Hgame Write Up – Week 1

Li4n0

2018 年 2 月 11 日

1 Web部分

1.1 Are you from Europe?

没错我就是欧洲人，一下子就抽中了!!!!!! 咳咳，好吧，其实刚刚开赛时飞速打开这道题然后的情况是一脸懵逼的: ????这都是啥？？只有拥有ssr的勇士才能拿flag？？要用ssr翻墙？？往哪翻啊？？然后点了几次召唤————————更懵逼了，这是在干啥。。（流下了没玩过游戏的泪水）。然后F12，发现有一大段js啊！大概看一遍，发现亮点————

```
function buyQuartz() {
    if (woainvzhuang == true) {
        var buy = confirm("圣晶石不够了，快氪金啊勇士。");
        if (buy) {
            quartz += 167;
            money += 518;
            alert("购买圣晶石成功。您目前持有圣晶石：" + quartz);
            $("#quartz").text(quartz);
            $("#money").text(money);
            woainvzhuang = false;
            return true;
        }
        else {
            alert("没钱玩什么游戏！");
            return false;
        }
    }
    else {
        alert("很抱歉，圣晶石一年限购一次，明年招新再来吧勇士。");
    }
}
```

基本~~看出了出题人的恶趣味~~看出了flag就应该藏在这段js里。所以再仔细看

一下，找到了与ssr有关的代码，

```
function getCard(num) {
    var SSR = 0.0000001;
    var SR = 0.15;
    var cards = [];
    var card;
    if (times > 100) {
        SSR *= 100;
```

再根据题目中说的召唤一百次后ssr概率提升100倍，明白了这里是在控制ssr的爆出几率。

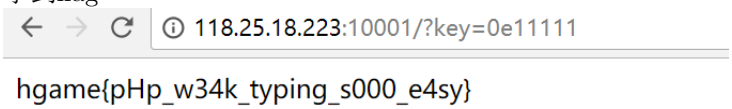
F12 network发现和后端没有交互，那么果断右键保存页面到本地，丧心病狂的把ssr的初始概率从0.00000001改成10000000000000 然后打开，召唤，get!

1.2 special number

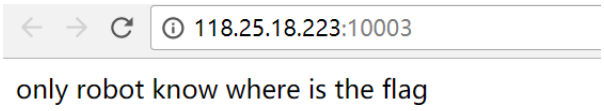
知识点：php弱类型 其实我还没开始学php,不过大概看得懂，而且之前也做过一些题目，所以这种基础题勉强可以应付。GET方式传递参数key的值，看一眼正则 `$pattern = '/^(?=.*[0-9].*)(?=.*[a-zA-Z].*).{7,}$/';` 第一位要求为数字，第二位为字母，长度至少为7，下面和"**********"进行比较，相等的条件下才能get flag。

这道题具体有两个知识点，第一、php中，0e12345、1e23456这样的字符串在比较时会被视为科学计数法，第二、字符串跟数字比较时，会根据字符串开始的部分把字符串化为数字进行比较，如'1aaaaa'==1 'aaaa'==0

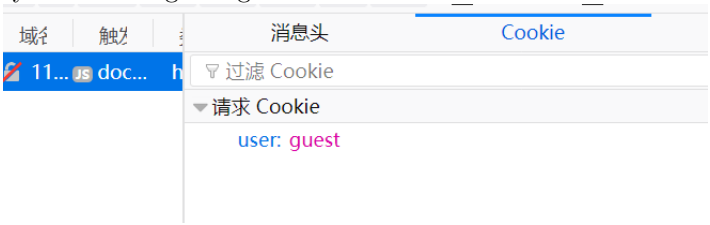
那么构造key=0e11111，由于0e11111==0=='**********'条件成立，便可拿到flag



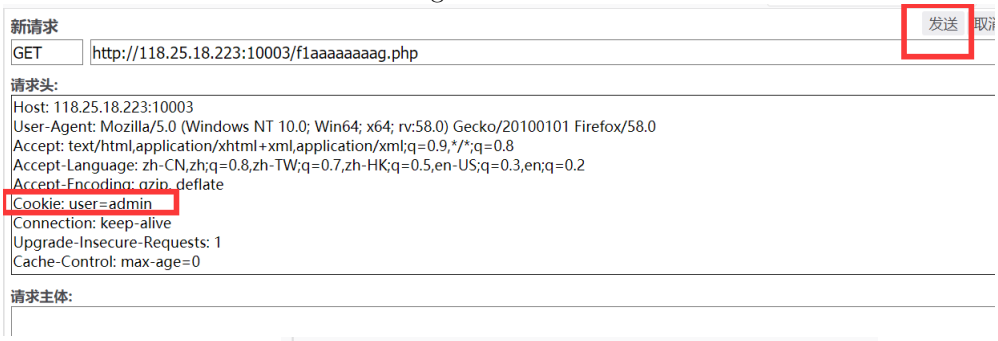
1.3 can u fin me?

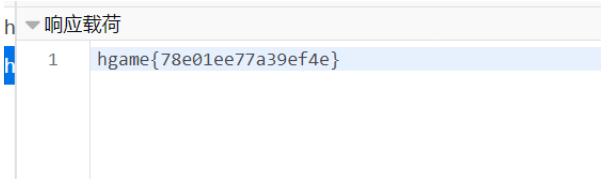


提示的很明显了，果断访问robots.txt,看到f1aaaaaaaag.php，访问后发现only admin can get flag?于是F12找到cookie



用Firefox自带的编辑和重发功能修改guest为admin并重新发送



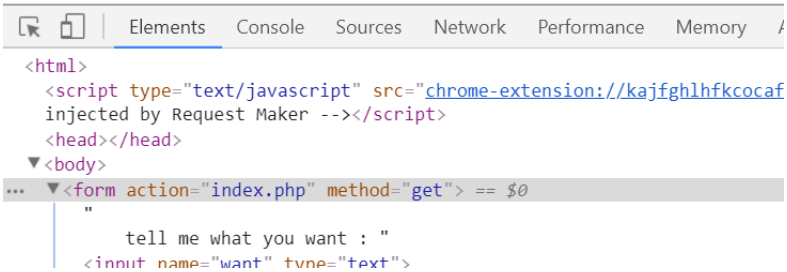


然后在响应里找到flag：

1.4 tell me what u want

打开题目链接，看到这个问题的时候，我居然天真的在输入框里输入了flag....

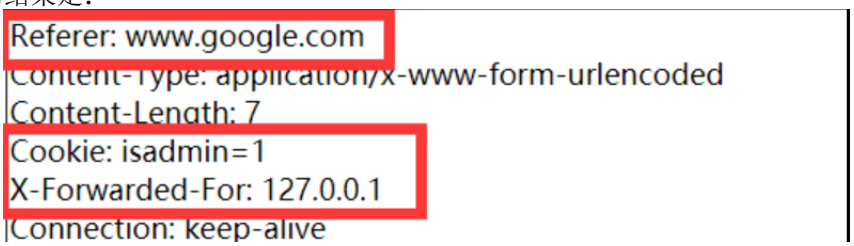
tell me what you want : submit
request method is error.I think POST is better



然鹅被告诉请求方法有问题，于是将form的method属性改成post再提交，然后是...:

tell me what you want : submit
https://www.wikiwand.com/en/X-Forwarded-For
only localhost can get flag

于是开始了不停地花式改请求头,依旧还是用firefox的编辑和重发，改到最后的结果是：

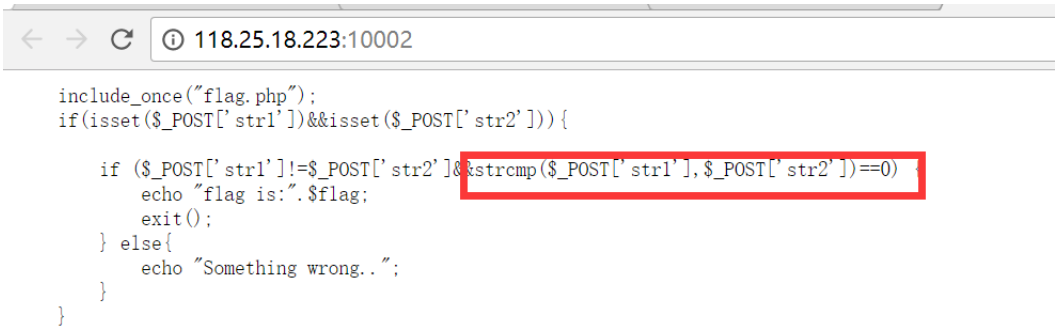


以及神奇的Icefox57.0

最后get flag：

1.5 我们不一样

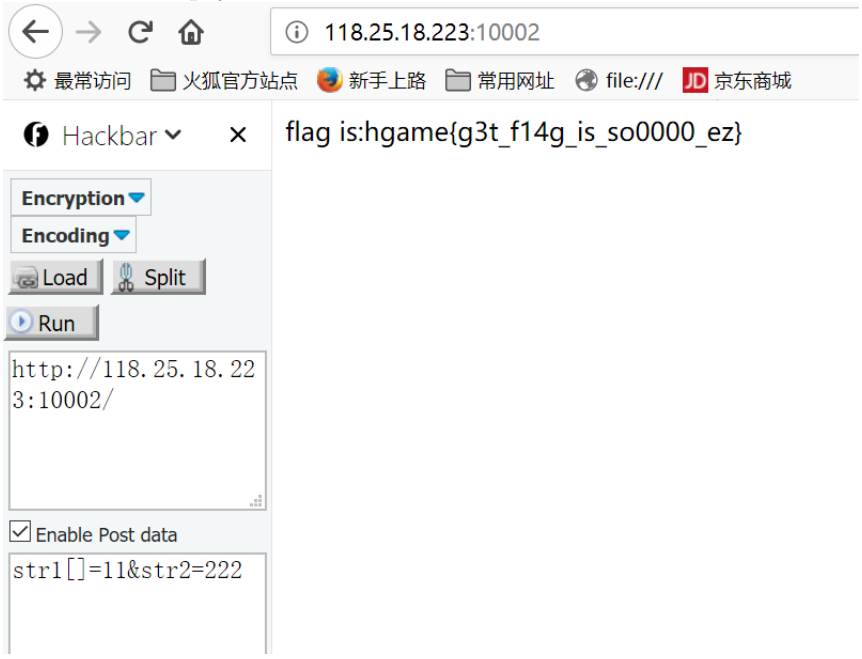
依然是考察弱类型比较的知识点 ：



注意到这里用到了strcmp()，这个神奇的函数只能比较两个字符串，而当参数的类型不符合要求的时候，在PHP 5.3以下（版本的问题一会再说）会发出警告，但是却会返回一个0!！而在弱类型比较中0==False 于是我们只要让strcmp的参数不是字符串，便可以使得条件成立拿到flag!

那么又要用到一个知识点，php会把str[]=xxx这样的参数视为一个名为str，值为[xxx]的数组.

于是构造这样的payload：

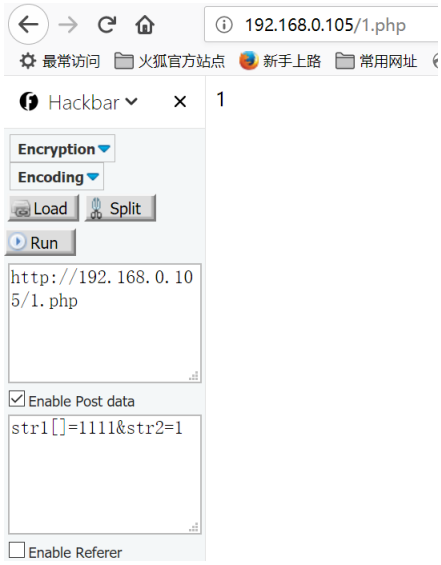


拿到flag

PS：蜜汁版本问题： 实际操作的时候，当我发现strcmp函数后，第一时间是去看了一下服务端的php版本，发现是7.0，顿时感觉没戏了(ノ ' □ ')ノ ┻━┻，因为印象中之前百度到php这个漏洞是5.3以下的，5.3以上的漏洞被修补了，于是再次百度php strcmp漏洞，结果发现百度上说法不一，说是5.3以后才出现的这个漏洞，也有人说是5.3以下的版本才有这个洞..... 于是不管那么多了，先提交一下试试，居然成功了....

于是自己在本地验证了一下strcmp在不同版本php中的表现：

```
<?php echo strcmp($_POST['str1'],$_POST['str2']);?>
```

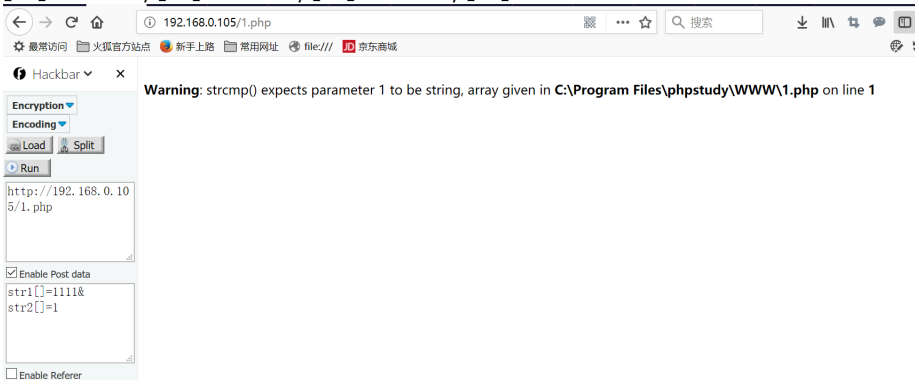


php 5.2.17:

当一个参数为数组，另一个参数是字符串时返回正常

当两个参数全部为数组时，返回0

php 5.3.29/php 5.4.45/php 5.5.38/php 5.6.27 ：



直接丢出来一个warning，看似没有返回任何值，也就是返回null，然而，null == False依然成立....

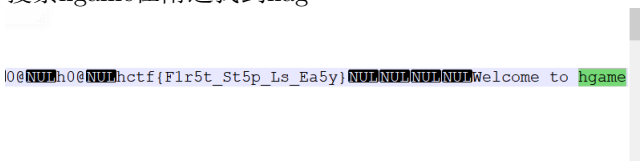
本地没有安装php7.0 运行所需要的依赖库，所以没法测试，不过根据题目的情况，7.0肯定也是可以的...

神TM版本限制(ノ ' □ ')ノ ⌒┻━┻，这不是通杀了吗，那百度上那群人都在说什么？？？

2 re部分

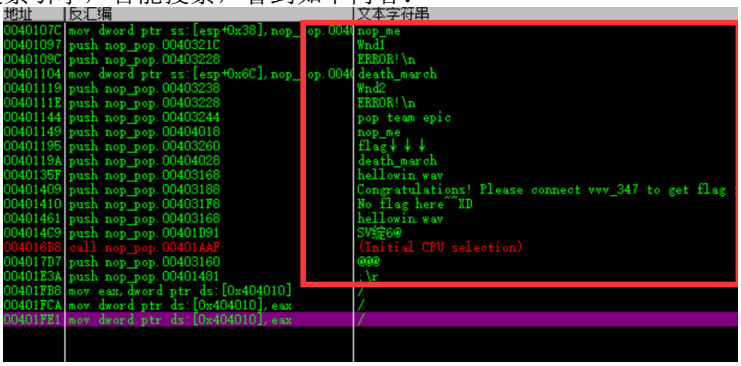
2.1 re0

emmm签到题么，觉得肯定很简单，于是下载后啥都没想直接notepad++打开，搜索hgame在附近找到flag

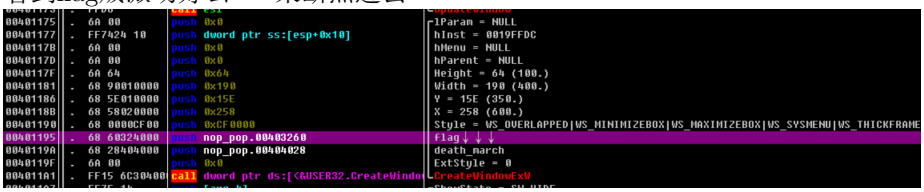


2.2 nop pop

这题能做出来是得益于曾经在吾爱破解上看过shark恒的od使用教程...看得本来就不多，忘完就更不多了。。但是nop填充还是记得的。。于是od载入右键中文搜索引擎，智能搜索，看到如下内容：



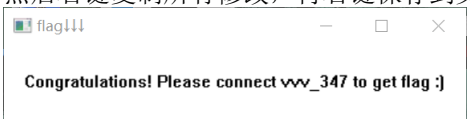
看到flag贼激动好么？？果断点进去



(ノ ` □ ′)ノ ┻━┻说好的flag呢？？人与人之间的信任呢？

大概看出这里实在设置窗口的一些参数，那么再退回去看其他的内容，注意到了nop me，点进去，既然已经提出让我nop u 了，那还客气什么？直接nop填充

然后右键复制所有修改，再右键保存到文件，双击打开，弹窗消失!：

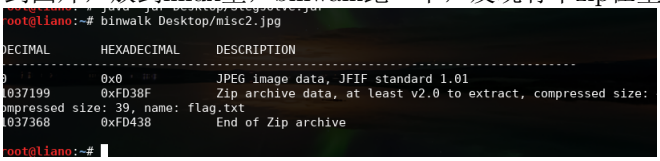


把文件发给vvv就能get到flag了!!!

3 misc

3.1 白菜2

拿到图片，放到linux里，binwalk跑一下，发现有个zip在里面



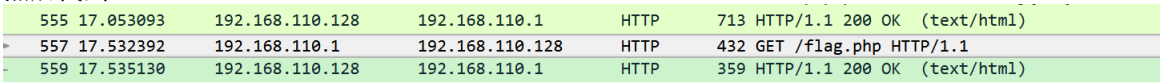
那么直接改后缀为zip，没有密码直接打开，看到flag.txt

3.2 pacp2

wireshark 打开流量包，按照题目说的，直接去找不得了的东西

在显示过滤器里输入http，使其只显示http协议的数据包

然后找到



追踪http流，在最下面的包里找到flag

```
Date: Mon, 29 Jan 2018 12:36:09 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/7.1.7
Content-Encoding: gzip

hgame{bfebcf95972871907c89893aa3096ec6}
```

分组 559。11 客户端 分组，11 服务器 分组，21 turn(s).点击选择。

4 cypto

4.1 easy Caesar

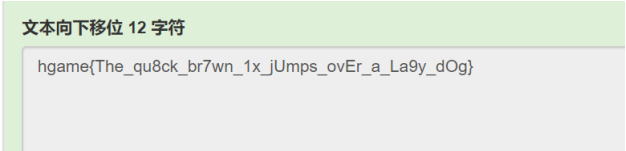
拿到密文后在百度上搜索凯撒密码在线解密，然后看到了hgame，无脑复制，提交，what？？？ Incorrect？

```
第10次解密:mlfrj{ymj_vz8hp_gw7bs_lc_ozrux_tajw_f_qf9d_itl}
第11次解密:lkeqi{xli_uy8go_fv7ar_lb_nyqtw_sziv_e_pe9c_hsk}
第12次解密:kjdph{wkh_tx8fn_eu7zq_la_mxpsv_ryhu_d_od9b_grj}
第13次解密:jicog{vjg_sw8em_dt7yp_lz_lworu_qxgt_c_nc9a_fqi}
第14次解密:ihbnf{uif_rv8dl_cs7xo_ly_kvnqt_pwfs_b_mb9z_eph}
第15次解密:hgame{the_qu8ck_br7wn_lx_jumps_over_a_la9y_dog}
第16次解密:gfzld{sgd_pt8bj_aq7vm_lw_itlor_nudq_z_kz9x_cnf}
第17次解密:feykc{rfc_os8ai_zp7ul_lv_hsknq_mtcp_y_jy9w_bme}
第18次解密:edxjb{qeb_nr8zh_yo7tk_lu_grjmp_lsbo_x_ix9v_ald}
第19次解密:dcwia{pda_mq8yg_xn7sj_lt_fqilo_kran_w_hw9u_zkc}
第20次解密:cbvhz{ocz_lp8xf_wm7ri_ls_ephkn_jqzm_v_gv9t_yjb}
第21次解密:baugy{nby_ko8we_vl7qh_lr_dogjm_ipyl_u_fu9s_xia}
第22次解密:aztfx{max_jn8vd_uk7pg_lq_cnfil_hoxk_t_et9r_whz}
第23次解密:zysew{lzw_im8uc_tj7of_lp_bmehk_gnwj_s_ds9q_vgy}
第24次解密:yxrdv{kyv_hl8tb_si7ne_lo_aldgj_fmvi_r_cr9p_ufx}
```

于是看了一下flag的内容，发现离奇的数字使得flag内容没有意义啊！qu8ck自然想到quick，i和1对应的话，说明偏移量为3，那么接下来的每个数字都加3看看呢？br0wn——brown 4x——fox la2y——lazy 好的，都有意义了，这回应该没错了吧！提交，又不对。。(ノ ' □ ')ノ ⌒┻━┻，简直不敢相信这么有意义的flag会是错的，于是接连提交这个flag的修改版。。。以至于三金学长以为我在爆破flag23333，贴一张后台提交flag记录的图纪念一下————

```
[NOTICE] 队伍 Li4n0 提交 Flag: hgame{the_qu1ck_br0wn_fox_jumps_over_a_la2y_dog} (错误)
[NOTICE] 队伍 Li4n0 提交 Flag: hgame{the_qu1ck_br0wn_4x_jumps_over_a_la2y_dog} (错误)
[NOTICE] 队伍 Li4n0 提交 Flag: hctf{the_qu1ck_br0wn_4x_jumps_over_a_la2y_dog} (错误)
[NOTICE] 队伍 Li4n0 提交 Flag: {the_qu1ck_br0wn_4x_jumps_over_a_la2y_dog} (错误)
[NOTICE] 队伍 Li4n0 提交 Flag: hgame{the_qu1ck_br0wn_4x_jumps_over_a_la2y_dog} (错误)
[NOTICE] 队伍 Li4n0 提交 Flag: hgame{the_qu1ck_br0wn_4x_jumps_over_a_la2y_dog} (错误)
```

于是暂时没思路了，以为是有什么骚操作在里面，就暂时搁浅了.。。直到做出下面的题，又遇到凯撒，解出flag还是有意义但是Incorrect，我才开始怀疑是我用的工具有问题....于是换用google搜到了一个在线凯撒解密，http://tools.matchzones.net/caesar_cipher

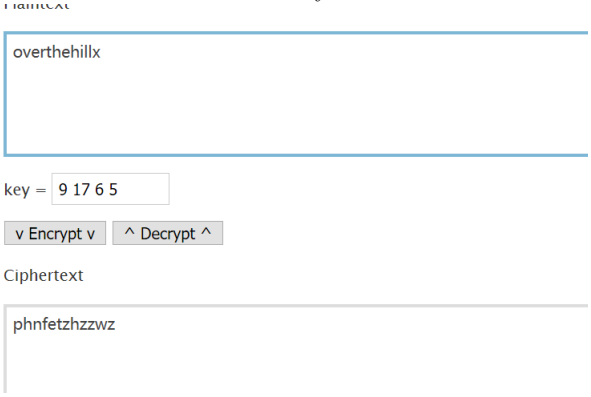


发现原来第一个工具把字母全都变成小写了.....
修改数字，提交，终于拿到了flag

4.2 Hill

之前从没听过这个加密，于是顺着题目给出的链接去看了一下，然后.....(ノ｀□′)ノ ┻━┻线性代数！矩阵变换!！我可是挂过线代的人啊..这还不如让我死...

于是求助万能的google，果然又找到了个在线解密Hill的网站，http://www.practicalcryptography.com/ciphers/hill-cipher/（仔细看了下，这是个蛮专业的密码学网站，而且大多有JS编写的在线解密工具，还是蛮好的一个站，收藏起来慢慢看），直接把key和密文输进去解密就好了。



4.3 confusion

第一眼过去感觉是摩斯密码，于是用摩斯密码在线解密http://www.zhongguosou.com/zonghe/moErSiCodeConverter.aspx

得到一串数字字母组合的字符，判断应该为base家族的加密

于是先用base64试试，结果得到了一堆乱码，于是再试试base32，结果报错

```
Traceback (most recent call last):
  File "C:/Users/liano/Desktop/python/test/2.py", line 10, in <module>
    a = base64.b32decode(text)
  File "C:\Program Files\Python36\lib\base64.py", line 205, in b32decode
    raise binascii.Error('Incorrect padding')
binascii.Error: Incorrect padding
```

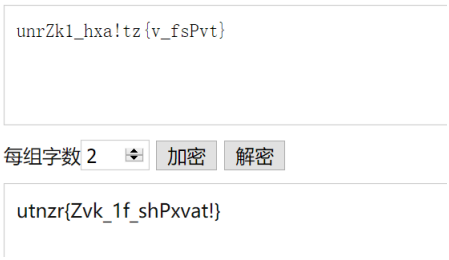
错误信息中说的很明显了，位数不对，那么尝试在后面加”=”补全，加到第四个时成功解密。

```
"C:\Program Files\Python36\python.exe" C:/Users/liano/Desktop/python/test/2.py
b'dW5yWmsxX2h4YSF0ent2X2ZzUHZ0fQ=='
```

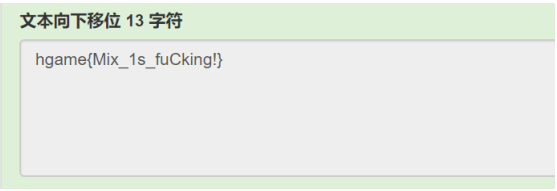
特征很明显了，再用base64解密

```
"C:\Program Files\Python36\python.exe" C:/Users/liano/Desktop/python/test/2.py
b'unrZk1_hxa!tz{v_fsPvt}'
```

栅栏，用在线工具http://www.qqxiuzi.cn/bianma/zhalanmima.php



根据flag的格式和”!”的位置可以判断每组字符数就是2，于是凯撒



get flag!