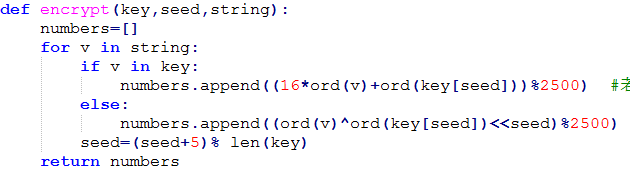
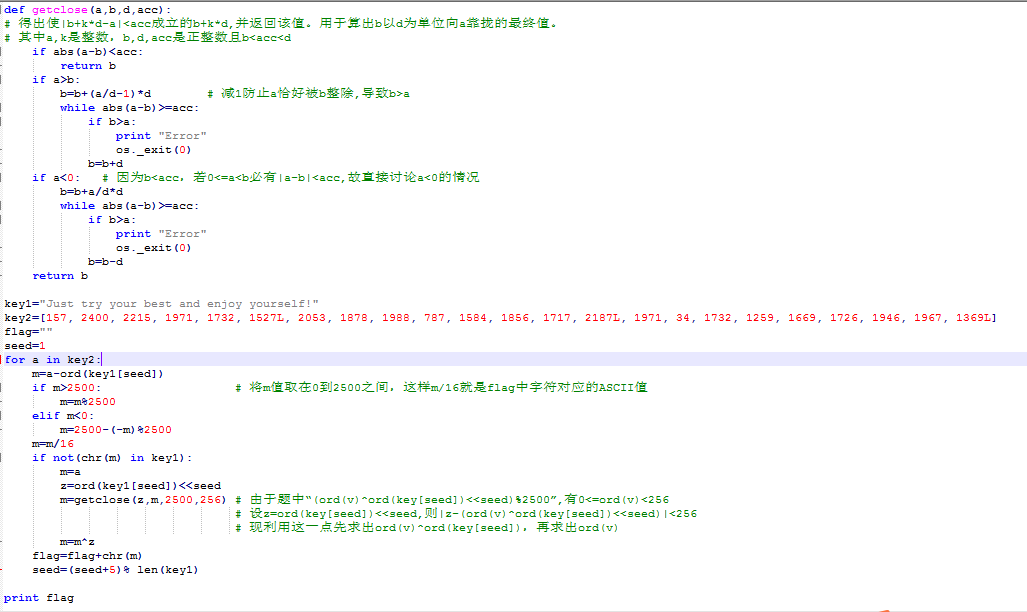
1. 小菜一碟

* 题目描述：这么简单的题目对你来说一定是小菜一碟吧~快来试试看！
* 分值：100分
* Flag：whctf{you\_are\_the\_best}
* 程序流程: 获得用户输入，然后encrypt处理用户输入和key1，处理后和预留数据(key2)比较，只有输入flag才能得到正确的key2.

encrypt算法如下:



分析程序, 得到, key1="Just try your best and enjoy yourself!" ; seed = 1 然后写encrypt算法的逆算法就可以, 当然按位爆破也可以= =



1. Crackme

* 题目描述：CrackMe，你可以的！
* 分值：200分
* Flag：whctf{$CrackersBABCCC37D8AD08C}
* 程序流程：

Name的正确输入为”Welcome2HUSTCrackers”（20 bytes,长度验证）。

对name的后8字符（“Crackers”，命名为temp1Str）进行hash（APHash），得到的hash值为unsigned int（32 bit），转化为十六进制的字符hash1Str。

Temp2Str = temp1Str | hash1Str。

然后对temp2Str进行BKDRHASH，得到的hash值再转化为字符串hash2Str。

最终resulStr = temp2Str | hash2Str，即为serial。

动态调试，找到字符串对比函数，再根据堆栈的地址可以找到正确输入计算得到的结果，字符串CrackersBABCCC37D8AD08C。注意flag格式……

1. 坐标定位

* 题目描述：快看，UFO！我要立刻向总部报告位置。
* 分值：200分
* Flag：whctf{30-30-55-114-25-6}
* 程序流程：

该APK文件安装后，需要用户输入特定的密码，输入正确会显示破解成功。该APK文件没有太多的保护，可以直接使用各种分析工具（如android killer等）反编译得到Java代码。

直接采用jd-gui会发现getTableFromPic()，getPwdFromPic()的smali代码无法正确转化，所以直接进行阅读。

获得正确注册码的代码逻辑为：

1. 从logo.png这张图片的偏移0x738d5处，读取一个映射表，768字节编码成UTF-8，即256个中文表

2. 从偏移0x73be0处读取51个字节编码的UTF-8（即17个中文字符）为最终比较的密码。然后通过输入的字符的转换，转换规则就是ASCII字符编码，去比较是否和最终密码相等。

1. 我讨厌数学

* 题目描述：数学没学好，你能帮我解出这道题么？
* 分值：200分
* Flag：whctf{Y0u\_ar3\_g00d\_a7\_m4th}
* 程序流程：

将用户输入转换成 6\*6 的矩阵A，不够的位数补1，然后求 A\*AT，得到结果矩阵C，与预留矩阵比对。相等则判定正确。

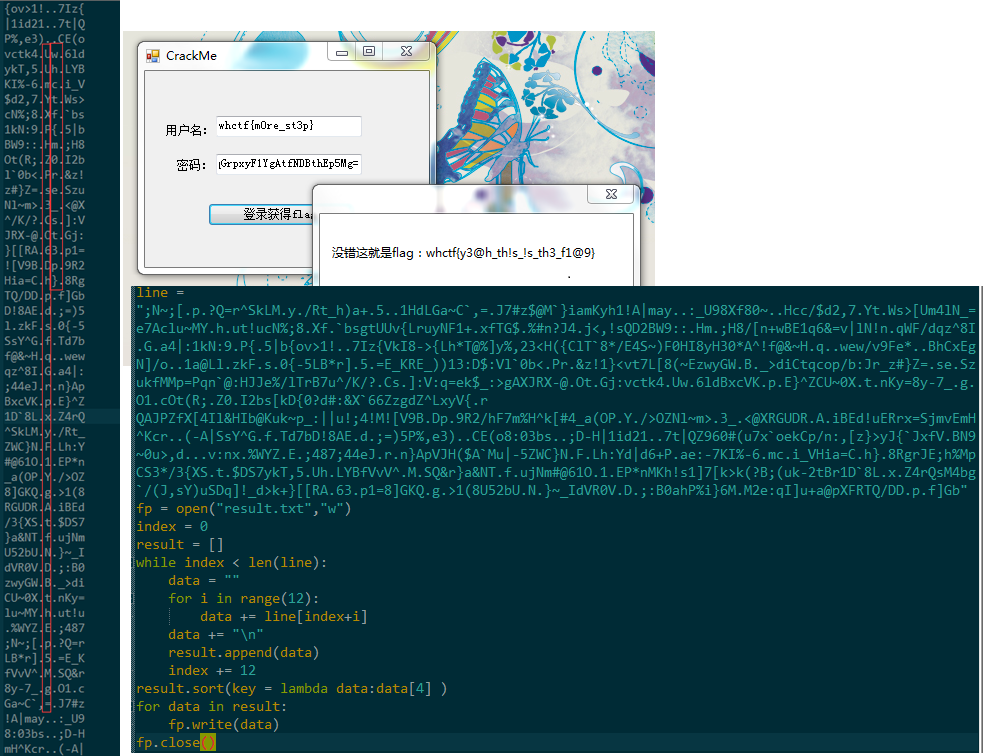
分析算法，发现一些限定条件：flag位数为27位，即矩阵的后9个数为1（数字1）；flag格式为whctf{……}，得到基础矩阵A。然后求解方程组。最后根据ascii码表转换得到flag。当然，按位爆破还是可以的……为啥都这么暴力呢……

1. 猜猜看

* 题目描述：这就是描述，hahahhahaha
* 分值：200分
* Flag：whctf{y3@h\_th!s\_!s\_th3\_f1@9}
* 程序流程：
* 图片解压得到exe。随便输入数据，登录显示乱码。

使用ILSpy逆向源码看到用户名和密码使用des加密获得最终结果，然而是自己验证自己。所以说用户名和密码并不是自己构造出来的。

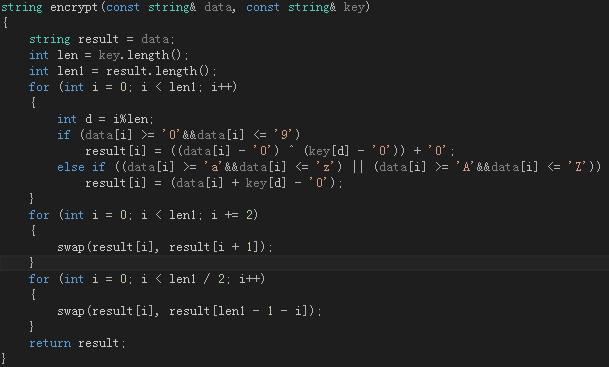
Tips中提到乱码有用、十二五、栅栏。使用栅栏解密，将乱码按12个字符分割，依次排列之后。每一行数据按照第5列的大小排序。之后可以得到格式化数据。



1. 来华科

* 题目描述：你要来华科咱们就去毛主席像下集合
* 分值：300分
* Flag：whctf{@38bb4b54f254d23e30?ce79cda52!7f}
* 程序流程：
* 图片中隐藏了一个exe，一个pyc，其中pyc是加密的。

抠出exe程序，之后逆向，可以看出加密算法的思路。加密算法源码如下：



Tips中提到7位数字与指定地名华科南大门毛主席像。可查看该地名坐标1144305作为key。解密得到data原始数据。

使用明文作为密码解压pyc文件，可以看到有一串字符和很多没用到的函数，使用1144305顺序依次调用这些函数可以得到flag。

