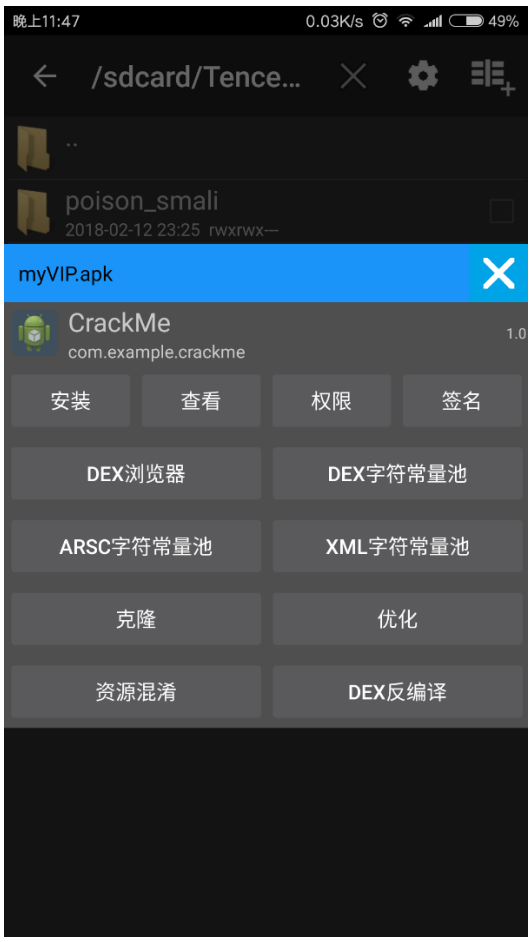
发现 3 个字符串分别对应 acc,add,abb 于是替换提交 falg 通过

Flag: moctf{Sign-indesk-english?}

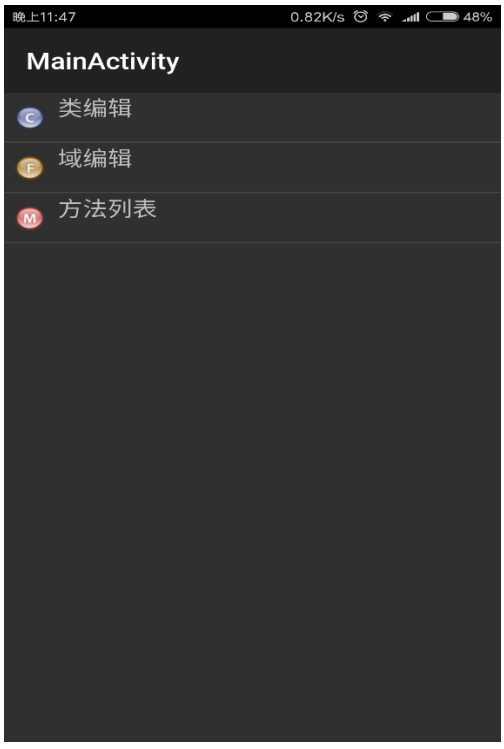
2:我的 vip 呢,那么大个的 vip
电脑上用 AndroidKiller V1.3.1 查看了一下 apk 的源码，
主要函数的源码为

```
switch (paramView.getId())
{
default:
  return;
case 2131296336:
  int i = a();
  paramView = new AlertDialog.Builder(this);
  paramView.setTitle("激活vip");
  if (i < 30)
  {
    paramView.setMessage("目前你拥有积分：" + i + ",你的积分不够啊，当然，你不一定要用积分");
    paramView.setNegativeButton("好吧", new a(this));
  }
  for (;;)
  {
    paramView.show();
    return;
    paramView.setMessage("成为vip用户需要消耗30点积分哦，决定了吗？");
    paramView.setPositiveButton("升级", new b(this));
    paramView.setNegativeButton("退出", new c(this));
  }
}
startActivity(new Intent(this, VipFunction.class));
```

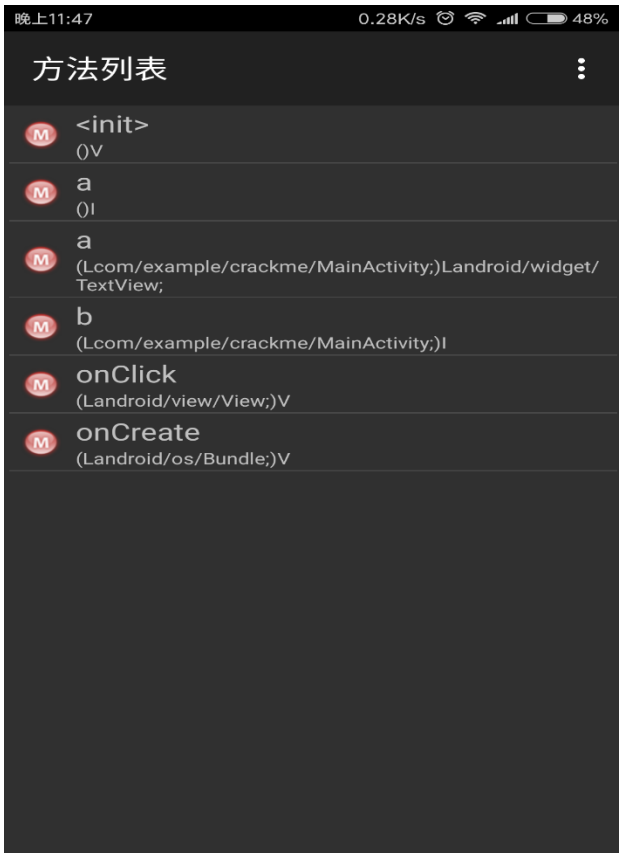
可以知道只要修改升级 vip 的积分点数即可，即把 30 修改为-1，但是苦于不会再电脑上修改耽搁了好久，终于发现了一款可以直接在安卓手机上一些的修改器 apkcrack,操作过程
选择 DEX 浏览器



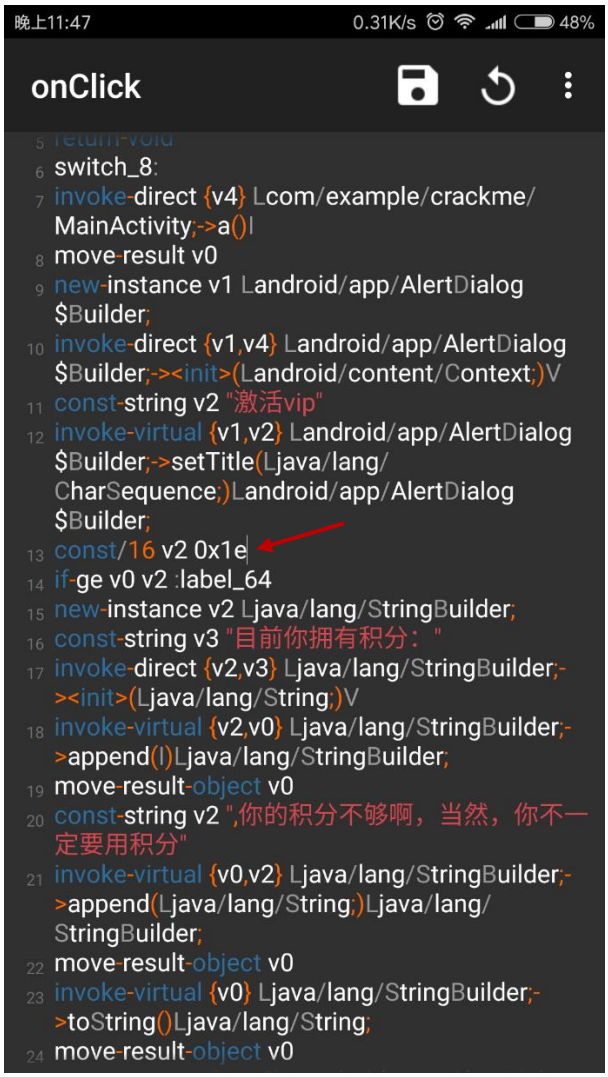
找到主要函数的位置选择方法列表



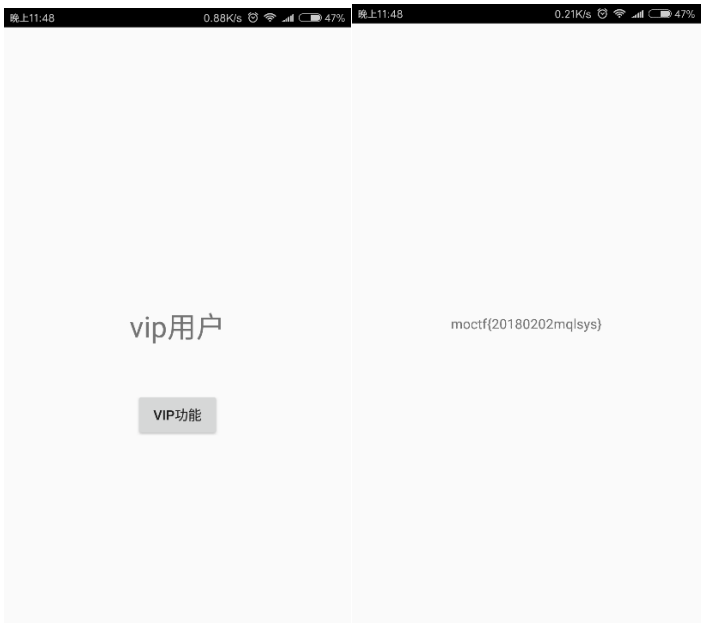
选择 onClick



修改红色箭头所指的位置为 0x-1,然后点击保存



最后安装修改后的 apk 文件，发现可以直接激活 vip 获得 falg



Flag:moctf{20180202mqlsys}

3:哇,有毒吧

这次用 apktool box 的 jadx 工具查看 apk 源码
主要函数代码

```
public void check(String name, String pass) {
    if (name.equals("MQLSY_s") && pass.equals("66666")) {
        Toast.makeText(this, "bW9jdGZ7dGhlX0NURl9JU18/fQ==", 0).show();
    } else if (name.equals("mqlsys") && pass.equals("23333")) {
        Toast.makeText(this, "bW9jdGZ7ZmFsc2U/fQ==", 0).show();
    } else if (name.equals(BuildConfig.FLAVOR) && pass.equals(BuildConfig.FLAVOR)) {
        Toast.makeText(this, "\u54c7\uff0c\u8fd9\u4f60\u90fd\u6562\u5c1d\u8bd5\uff0c\u5389\u5bb3\u5389\u5bb3", 0).show();
    } else if (name.equals("MQL") && pass.equals("2018")) {
        Toast.makeText(this, "bW9jdGZ7dGhpc19pc24ndF9mbGFnfQ==", 0).show();
    } else if (name.equals("admin") && pass.equals("admin")) {
        Toast.makeText(this, "\u767b\u5f55\u6210\u529f", 0).show();
    } else if (name.equals("MQL") && pass.equals("666")) {
        Toast.makeText(this, "bW9jdGZ7dHJ1ZT99", 0).show();
    } else {
        Toast.makeText(this, "\u767b\u5f55\u5931\u8d25", 0).show();
    }
}
```

里面有几个 base64 编码的字符串全部解码后为
moctf{the_CTF_IS_?}
moctf{false?}
moctf{this_isn't_flag}
moctf{true?}全部提交试一遍结果第一个直接通过真的有毒；
Flag: moctf{the_CTF_IS_?}