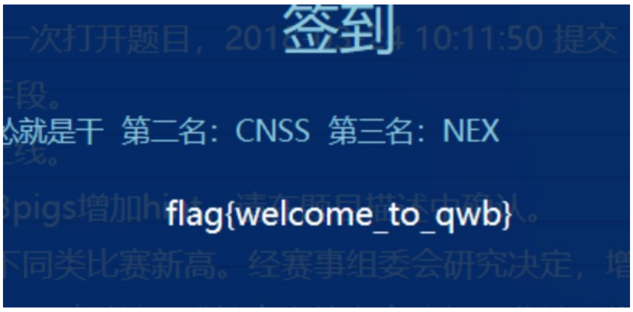
第二届强网杯部分题writeup

转载

weixin_30457465 于 2018-04-11 22:52:00 发布 160 收藏 1
文章标签： php python
原文链接：http://www.cnblogs.com/kagari/p/8799267.html
版权

0x00 题目名称 签到

操作内容：



签到

一次打开题目，201 4 10:11:50 提交

手段。

总就是干 第二名：CNSS 第三名：NEX

线。

3pigs增加h flag{welcome_to_qwb} 。

不同类比赛新高。经赛事组委会研究决定，增

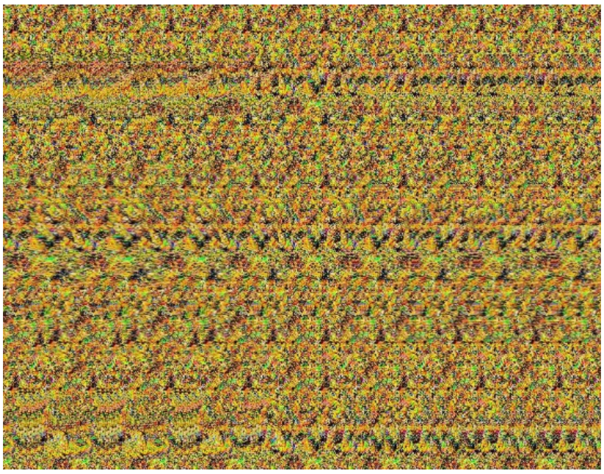
FLAG值：

flag{welcome_to_qwb}

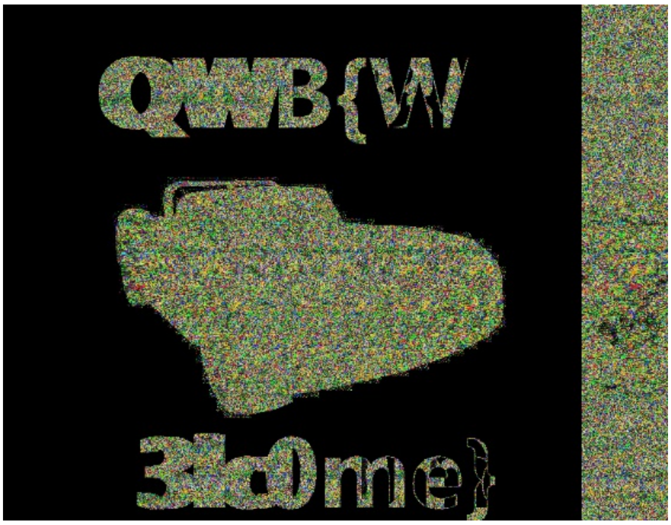
0x01 题目名称 Weclome

操作内容：

通过查看文件发现是一个bmp格式的图片文件，然后加上后缀.bmp，如图



将图片放入色道，通过变换得到flag



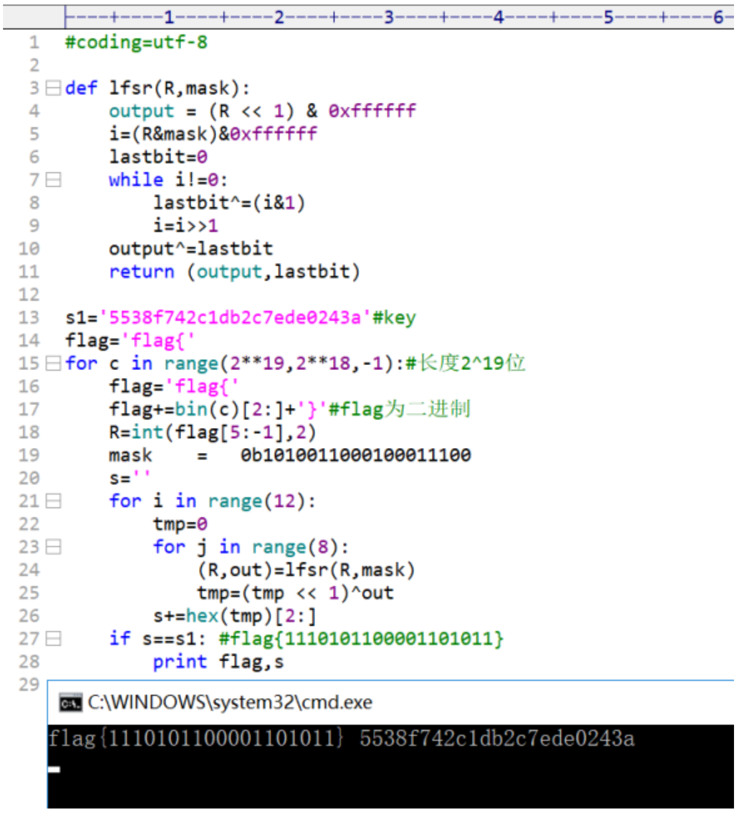
FLAG值：

QWB{W3lc0me}

0x02 题目名称 streamgame1

操作内容：

密码长度不大，暴力破解得到flag



```python
#coding=utf-8

def lfsr(R,mask):
    output = (R << 1) & 0xffffff
    i=(R&mask)&0xffffff
    lastbit=0
    while i!=0:
        lastbit^=(i&1)
        i=i>>1
    output^=lastbit
    return (output,lastbit)

s1='5538f742c1db2c7ede0243a'#key
flag='flag{'
for c in range(2**19,2**18,-1):#长度2^19位
    flag='flag{'
    flag+=bin(c)[2:]+'}'#flag为二进制
    R=int(flag[5:-1],2)
    mask    =   0b1010011000100011100
    s=''
    for i in range(12):
        tmp=0
        for j in range(8):
            (R,out)=lfsr(R,mask)
            tmp=(tmp << 1)^out
        s+=hex(tmp)[2:]
    if s==s1: #flag{1110101100001101011}
        print flag,s
```

C:\WINDOWS\system32\cmd.exe

```
flag{1110101100001101011} 5538f742c1db2c7ede0243a
```

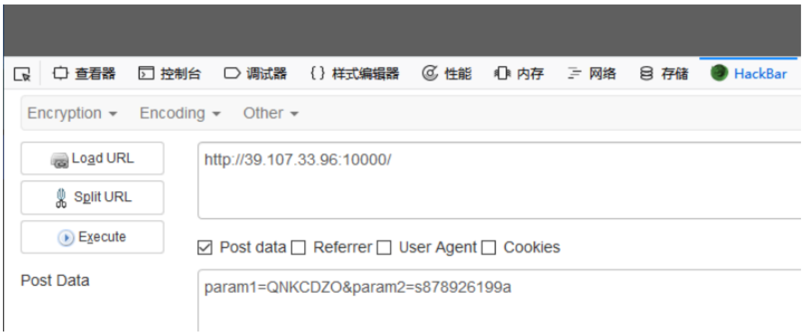
FLAG值：

flag{1110101100001101011}

0x03 题目名称 web签到

操作内容：

第一关利用PHP弱类型



http://39.107.33.96:10000/

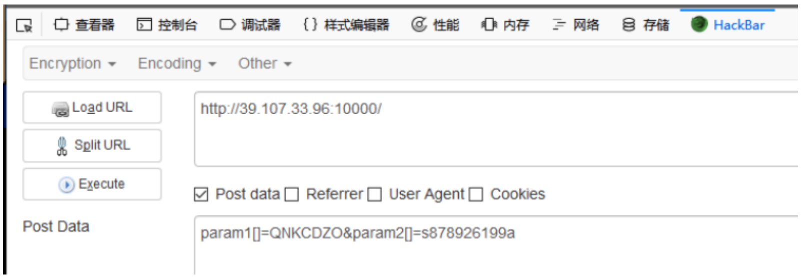
☑ Post data □ Referrer □ User Agent □ Cookies

Post Data

param1=QNKCDZO&param2=s878926199a

Php在处理哈希字符串时候0e开头的都解释为零

第二关利用数组



http://39.107.33.96:10000/

☑ Post data □ Referrer □ User Agent □ Cookies

Post Data

param1[]=QNKCDZO&param2[]=s878926199a

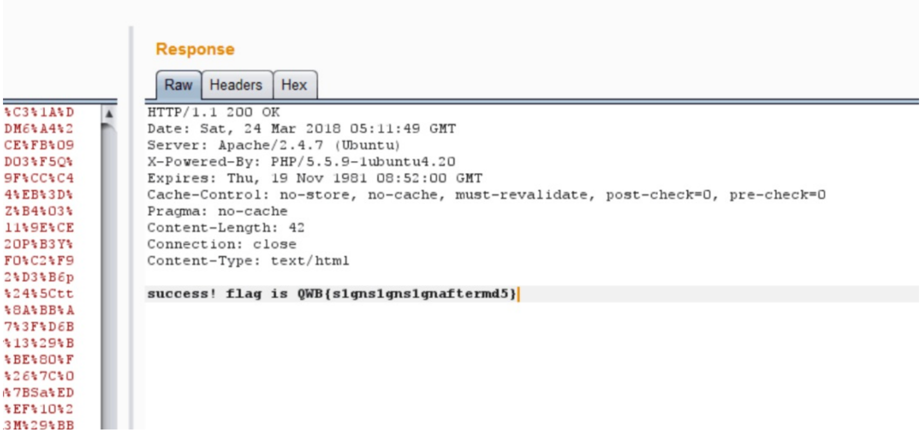
两个数组的md5无法计算数组所以都返回0

第三关

利用如下两个图片md5相同，转为url编码后提交

转换方式为

```
 a=urllib.quote(open("1.jpg","rb").read()[:3200000])


In [7]: with open('1.txt','a') as f:

   ...:     f.write(a)

   ...:


In [8]: b=urllib.quote(open("2.jpg","rb").read()[:3200000])


In [9]: with open('2.txt','a') as f:

   ...:     f.write(b)
```



```
%C3%1A%D
DM6%A4%2
CE%FB%09
D03%F5Q%
9F%CC%C4
4%EB%3D%
Z%B4%03%
11%9E%CE
20P%B3Y%
F0%C2%F9
2%D3%B6p
%24%5Ctt
%8A%BB%A
7%3F%D6B
%13%29%B
%BE%80%F
%26%7C%0
%7BSa%ED
%EF%10%2
3M%29%BB
```

```
HTTP/1.1 200 OK
Date: Sat, 24 Mar 2018 05:11:49 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 42
Connection: close
Content-Type: text/html

success! flag is QWB{s1gns1gns1gnaftermd5}
```

得出flag

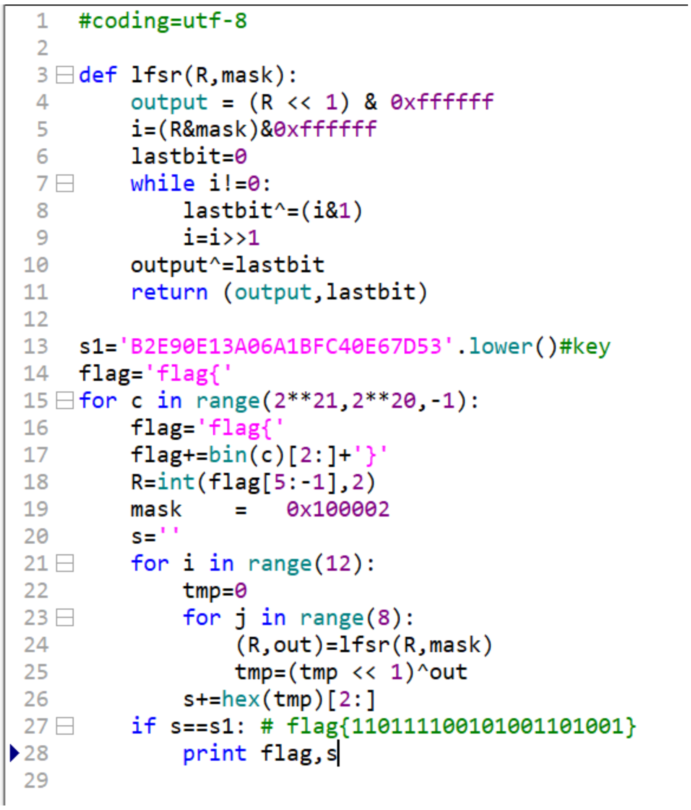
FLAG值：

QWB{s1gns1gns1gnaftermd5}

0x04 题目名称 streamgame2

操作内容：

密码长度不大，暴力破解得到flag



```
#coding=utf-8

def lfsr(R,mask):
    output = (R << 1) & 0xffffff
    i=(R&mask)&0xffffff
    lastbit=0
    while i!=0:
        lastbit^=(i&1)
        i=i>>1
    output^=lastbit
    return (output,lastbit)

s1='B2E90E13A06A1BFC40E67D53'.lower()#key
flag='flag{'
for c in range(2**21,2**20,-1):
    flag='flag{'
    flag+=bin(c)[2:]+'}'
    R=int(flag[5:-1],2)
    mask    =   0x100002
    s=''
    for i in range(12):
        tmp=0
        for j in range(8):
            (R,out)=lfsr(R,mask)
            tmp=(tmp << 1)^out
        s+=hex(tmp)[2:]
    if s==s1: # flag{110111100101001101001}
        print flag,s

```

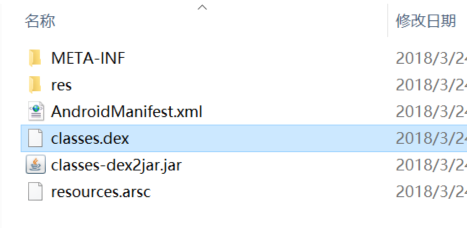
FLAG值：

Flag{110111100101001101001}

0x05 题目名称 simplecheck

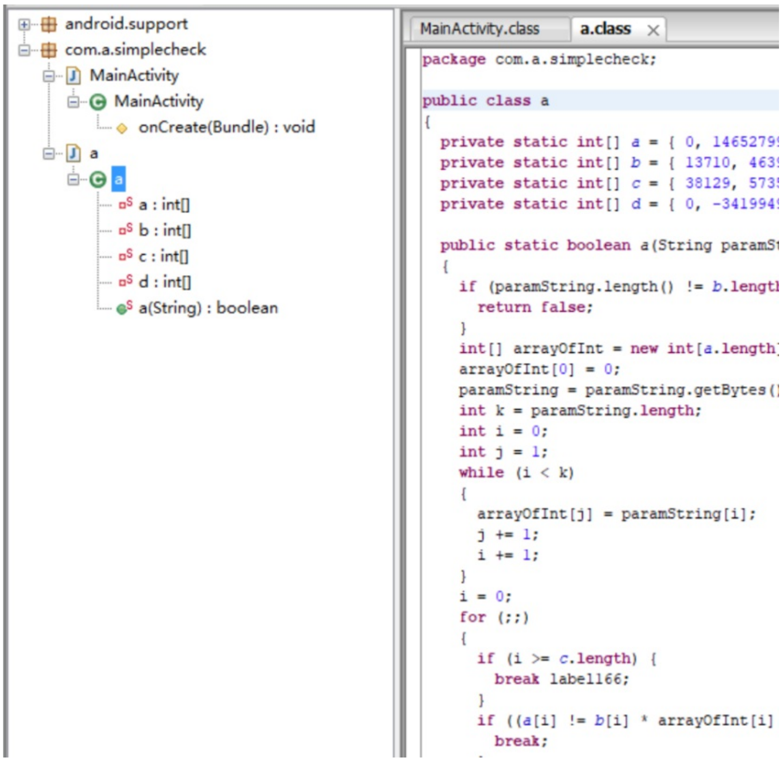
操作内容：

这是一个apk逆向题，360压缩打开apk解压classes.dex，dex2jar.bat转成jar



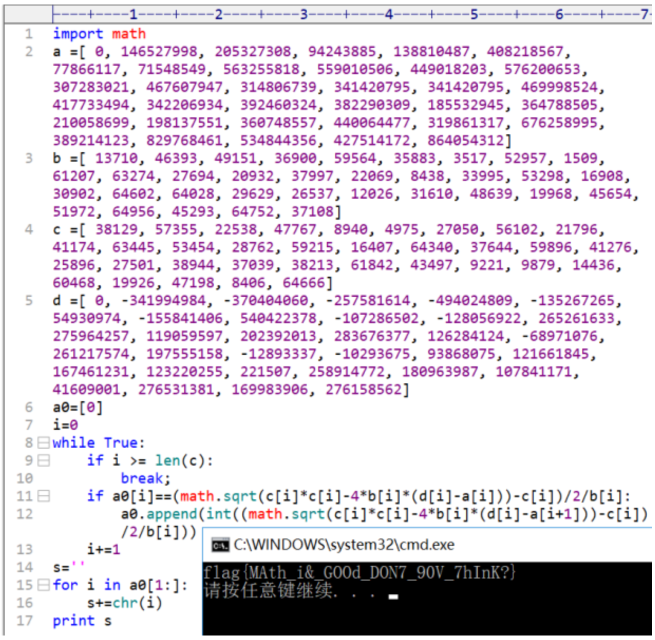
名称	修改日期
META-INF	2018/3/2
res	2018/3/2
AndroidManifest.xml	2018/3/2
classes.dex	2018/3/2
classes-dex2jar.jar	2018/3/2
resources.arsc	2018/3/2

观察到有两个类，其中a类为包含加密方法简单概括就是迭代版的平方差公式



```
package com.a.simplecheck;

public class a
{
  private static int[] a = { 0, 14652799
  private static int[] b = { 13710, 4639
  private static int[] c = { 38129, 5735
  private static int[] d = { 0, -3419949

  public static boolean a(String paramSt
  {
    if (paramString.length() != b.lengtl
      return false;
    }
    int[] arrayOfInt = new int[a.length]
    arrayOfInt[0] = 0;
    paramString = paramString.getBytes()
    int k = paramString.length;
    int i = 0;
    int j = 1;
    while (i < k)
    {
      arrayOfInt[j] = paramString[i];
      j += 1;
      i += 1;
    }
    i = 0;
    for (;;)
    {
      if (i >= c.length) {
        break label166;
      }
      if ((a[i] != b[i] * arrayOfInt[i]
        break;
```

使用python写出解密脚本



```
import math
a =[ 0, 146527998, 205327308, 94243885, 138810487, 408218567,
77866117, 71548549, 563255818, 559010506, 449018203, 576200653,
307283021, 467607947, 314806739, 341420795, 341420795, 469998524,
417733494, 342206934, 392460324, 382290309, 185532945, 364788505,
210058699, 198137551, 360748557, 440064477, 319861317, 676258995,
389214123, 829768461, 534844356, 427514172, 864054312]
b =[ 13710, 46393, 49151, 36900, 59564, 35883, 3517, 52957, 1509,
61207, 63274, 27694, 20932, 37997, 22069, 8438, 33995, 53298, 16908,
30902, 64602, 64028, 29629, 26537, 12026, 31610, 48639, 19968, 45654,
51972, 64956, 45293, 64752, 37108]
c =[ 38129, 57355, 22538, 47767, 8940, 4975, 27050, 56102, 21796,
41174, 63445, 53454, 28762, 59215, 16407, 64340, 37644, 59896, 41276,
25896, 27501, 38944, 37039, 38213, 61842, 43497, 9221, 9879, 14436,
60468, 19926, 47198, 8406, 64666]
d =[ 0, -341994984, -370404060, -257581614, -494024809, -135267265,
54930974, -155841406, 540422378, -107286502, -128056922, 265261633,
275964257, 119059597, 202392013, 283676377, 126284124, -68971076,
261217574, 197555158, -12893337, -10293675, 93868075, 121661845,
167461231, 123220255, 221507, 258914772, 180963987, 107841171,
41609001, 276531381, 169983906, 276158562]
a0=[0]
i=0
while True:
    if i >= len(c):
        break;
    if a0[i]==(math.sqrt(c[i]*c[i]-4*b[i]*(d[i]-a[i]))-c[i])/2/b[i]:
        a0.append(int((math.sqrt(c[i]*c[i]-4*b[i]*(d[i]-a[i+1]))-c[i])
        /2/b[i]))
    i+=1
s=''
for i in a0[1:]:
    s+=chr(i)
print s
```

```
flag{MAth_i&_GOOd_DON7_90V_7hInK?}
请按任意键继续. . .
```

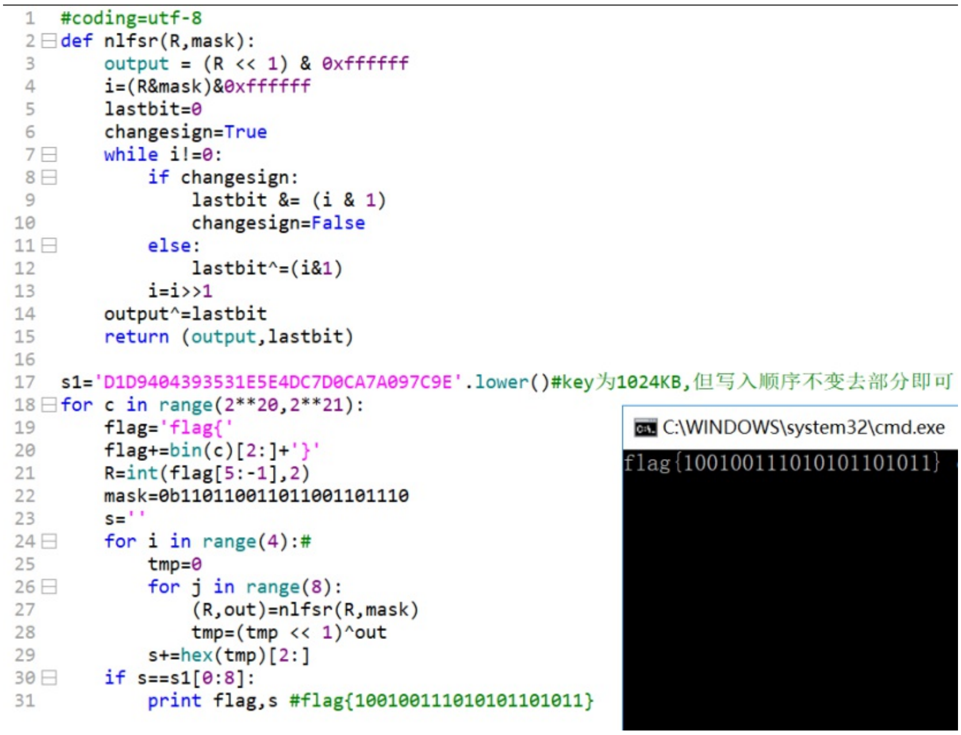
FLAG值：

flag{MAth_i&_GOOd_DON7_90V_7hInK?}

0x06 题目名称 streamgame4

操作内容：

密码不长，加密后去部分进行破解



```python
#coding=utf-8
def nlfsr(R,mask):
    output = (R << 1) & 0xffffff
    i=(R&mask)&0xffffff
    lastbit=0
    changesign=True
    while i!=0:
        if changesign:
            lastbit &= (i & 1)
            changesign=False
        else:
            lastbit^=(i&1)
        i=i>>1
    output^=lastbit
    return (output,lastbit)

s1='D1D9404393531E5E4DC7D0CA7A097C9E'.lower()#key为1024KB,但写入顺序不变去部分即可
for c in range(2**20,2**21):
    flag='flag{'
    flag+=bin(c)[2:]+'}'
    R=int(flag[5:-1],2)
    mask=0b110110011011001101110
    s=''
    for i in range(4):#
        tmp=0
        for j in range(8):
            (R,out)=nlfsr(R,mask)
            tmp=(tmp << 1)^out
        s+=hex(tmp)[2:]
    if s==s1[0:8]:
        print flag,s #flag{100100111010101101011}
```

```
flag{100100111010101101011}
```

FLAG值：

flag{100100111010101101011}

转载于:https://www.cnblogs.com/kagari/p/8799267.html