【Writeup】第六季极客大挑战(部分题目)

原创

lymh 于 2015-10-31 22:51:17 发布 5936 收藏 2

分类专栏： 其它记录 文章标签： 网络安全 极客大挑战 CTF Writeup

本文链接：https://blog.csdn.net/lymingha0/article/details/49537977

好久没做CTF题了，一是感觉前几次网赛被虐的够呛，二是各种杂事也越来越多。偶然看到了网上这套成都信息工程大学的练习题，感觉难度上比较适合我这种菜鸟，于是抽空做了一些，然而由于水平和时间原因最终也才完成11/41，这里就记录一下我解出的11道题。以及将来学会的题，也会在后面增加。

Misc (杂项)

签到题

听说关注syclover微博，私信有惊喜呦。

一开始微博加错了，加了个无辜的妹子。。。正确的ID是 @三叶草小组Syclover，加关注后它会自动私信flag。

flag： SYC{Welcome_To_Geek_Challenge_2015}

口号更新

hi！你的flag掉了，在zone里面，同样存在一个小提示，快去更新口号，听说更新内容为flag_flag_flag的时候会爆出flag。

查看 geek.sycsec.com/zone 的源代码，发现如下注释：

```
<!--do you kown how to update slogan?  /slogan -->
```

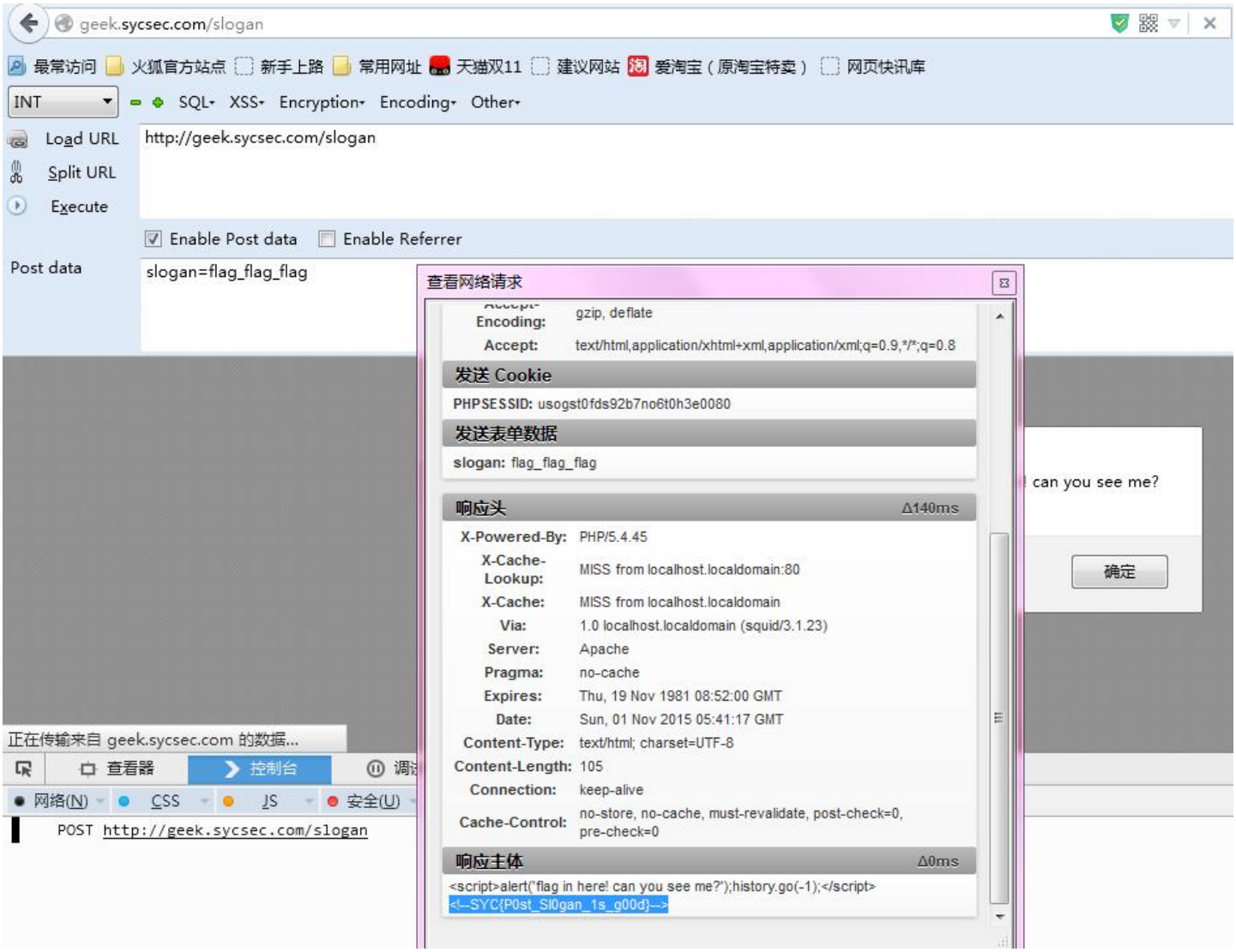
然后尝试访问 geek.sycsec.com/slogan，果然存在这个页面，但是个空白页。联想到题干让“更新口号”，所以可能是要传东西上去，尝试GET或POST上去。而更新的是口号（英文slogan），所以自然想到传的应该是：slogan=flag_flag_flag。

先GET一下，失败了： geek.sycsec.com/slogan?slogan=flag_flag_flag

然后用burpsuite POST了一下，又失败了，于是这题就放了好久。。。直到学长说用Firefox的Hackbar去POST能过。。。这简直是坑我们Chrome选手啊。。。

然后用Firefox搞了一发，果然弹窗了，在响应中找到了flag。

截图如下：



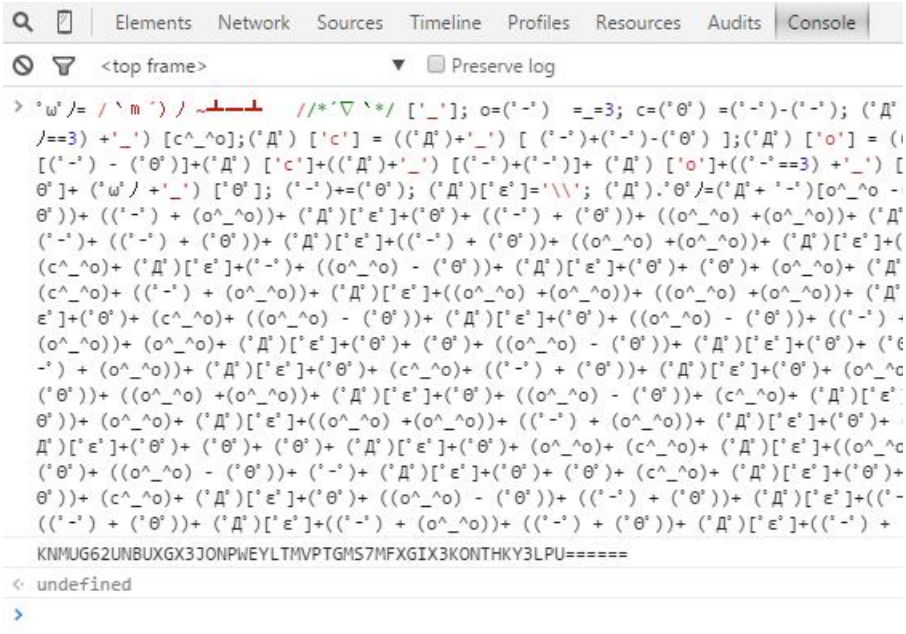
(?Д?)

(ﾟДﾟ) 同学们都太给力了，我必须要放一点新题目了。
http://geek.sycsec.com/download/misc/AAencode

打开题目看到了一堆颜文字。。。

最开始看到这种神奇代码是在知乎一个问题下（时间略久找不到链接了），把那段颜文字复制到Console里跑一下就能自动点赞+关注，后来了解到是一种叫AAencode的js代码加密，可以在 这个网站 在线加密。

同理，将这段代码扔到Console里跑一下：



得到一段神奇的字符串：

> KNMUG62UNBUXGX3JONPWEYLTMVPTGMS7MFXGIX3KONTHKY3LPU======

有点像base64，但是解不出来，就只能做到这里了。。。

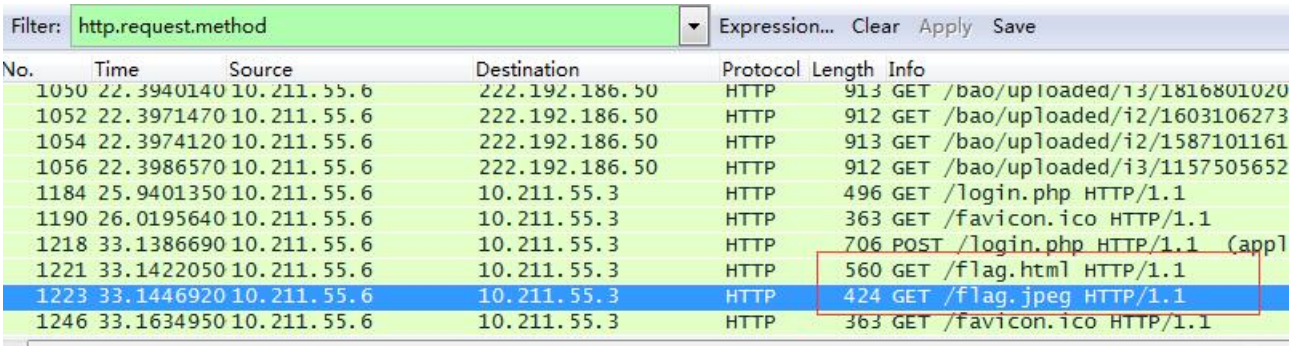
PS. 感谢评论区的同学，这是base32编码，网上可以找到解码器，解码后的结果是：

> SYC{This_is_base_32_and_jsfuck}

大鲨鱼

有同学反映这次没有图片相关的题目，那我出一道好了。 大家快来做啊。
http://geek.sycsec.com/download/misc/wireshark.pcapng

这个是流量包文件，一般用Wireshark分析。打开发现总共有1200多条报文，那就筛选一下，看里面有没有我们感兴趣的内容，一看果然有：



说明在1223号这里请求了flag.jpeg，然后去掉筛选往下找，发现在1239号收到了这张图片。于是打开1239号并把图弄出来（Wireshark右键菜单的“Export Selected Packed Bytes…”可以把整块内容导出到新文件，挺好用的功能~），打开导出的图片，获得flag：

SYC{Wireshark_is_awesome}

会不会写代码？

会不会写代码？听说里面隐藏了一个flag(syc是要大写)
http://geek.sycsec.com/download/misc/gbab7854e8c894a53c456d6da30bec68

打开看了看，好像是个git的配置文件，并没用过git，先留坑。。。

手速够不够快？

锻炼了多年的手速来这里看看够不够快 nc 222.18.158.229 30002

表示没做过这种题，先留坑。。。

仔细瞧一瞧？

这部动漫给赞，可以仔细看看。
http://geek.sycsec.com/download/misc/5efd5e5da5322793d07ab49b21368cc5.html

打开就是这张图（金木小天使–）：

二进制查看，发现里面嵌入了压缩文件（头标志PK），于是将文件扩展名改为rar打开，发现了里面的flag.txt文件，内容如下：

> flag在此，看起来好像是被编码了，听说解码这个后是一个加密，加油~
> VBF{Wk3_Hqf0g3_I0u_b
> 0x_1x}

这种形如&#加上数字的编码可被浏览器解释变为对应字符，数字就是相应字符的unicode编码。这段编码可被浏览器直接解释为：

> VBF{Wk3_Hqf0g3_l0u_b0x_1x}

然后尝试着把最前面的“VBF”映射到“SYC”，发现果然是移位加密。移位解密后的结果为：

> SYC{Th3_Enc0d3_F0r_y0u_1u}

re200_1

感觉是RE题乱入到Misc区里了，逆向并不会。。。

Web

Vous ferez Fran?ais

http://web1.sycsec.com/c8bb427af2bc740a11fd1784c1f11735/
你好，请问你会法语吗？ 呃。。我不会。 什么？法语你都不会！还来做geek.

既然扯到语言，九成是要改报头的Accept-Language字段了，于是改为French提交，得到flag：

小明

http://web1.sycsec.com/d900342ce35a24bca80c965e4380056f/
小明？ 嗯。怎么了，老师？ 滚出去。

点击后跳转到这个url：
http://web1.sycsec.com/d900342ce35a24bca80c965e4380056f/include.php?file=text.php
查看报头发现有一个Tips字段：try to read README，于是尝试访问：
http://web1.sycsec.com/d900342ce35a24bca80c965e4380056f/include.php?file=README.php

页面上有如下内容：

> 想必你对php的LFI已经有一定的了解了,但你能拿到这个页面的源码么？

简单百度了一些，貌似是可以利用文件包含漏洞拿shell的，然而时间不太够没仔细学，先留坑。。。

http_

http://web1.sycsec.com/0bf127f0b4458c7652622b093a85b30a/

Web中的签到题，看报头发现有Flag字段：SYC{1_4M_HttP_He4der}

小明2

http://web1.sycsec.com/12fee4c35daf89c236efbb210026ec8b/
小明？ 嗯？ 滚出去？

打开网页发现如下内容：

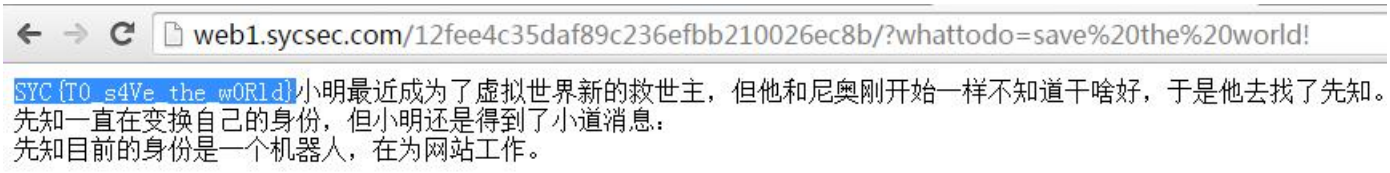
> 小明最近成为了虚拟世界新的救世主，但他和尼奥刚开始一样不知道干啥好，于是他去找了先知。
> 先知一直在变换自己的身份，但小明还是得到了小道消息：
> 先知目前的身份是一个机器人，在为网站工作。

看到“机器人”猜测目录下有robots.txt，访问之发现该目录下有index.php.bak文件，访问之发现如下php源码：

```php
<?php
 $whattodo = "nothing";

 @extract($_REQUEST);
 if($whattodo == "save the world!"){
  echo $flag;
 }
?>
```

这个extract()函数可以覆盖变量的值，于是构造url获得flag：



asp你会吗？

有人说这里有flag 我不信（flag是SYC{shell的密码}）
http://web1.sycsec.com/63f4e9530ce4759821452cba6599931f/www.zip

没思路先留坑。。。

来来来，写代码

听说这一届学弟学妹写代码写的很溜啊，来来来，写一发脚本吧。
http://web1.sycsec.com/b33804a7301e583ca6a473c1c092b09f/

> 来来来，小伙子，写个脚本来爆破的我的变量吧哈哈哈！！！！！
> Tips:变量名SYC**

GET还是POST也没说，于是大暴力。。。并没跑出来。。。

小彩蛋

zone里面隐藏着一个小彩蛋，不知道聪明的你看到了没。

flag藏在这个url里：http://geek.sycsec.com/assets/default/css/jk.min.css

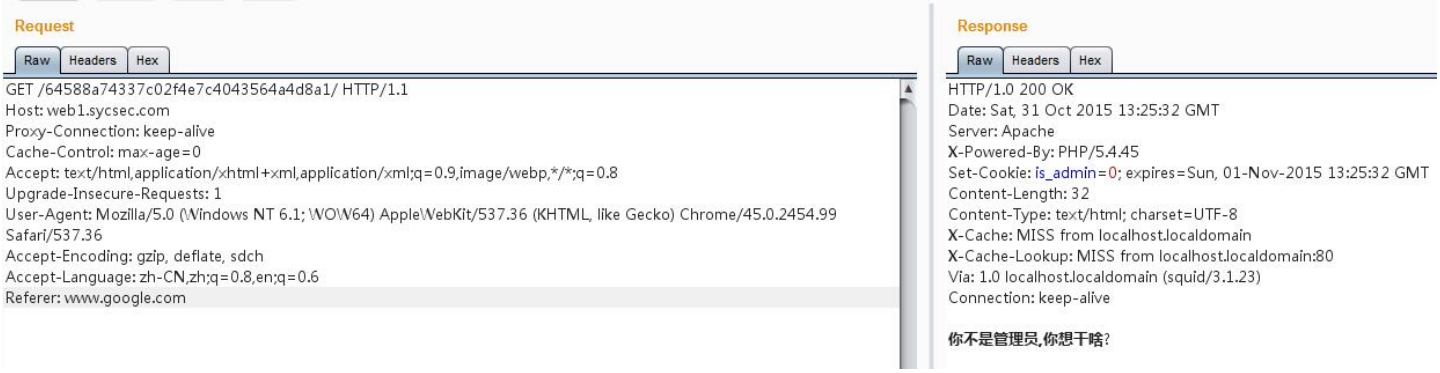
```
.flag:before{
 content: "SYC{Css_Als0_Can_h1D3_F1ag}";
 color: transparent;
 display: none;
}
```

饼干饼干饼干

http://web1.sycsec.com/64588a74337c02f4e7c4043564a4d8a1

打开以后提示：只能通过谷歌来访问噢！

推测是构造报头的referer字段，加上以后返回：



于是加上cookie访问：

sqli1

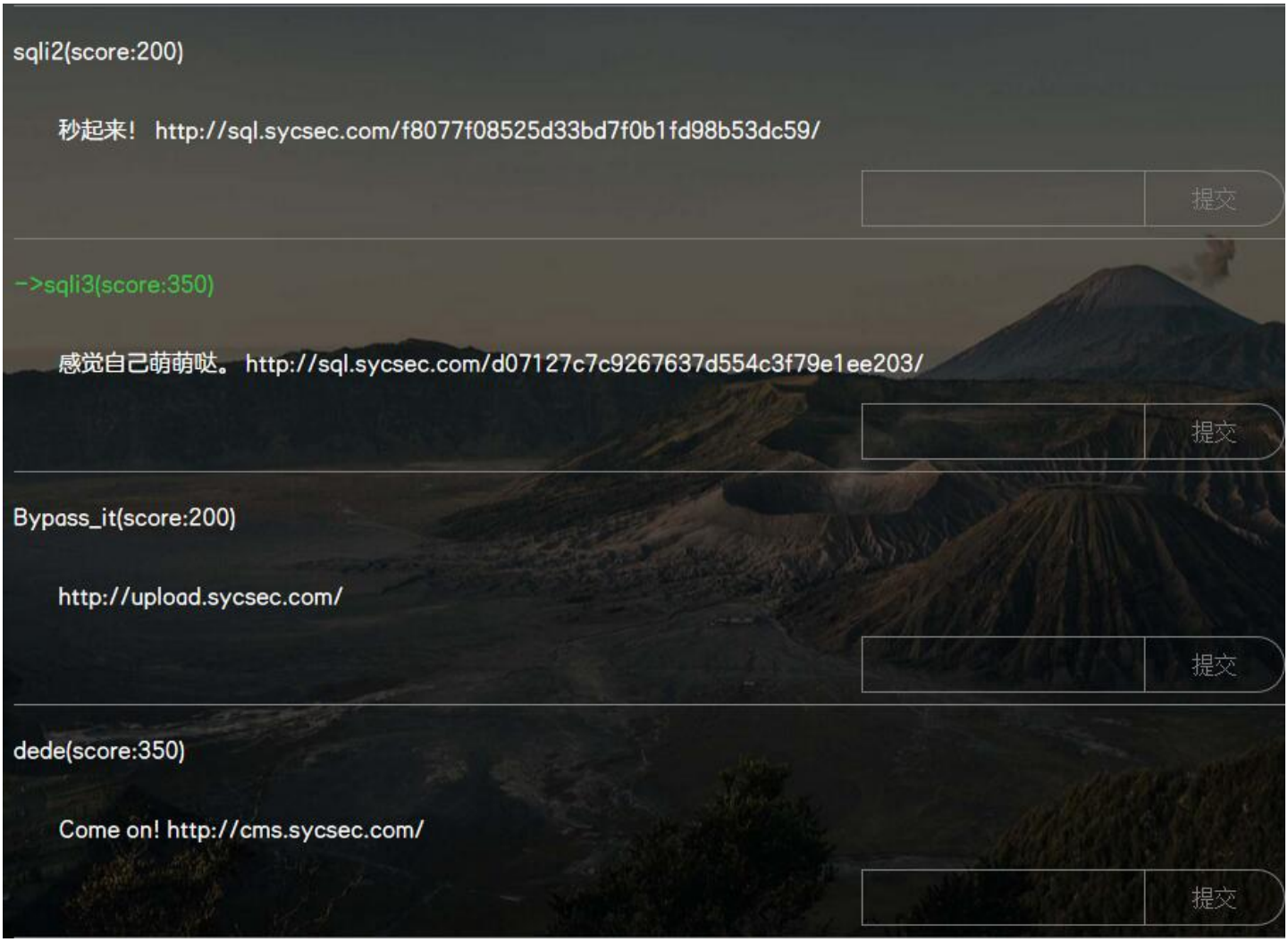
快来秒！ http://sql.sycsec.com/5f3b974ef6337582f2eeb8da24059c7a/

我是直接拿sqlmap扫的。。。

```
>sqlmap.py -u http://sql.sycsec.com/5f3b974ef6337582f2eeb8da24059c7a/?uid=1 -D sql1 -T flag -C flag --dump
```

flag：SYC{Sql_Inject10n_0n3_ppp}

之后的web题都没做，具体有这些：



Reverse & Linux

这部分不熟，没做。

Program

Transposition cipher

详情请看 http://geek.sycsec.com/download/program/program100/Transposition_cipher.html

介绍了一种置换加密方法，先每行7个字符横着写原文，然后竖着一列一列组成密文。给了一段密文让置换成原文。

了解原理后，代码实现并不难，下面是我用C写的解密代码：

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <math.h>
#include <iostream>
#include <algorithm>
using namespace std;

char mp[1100][8];
int orikey[7] = {7, 6, 5, 2, 1, 3, 4};
int key[7]    = {5, 4, 6, 7, 3, 2, 1};
int main()
{
    freopen("in.txt", "r", stdin);
    freopen("out.txt", "w", stdout);
    int hang = 1075;
    char c;
    int i = 0, j = 0, cnt = 0;
    while((c = getchar()) != EOF){
        //cnt++;
        mp[i++][key[j]] = c;
        if(i == hang){
            j++;
            i = 0;
        }
    }
    for(int ii=0; ii<hang; ii++){
        for(int jj=1; jj<=7; jj++){
            putchar(mp[ii][jj]);
        }
        putchar('\n');
    }
    return 0;
}
```

后面两题没来得及看。。。

总结一下，感觉自己还是太水了。马上就该“问鼎杯”了，不知道今年我们几个能不能达到周神去年一半的水平T^T

不过既然选择了这个方向，就要尽量多学一点、多会一点，争取以后比赛不当吊车尾。