广东省第一届“强网杯” writeup

原创

giantbranch 于 2015-12-01 18:03:48 发布 13652 收藏 3
分类专栏： 信息安全 CTF

广东的没人把pwn和re给做出一道，我们都还刚起步啊

10分签到题：

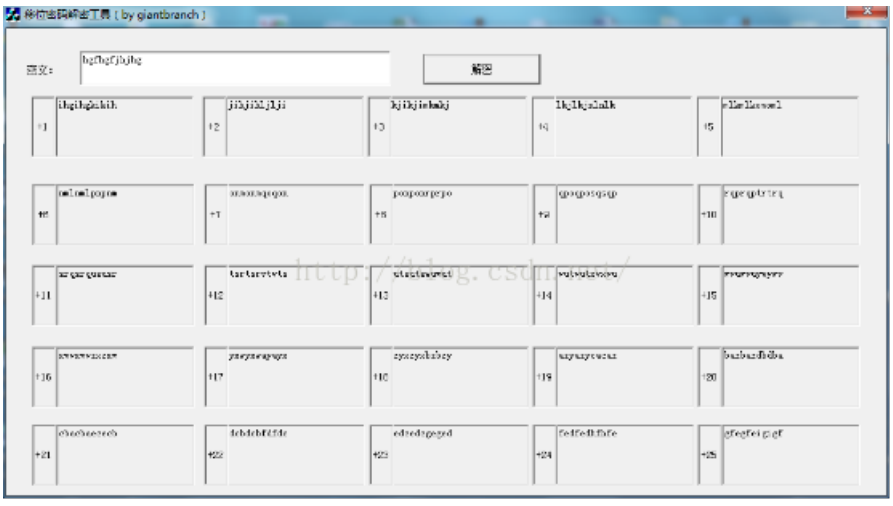
直接复制

管理员常用密码：

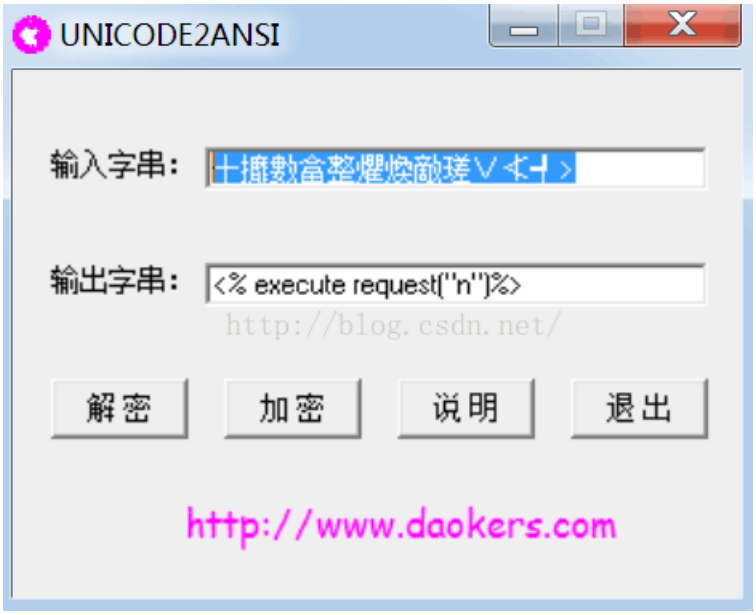
admin

有个移位密码的题

（好像是ROT13吧，反正也是移位）：直接用自己的工具，下面为自己乱打的字符，忘记比赛的密文了



一句话乱码：下了个工具，当然下图的字串不是比赛的字串

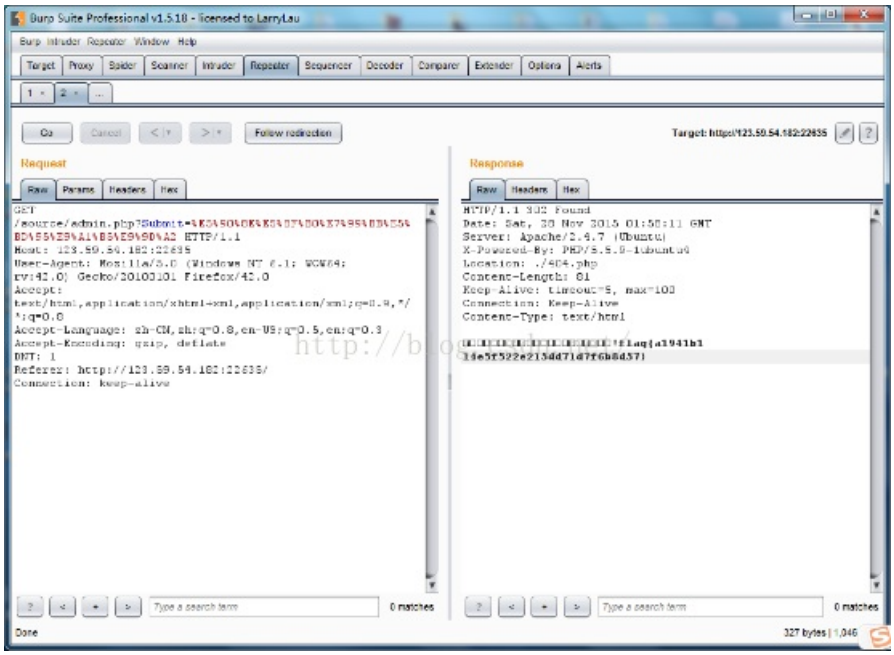


那个js加密的：直接在控制台unescape("")一下

密码被篡改了的：猜是MD5，但一看多了个l，把l去掉再到cmd5解一下就行

彩蛋80：

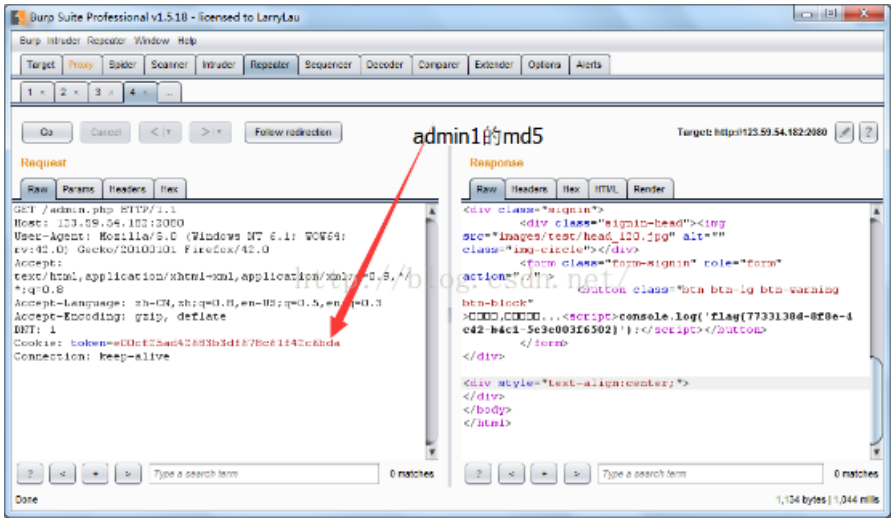
直接brupsuite抓包，发到repeater去，再go即可，右边直接出flag



跳来跳去80：

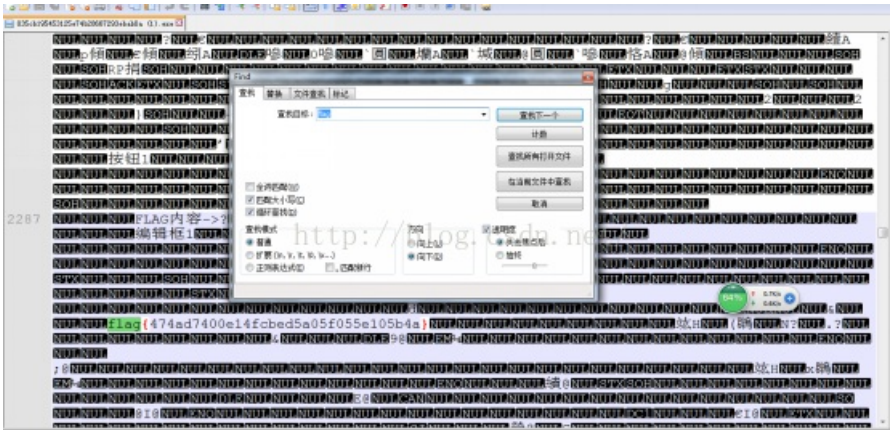
这一题用用burpsuite抓包，发现token都是设置为test2的md5，而且响应包会把token，delete掉，这应该是cookie欺骗，于是就改cookie为md5(admin),不行，又设置md5(admin2)，

最有有个队员说admin1试一下，一试就有，直接出flag



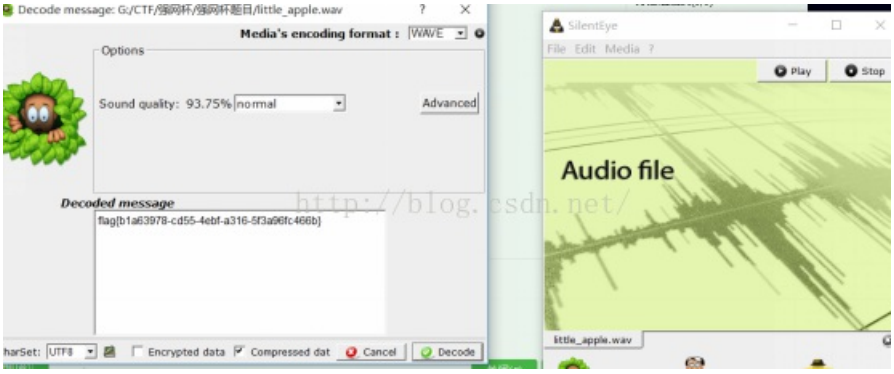
眼前80:

直接notepad++打开，搜一下flag就有



小苹果音频80：

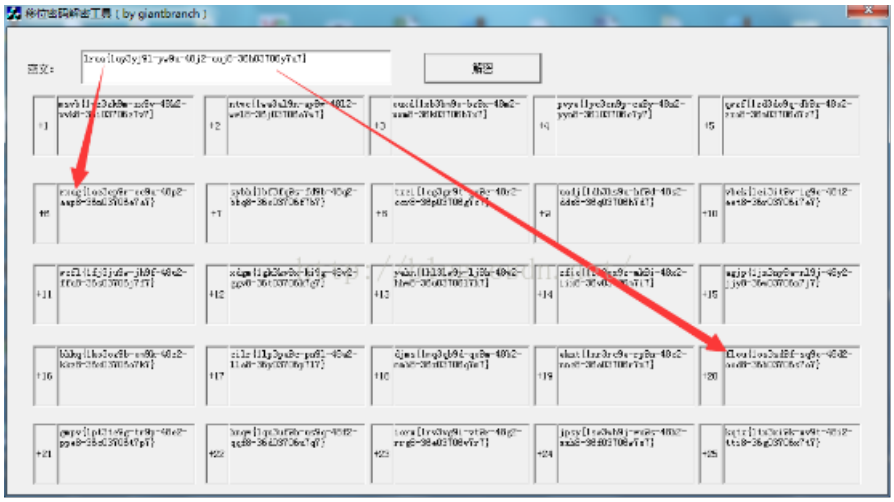
用音频解密软件直接解出flag



经典密码100：

这是一个凯撒密码的变形

再用自己写的软件解一下密，发现fa跟lg分开了。一个+6一个+20（即-6）



首先以为是两个两个隔着来加密，结果不对

就发现l和r是偶数（ASCII码），就+20（-6），u跟a是奇数，就+6

写个脚本

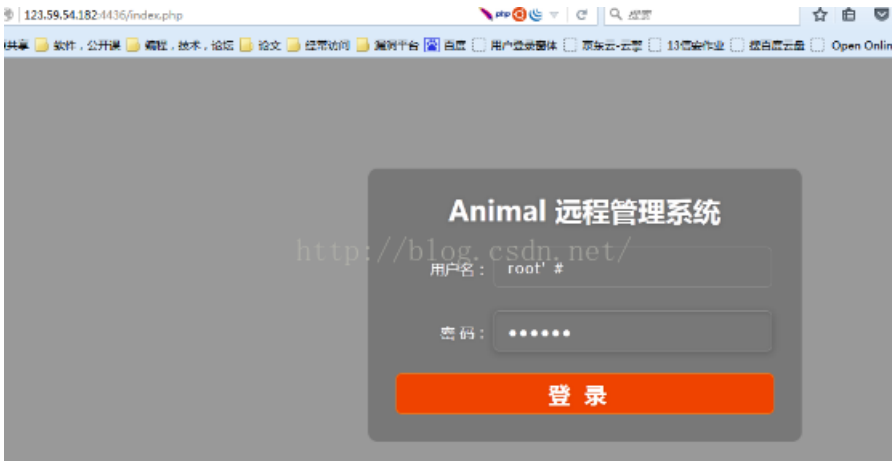
```python
#!/usr/bin/env python

def main() :
    str = "lrua{1uy3yj9l-yw9u-48j2-uuj8-36h03706y7u7}"
    res = ""
    for i in xrange(0, len(str)) :
        i_ch = ord(str[i])
        if (str[i] != "{") and (str[i] != "}") and (str[i] != "-") :
            if (i_ch >= ord('a')) and (i_ch <= ord('z')) :
                if i_ch % 2 != 0 :
                    i_ch = i_ch + 6
                else :
                    i_ch = i_ch - 6
                if i_ch > ord('z') :
                    i_ch = i_ch - ord('z') + ord('a') - 1
                if i_ch < ord('a') :
                    i_ch = i_ch - ord('a') + ord('z') - 1
        res = res + chr(i_ch)
    print res
if __name__ == "__main__" :
    main()
```


直接出flag

远程登陆：

直接注释登陆(密码就可以随便填了)，就有root权限,源代码的提示简直坑爹

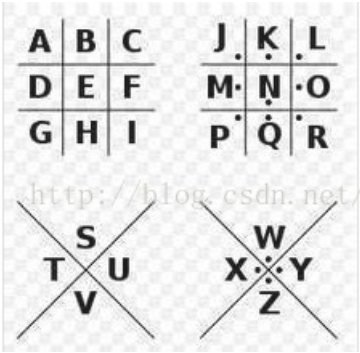


猪圈200：

先base64，再十六进制转化成字符，再base32，再base64

得到ocjp{zkirjwmo-ollj-nmlw-joxi-tmolnrnotvms}

又有个小心猪圈



右边的跟左边的一一对应，在左边的换成右边，右边的换成左边即可得到flag

大黑阔200：

通过提取tcp流（wireshark的follow tcp dump）可得到以下对话：

[{'content':'next week

','stime':'15:37:07'}]

[{'content':'hi

','stime':'15:36:39'}]

content=i am here what?&sender=haiou&geter=haozi

15:36:48

[{'content':'we can go somewhere to have a rest','stime':'15:37:30'}]

[{'content':'where are you going ?','stime':'15:38:05'}]

content=i don't have idea&sender=haiou&geter=haozi

[{'content':'how about tangshang','stime':'15:38:25'}]

content=but i was born in tangshan&sender=haiou&geter=haozi

[{'content':'wow....','stime':'15:38:47'}]

[{'content':'then how about tianyahaijiao','stime':'15:38:57'}]

content=sounds like not bad&sender=haiou&geter=haozi

content=where is that?&sender=haiou&geter=haozi

[{'content':'i ....do not know','stime':'15:39:30'}]

[{'content':'but i can check in my map img','stime':'15:39:43'}]

content=if it is a place with water....&sender=haiou&geter=haozi

[{'content':'then?','stime':'15:40:06'}]

content=i can not swim&sender=haiou&geter=haozi

[{'content':'god....','stime':'15:40:20'}]

[{'content':'then...you dont want go anywhere?','stime':'15:40:38'}]

content=i have no idea&sender=haiou&geter=haozi

[{'content':'how about wangsicong 100?

','stime':'15:41:36'}]

content=what meaning?&sender=haiou&geter=haozi

[{'content':'how about wangsicong 100?','stime':'15:41:52'}]

[{'content':'guominlaogong ','stime':'15:42:05'}]

[{'content':'lol...','stime':'15:42:10'}]

content=what is 100?&sender=haiou&geter=haoziHTTP/1.1 200 OK

[{'content':'his family has alot of building..you know..','stime':'15:42:44'}]

content=yes....&sender=haiou&geter=haozi

content=but i really do not know the way&sender=haiou&geter=haozi

content=canyou show me the way in the map?&sender=haiou&geter=haozi

[{'content':'ok','stime':'15:43:44'}]

[{'content':'upload to me','stime':'15:43:49'}]

content=ok

&sender=haiou&geter=haozi

content=see that?&sender=haiou&geter=haoziHTTP/1.1 200 OK

[{'content':'well! ','stime':'15:44:35'}]

其中序号为8的tcp流还有个传输的文件，还原出来是一个地图

再看看对话，最后有个王思聪100，还有his family has alot of building

那就百度：万达 100，搜到第100家店是昆明西山的万达广场盛大开业

用图形工具处理一下就清楚了一点了

又一个后台：

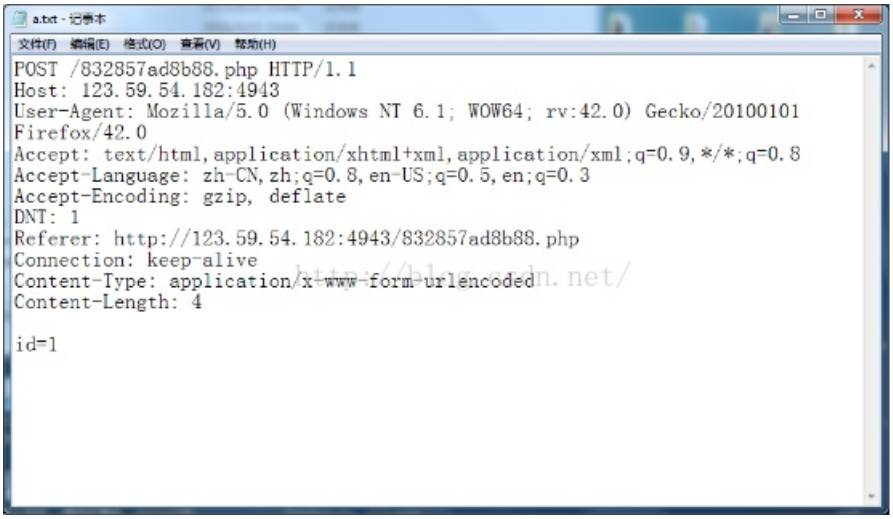
看源码：

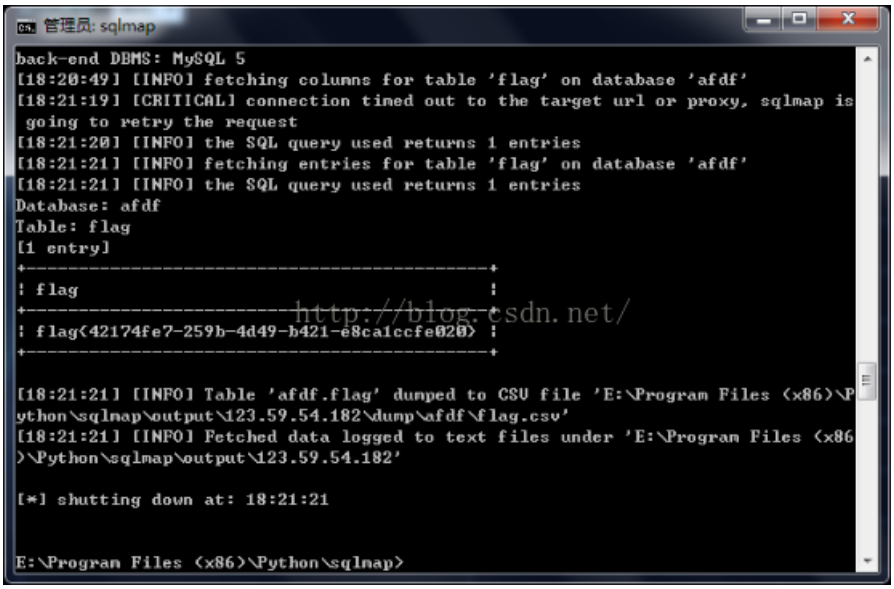
好像做过这题

如果不用数据库，后台直接写等号===的话，完全没法搞，于是就想到之前的题，传个数组进去，后台应该是至直接strcmp判断pass参数，直接得出后台地址，而且他也显示hackmeplease，那个pass参数

看到这个，一看就知道注入

将burpsuite抓到请求信息拿到sqlmap跑即可





单身狗300:

用qq截图把那个正方形把狗覆盖掉（具体可用ps叠上狗那位置），扫一扫，就有了

女神500：

分析下面的图片，从背景的树来看，棕榈树属于南方，故可以锁定在广浙一带。

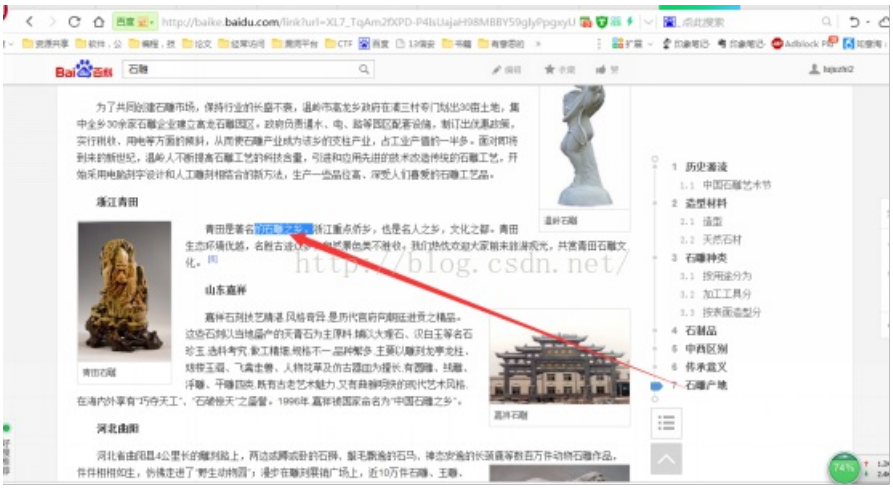
分析背景的广告牌，大致可以看出是石雕

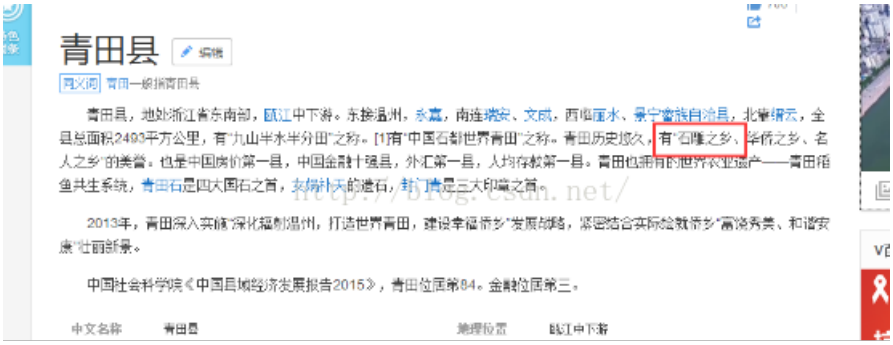
分析天气可以看到是多云，百度一下附近的天气

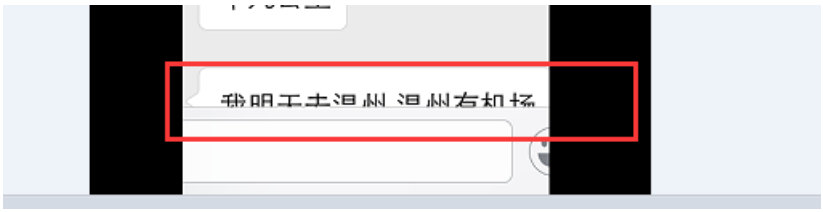
百度石雕，看到所有的石雕产地中，青田离温州最近，下图表明她在温州附近，不然不会去温州的机场而不去其他机场

根据这张图可以推测9.22日 多云的天气，百度了下跟2015年的历史天气，跟那个taxi那张图的背景吻合

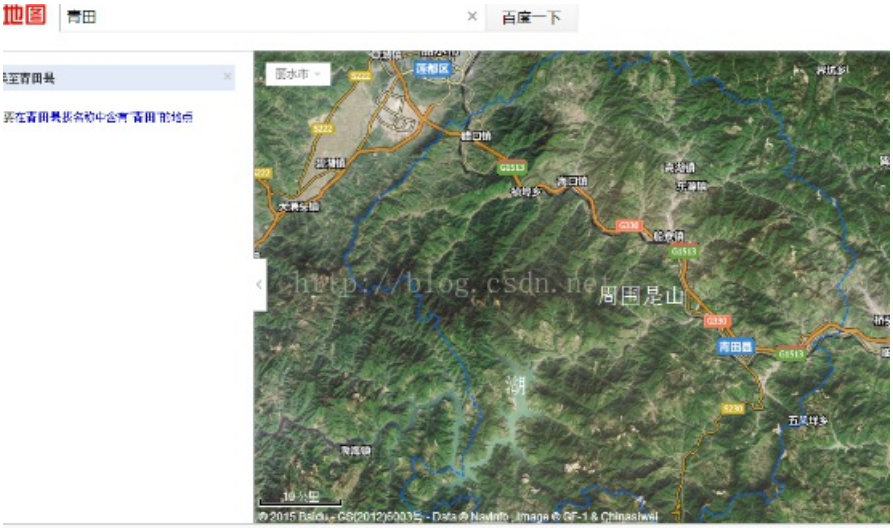
2015-09-03	32	24	雷阵雨	北风	微风
2015-09-04	33	25	雷阵雨转多云	北风	微风
2015-09-05	32	24	雷阵雨转阵雨	北风	微风
2015-09-06	29	21	中雨转多云	北风	微风
2015-09-07	31	22	多云	北风	微风
2015-09-08	32	21	多云转晴	北风	微风
2015-09-09	32	21	多云	北风	微风
2015-09-10	31	20	晴转多云	北风	微风
2015-09-11	32	21	晴转多云	北风	微风
2015-09-12	28	20	阴	北风	微风
2015-09-13	29	21	多云	北风	微风
2015-09-14	26	22	小雨	北风	微风
2015-09-15	24	19	小雨	北风	微风
2015-09-16	29	18	阴转多云	北风	微风
2015-09-17	31	19	晴转多云	北风	微风
2015-09-18	30	20	多云转阴	北风	微风
2015-09-19	26	21	阵雨	北风	微风
2015-09-20	23	20	阵雨转小雨	北风	微风
2015-09-21	24	20	阵雨转阴	北风	微风
2015-09-22	26	20	小雨	北风	微风
2015-09-23	29	22	多云转阴	北风	微风
2015-09-24	31	22	多云转阴	北风	微风
2015-09-25	26	22	小雨	北风	微风





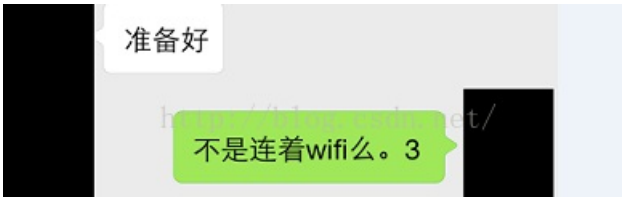


周围是山，有湖符合



再看看手机通知栏的截图，信号不好的话，gps可能有点问题，显示的是北京

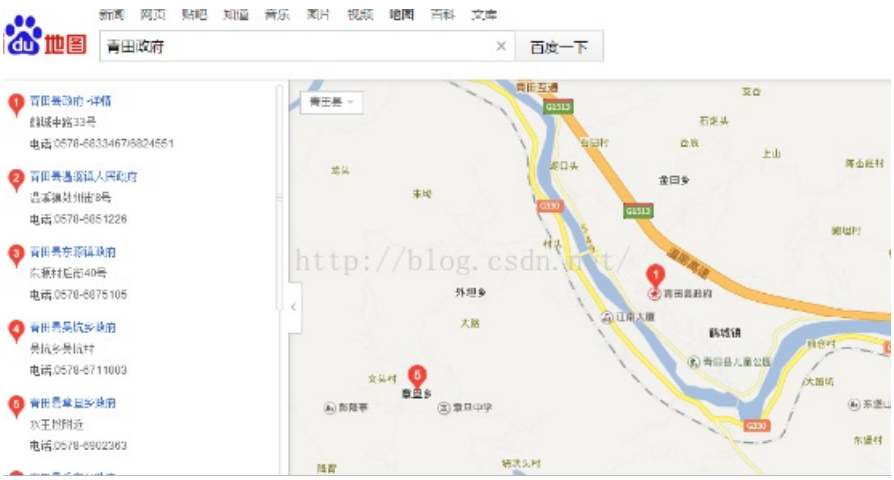
而且手机通知栏截图的主色调是粉红色，应该是女生，就是女神



连接的wifi很可能就是酒店的名称，很多酒店都是这样命名的，可以这样用wifi做广告，何乐而不为呢

对面很热闹，跟着就应该县中心，百度地图一般都把字标在政府那，政府一般都在繁华地区

先找到政府



跟着无意外，女神就在政府对面

因为wifi后两个字母为bg，所以就大胆肯定是宾馆，直接在政府对面百度宾馆

直接在政府对面，沿着江南大道上下寻找，找到了一个青田（qt）皇家（hj）风尚（fs）宾馆（bg），跟wifi名称完全吻合，提交就有了，而且附近也有美发店，房间色调跟女神的拍照的基本一致


宾馆
百度一下
商户免费认证


青田皇家风尚宾馆 详情»
地址： 水南村秦冠路2号
电话： (0578)6065666
3.7 参考价： 158元
详情：去哪儿
到这去
从这出发
在附近找
美发
搜索
酒店 餐馆 银行 医院 公交站


美发
默认排序
有优惠
正在团购
35米
171米
81米
92米