CnHongKeCTF By 天璇

Web

爆破

```
import requests
import hashlib
url="http://121.237.133.157:20183/result.php"
headers={
    "Cookie":'session=c4d984ac-4757-4e06-953f-c9eb0c74193c'
}
for i in range(0,9):
    for j in range(0,9):
        for q in range(0,9):
            for k in range(0,9):
                i=str(i)
                j=str(j)
                q=str(q)
                k=str(k)
                a=str(i+j+q+k)
                t=hashlib.md5(a.encode('utf-8')).hexdigest()
                data={
                    'number':a,
                    'sign':str(t)
                }
                req=requests.post(url=url,headers=headers,data=data)
                print(a)
                if 'Bad' not in req.text:
                    print(a)
                    print(req.text)
```

```
3681
{ "flag" : "CnHongKe{a4b85141cc4341b59d52ff8150c57d7b}
" }
3682
```

Misc

Picture

Stegsolve改色道，挨个扫描即可 拼接就是flag

What's this

一个邮件发送包，正文部分是base64。
PNG，打开看有第二部分flag
前面有Quoted-Printable 里面GBK2312编码有一段，

最前面还有一小段Base64
有flag的开头。
组合就是flag

Cry

随便选两个Round的第二个数构造一个$a-b=(y_a-y_b)p$再和n求GCD即可得出p
~~题目附件有问题~~

```
a =
643589808109831206919328234179591554026124059809749057227111749040437689330460800424243942931206795187280460675759460366430172654146922998015787222989782597976018733187194019143564854886058611915569783145503336546231380867908138879395210171706016651896401473392042420379329349589828280175940543607255416772431728188653211
b =
261315212680123535760592640960755534363410891402744507142444256312660247731491341886153489405950326962087633021595312088948475492419378424024250157114471058142432998359750390514073255663090419344757882820322385621977539795923490230800414008808550178933205114088238041973428933548863596024436580795007856828202834341070758 9
n =
182304750222411071115020096381448463264626974447939775221627551403920287756303331396715704139683000556096247329050175764923184810497657193951781019172590789504914784046192129307129621763704747934582645424281744116489843854964155158884502364926391036558379687589120011278812980143738334920440544475383687773519594728281034905235194024997946255095447462248491313583914278032746607273650083343215151279139632676715536711335119566267490270633486847000621452143358684630588030669366469581274718455392765939627080444064905929984142736672320175305027129471658329178267534793383154501934495535068303992230364332136906351280 87
p = GCD(a - b, n)


e = 65537
c =
150011753196109467952223439240354875340085847094618782261438999064488438501207799284209444324650297857529710336891990658704083517941559454466865247005334705629911723846677100594518050090083054248056705960389117476457843295327866263243977784129577264956834227665221907461321885709469963323827870960325203480159145348373889164341881117444522807968339696382205564028552506731168131359212445909312784057852335810547164104170940164434031622802101047933019555691992645276684875399685064019744019951826911105453679151211986056420216034733761244008938815872086597174580334854220583047531620147715661563328109285027068041887 37
q = n // p
print(long_to_bytes(pow(c, inverse(e, (p - 1)*(q - 1)), n)))


'''
b'CnHongKe{11b1df76}'
'''
```

APK

Toosimple

```
int v0; // r0
int v1; // r1
int i; // r3
char v3; // r5
int v4; // r3
_BYTE *result; // r0
char v6[24]; // [sp+4h] [bp-2Ch] BYREF

memcpy(v6, "SCKLS3f;j&Bpa9zl[mWu60", 0x16u);
v0 = 11;
v1 = 1;
for ( i = 0; i != 21; ++i )
{
  v3 = v6[i];
  if ( i > 10 )
    v6[i] = v3 - v0--;
  else
    v6[i] = v3 + v1++;
}
v4 = 0;
result = string;
do
{
  string[v4] = v6[v4];
  ++v4;
}
while ( v4 != 22 );
string[23] = 0;
return result;
}
```

直接计算出Key就行

```c
#include <stdio.h>
#include <stdlib.h>>
int main()
{
    int v0; // r0
    int v1; // r1
    int i; // r3
    char v3; // r5
    int v4; // r3

    char v6[24] = "SCKLS3f;j&Bpa9zl[mWu60";
    v0 = 11;
    v1 = 1;
    for ( i = 0; i != 21; ++i )
    {
        v3 = v6[i];
        if ( i > 10 )
            v6[i] = v3 - v0--;
        else
        v6[i] = v3 + v1++;
    }
    v4 = 0;
    for(v4 = 0;v4 < 22;v4 ++){
        printf("%c",v6[v4]);
    }
    return 0;
}
```

Crackme2

```java
    @Override  // android.view.View$OnClickListener
    public void onClick(View arg26) {
        String name3 = ((EditText)HelloAndroid.this.findViewById(0x7F050004)).getText().toString();  // id:txt_name
        int name3lenght = name3.length();
        String name4 = "";
        String serial_entered = ((EditText)HelloAndroid.this.findViewById(0x7F050006)).getText().toString();  // id:txt_serial
        if(name3lenght >= 4) {
            goto label_31;
        }

        try {
            Toast.makeText(HelloAndroid.this.getApplicationContext(), "Min 4 chars", 1).show();
            return;
        label_31:
            int i;
            for(i = 0; true; ++i) {
                if(i >= name3.length()) {
                    String v12_1 = String.valueOf(Integer.parseInt(name4.substring(0, 5)) ^ 0x6B016);
                    TelephonyManager mTelephonyMgr = (TelephonyManager)HelloAndroid.this.getSystemService("phone");
                    String imei2 = mTelephonyMgr.getDeviceId();
                    String simsn = mTelephonyMgr.getSimSerialNumber();
                    String temp02 = imei2.substring(0, 6);
                    if(String.valueOf(v12_1) + "-" + String.valueOf(((long)(Integer.parseInt(temp02) ^ Integer.parseInt(simsn.substring(0, 6))))) + "-" + temp02.equals(serial_entered)) {
                        Toast.makeText(HelloAndroid.this.getApplicationContext(), "God boy", 1).show();
                        return;
                    }

                    Toast.makeText(HelloAndroid.this.getApplicationContext(), "Bad boy ", 1).show();
                    return;
                }

                int j = name3.charAt(i);
                name4 = String.valueOf(name4) + j;
            }
        }
        catch(Exception v22) {
            Toast.makeText(HelloAndroid.this.getApplicationContext(), "Another Error Ocurred :(", 1).show();
            return;
        }
    }
```

逻辑很简单，用户名test
获取设备ID和SIM序列号取前6位，然后进行一系列异或后串成一个xxx-xxx-xxx格式的序列号作为解锁码

直接使用主办方给出的设备ID和SIM序列号，异或后得到序列号