php反向代理ctf,ctf题目writeup（7）

转载

嘉禾博研左方程 于 2021-03-11 22:17:07 发布 45 收藏
文章标签： php反向代理ctf
2019.2.3

继续刷bugku的题，题目地址：https://ctf.bugku.com/challenges

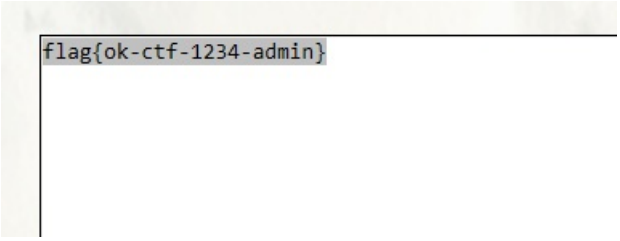
1.

ok
30

Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook? Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook!
Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook? Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook.

ook和brainfuck都到这个网站：

https://www.splitbrain.org/services/ook



flag{ok-ctf-1234-admin}

2.

这不是摩斯密码

30

下载看看吧

1.txt

Flag

Submit

+++++ +++++ [->++ +++++ +++++.+ +++++ .-- -- -.+++ +++.<

++++[->+++ ++ +++.< +++[- >---<]>--- .---- .--- ----<

]>--- ----- ----- .+++ ++++<]>+++ ++.- -----

-. +++ +++++ ++ .-- -- ----.

>---- ------- ----. +++++ +..++ +++.+ .-- -- --.

+[->+ +++++ ++ ++.++ +.+++ +++++ +.--- -.+++ ++. +++++++

++.<

这个就是brainfuck 还是到上述网站就行

flag{ok-c2tf-3389-admin}

3.

easy_crypto

30

0010 0100 01 110 1111011 11 11111 010 000 0 001101 1010 111
100 0 001101 01111 000 001101 00 10 1 0 010 0 000 1 01111 10
11110 101011 1111101

这道题是莫尔斯电码对应ascii的转换：

对应电码	字符
01	A
1000	B
1010	C
100	D
0	E
0010	F
110	G
0000	H
00	I
0111	J
101	K
0100	L
11	M
10	N
111	O
0110	P
1101	Q
010	R
000	S
1	T
001	U
0001	V
011	W
1001	X

高亮显示重复值
C01
C1000
C1010
C100
C0
C0010
C110
C0000
C00
C0111
C101
C0100
C11
C10
C111
C0110
C1101
C010
C000
C1
C001
C0001
C011
C1001

示例：

待解电码串	解码后的字符串
11111	0
01111	1
00011	3
00111	2
00111	2
00000	5
11111	0
11100	8
00111	2
11111	0
00000	5
00011	3
11111	0
11111	0
11111	0
11100	8
10000	6
01111	1
11000	7
00001	4

其实 摩斯电码中的 .就是0 -就是1

也可以用python直接处理，或者你用文本编辑器替换嘿嘿。

4.

看到后面两个AA不由自主想到两个等号 ==

A的ascii是65 =是61 所以写个脚本把所有符号往前移4位。

```
def caesar(text):
for i in range(len(text)):
print("{}".format(chr(int(ord(text[i])-4))),end='')
caesar('e6Z9i~]8R~U~QHE{RnY{QXg~QnQ{^XVIRXIp^XI5Q6Q6SKY8jUAA')
```

a2V5ezY4NzQzMDAwNjUwMTczMjMwZTRhNThlZTE1M2M2OGU4fQ==

直接base64解密：

key{68743000650173230e4a58ee153c68e8}

5.

这里散乱的方式需要按照这个提示重新排列，正好可以分为6个字符一组，然后他们目前的编号顺序是 2 1 6 5 3 4 所以我们把他们的编号变成 1 2 3 4 5 6就好了。

flag{52048c453d794df1}@@(后面@删除就是flag)

6.

提示很明显，直接凯撒：

```
MSW{byly_Cm_slol_lYqUlx_yhdls_Cn_Wuymul_il_wuff_bcg_pCwnll_cm_u_Yrwyffyhn_guh_cz_sio_quhn_ni_ayn_bcm_chzilguncihm_sio_wuh
```

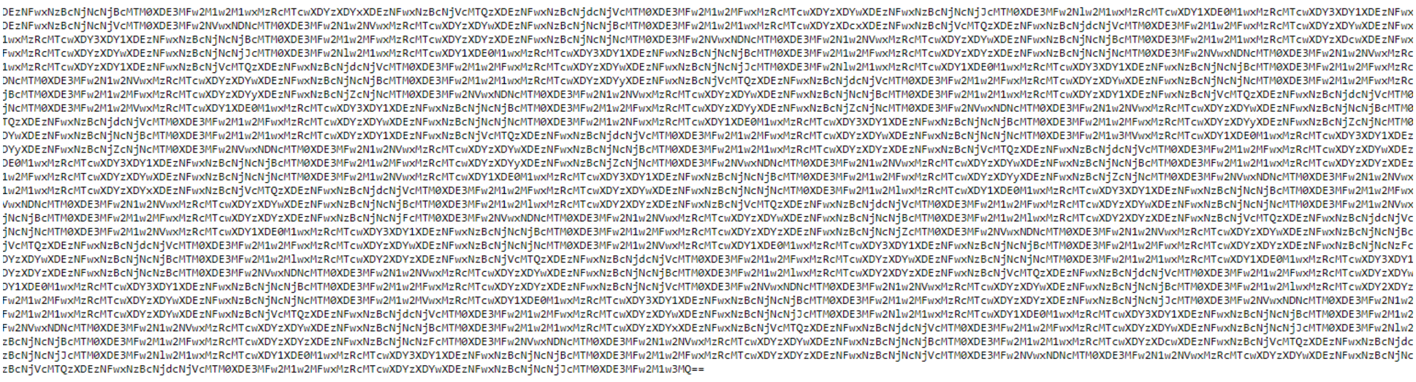
结果：（字符数统计：3380）

```
NTX{czmz_Dn_tJpm_mZrVmy_zieJt_Do_Xvznvm_jm_xvgg_cdh_qDxoJm_dn_v_Zsxzggzio_hvi_da_tjp_rvio_oj_bzo_cdn_diajmhvodjin_tjp_xv
OUY{dana_Eo_uKqn_nAsWnz_ajfKu_Ep_Ywaown_kn_ywhh_dei_rEypKn_eo_w_Atyahhajp_iwj_eb_ukq_swjp_pk_cap_deo_ejbkniwpekjo_ukq_yw
PVZ{ebob_Fp_vLro_oBtXoa_bkgLv_Fq_Zxbpxo_lo_zxii_efj_sFzqLo_fp_x_Buzbiibkq_jxk_fc_vlr_txkq_ql_dbq_efp_fkclojxqflkp_vlr_zx
QWA{fcpc_Gq_wMsp_pCuYpb_clhMw_Gr_Aycqyp_mp_ayjj_fgk_tGarMp_gq_y_Cvacjjclr_kyl_gd_wms_uylr_rm_ecr_fgq_gldmpkyrgmlq_wms_ay
RXB{gdqd_Hr_xNtq_qDvZqc_dmiNx_Hs_Bzdrzq_nq_bzkk_ghl_uHbsNq_hr_z_Dwbdkkdms_lzm_he_xnt_vzms_sn_fds_ghr_hmenqlzshnmr_xnt_bz
SYC{here_Is_yOur_rEwArd_enjOy_It_Caesar_or_call_him_vIctOr_is_a_Excellent_man_if_you_want_to_get_his_informations_you_ca
TZD{ifsf_Jt_zPvs_sFxBse_fokPz_Ju_Dbftbs_ps_dbmm_ijn_wJduPs_jt_b_Fydfmmfou_nbo_jg_zpv_xbou_up_hfu_ijt_jogpsnbujpot_zpv_db
UAE{jgtg_Ku_aQwt_tGyCtf_gplQa_Kv_Ecguct_qt_ecnn_jko_xKevQt_ku_c_Gzegnngpv_ocp_kh_aqw_ycpv_vq_igv_jku_kphqtocvkqpu_aqw_ec
VBF{khuh_Lv_bRxu_uHzDug_hqmRb_Lw_Fdhvdu_ru_fdoo_klp_yLfwRu_lv_d_Hafhoohqw_pdq_li_brx_zdqw_wr_jhw_klv_lqirupdwlrqv_brx_fd
WCG{livi_Mw_cSyv_vIaEvh_irnSc_Mx_Geiwev_sv_gepp_lmq_zMgxSv_mw_e_Ibgippirx_qer_mj_csy_aerx_xs_kix_lmw_mrjsvqexmsrw_csy_ge
XDH{mjwj_Nx_dTzw_wJbFwi_jsoTd_Ny_Hfjxfw_tw_hfqq_mnr_aNhyTw_nx_f_Jchjqqjsy_rfs_nk_dtz_bfsy_yt_ljy_mnx_nsktwrfyntsx_dtz_hf
YEI{nkxk_Oy_eUax_xKcGxj_ktpUe_Oz_Igkygx_ux_igrr_nos_bOizUx_oy_g_Kdikrrktz_sgt_ol_eua_cgtz_zu_mkz_noy_otluxsgzouty_eua_ig
ZFJ{olyl_Pz_fVby_yLdHyk_luqVf_Pa_Jhlzhy_vy_jhss_opt_cPjaVy_pz_h_Lejlsslua_thu_pm_fvb_dhua_av_nla_opz_pumvythapvuz_fvb_jh
AGK{pmzm_Qa_gWcz_zMeIzl_mvrWg_Qb_Kimaiz_wz_kitt_pqu_dQkbWz_qa_i_Mfkmttmvb_uiv_qn_gwc_eivb_bw_omb_pqa_qvnwzuibqwva_gwc_ki
BHL{qnan_Rb_hXda_aNfJam_nwsXh_Rc_Ljnbja_xa_ljuu_qrv_eRlcXa_rb_j_Nglnuunwc_vjw_ro_hxd_fjwc_cx_pnc_qrb_rwoxavjcrxwb_hxd_lj
CIM{robo_Sc_iYeb_bOgKbn_oxtYi_Sd_Mkockb_yb_mkvv_rsw_fSmdYb_sc_k_Ohmovvoxd_wkx_sp_iye_gkxd_dy_qod_rsc_sxpybwkdsyxc_iye_mk
```

这个就是找有意义的单词，很显然就是它了：

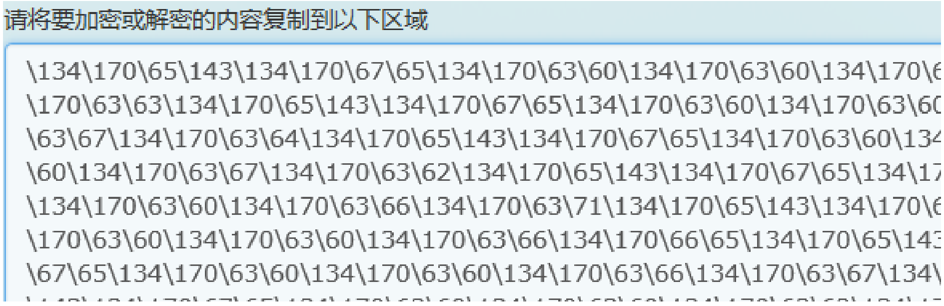
SYC{here_Is_yOur_rEwArd_enjOy_It_Caesar_or_call_him_vIctOr_is_a_Excellent_man_if_you_want_to_get_hi

7.



乍一看挺吓人的，直接base64：

又是一大段：



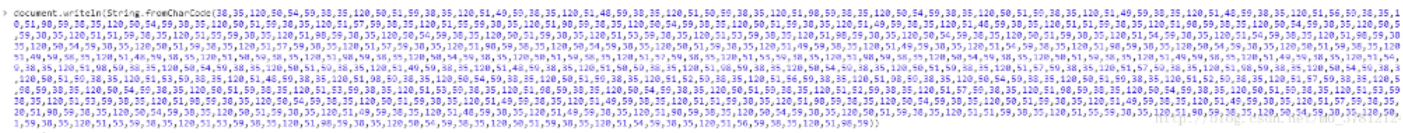
最多三个一组，最大是7，那就差不多是八进制。

转成16进制：

> \u0053\u0074\u0072\u0069\u006e\u0067\u002e\u0066\u0072\u006f\u006d\u0043\u0068\u0061\u0072\u0043\u006f\u0064\u0065\u0028\u0033\u0038\u002c\u0033\u0035\u002c\u0031\u0032\u0030\u002c\u0035\u0030\u002c\u0035\u0034\u002c\u0035\u0039\u002c\u0033\u0038\u002c\u0033\u0035\u002c\u0031\u0032\u0030。。

这就是unicode了。。。再转：

String.fromCharCode()是把ASCII码转成字符串，有很多种方法继续解码，可以直接chr()中间的数字，或者直接在游览器里面输入document.writeln()加上上面这段：
即



输出：

```
1  &#102;&#108;&#97;&#103;&#37;&#55;&#66;&#99;&#116;&#102;&#95;&#116;&#102;&#99;&#50;&#48;&#49;&#55;&#49;&#55;&#113;&#119;&#101;&#37;&#55;&#68;
```

随便找个游览器输入上面的字符串就可以了
输出：

> flag%7Bctf_tfc201717qwe%7D

%7B和%7D是URL编码的{和}，所以最后答案就出来了。

flag{ctf_tfc201717qwe}

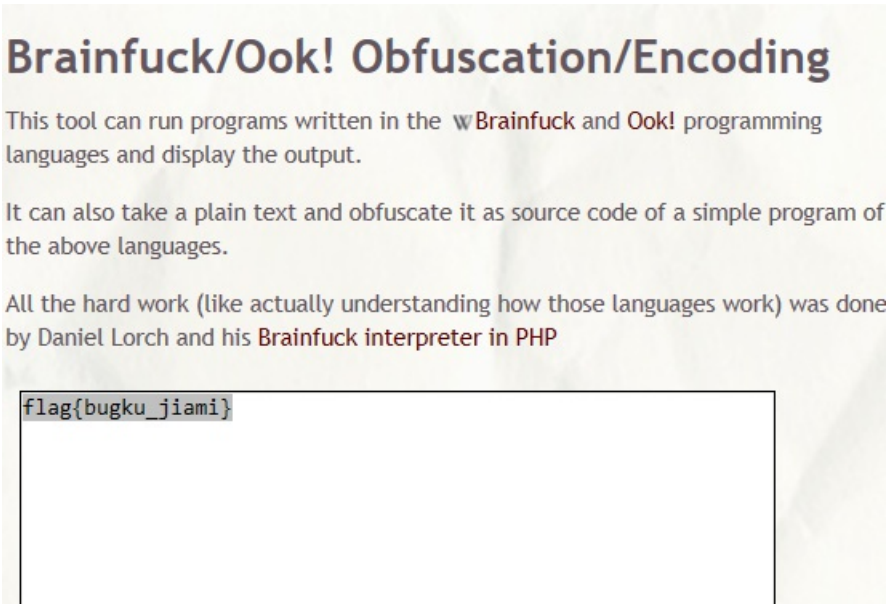
8.

.!?

80

.... !?!! .?.... .... ?.?! .?... !....
.... !.?.. ..... !?!!. ?!!!! !!?.? !.?!! !!!.. .... !.?.
....!? !!.?. ..... .?.? !.?.. ..... !.?. .... !?!!. ?!!!!
!!!!! !?.?! .?!.? ....! ?!!.? ....?. ?!.?. ..... !.?.. .....
!?!!. ?!!!! !!?.? !.?!! !!!!! !!!!. ....!. ?..... ...!? !!.?. .....
??!. ?...!. ?..... ..... !?!!. ?!!!! !!!!? .?!.? !!!!! !!!!! !!!.? .....
..!?! !.?.. ....? .?!.? ....! .!!!. !!!!! !!!!! !!!!! !!.?. ..... .!?!!
.?... ...?. ?!.?. ..... ! !!! !!!!! !.?.. ....!?! !.?.. ..... .?.?!
.?... ..... !.?.

其实这也是Ook加密，直接网站：



flag{bugku_jiami}

9.

奇怪的密码

100

突然天上一道雷电
gndk€rlqhmtkwwp}z

看这个格式应该是flag{。。。。}什么的。

对比一下 g 左移一位是f n左移两位是l 。。。以此类推。

可以直接算或者写代码

str='gndk€rlqhmtkwwp}z'

j = 1

for i in str:

print(chr(ord(i)-j))

j+=1

flag{lei_ci_jiami}

10.

百度一下，这个是什么杰斐逊轮转加密：

，比如第一个密钥匙：2、密文匙：H

把转盘第二行单独提出来 2：

从H的地方一直剪切，把剪切的内容放在最前面，变成 2：

依次类推把14行都按这样的方式整一遍就得到这个：

2：

5：

1：

3：

6：

4：

9：

7：

8：

14：

10：

13：

11：

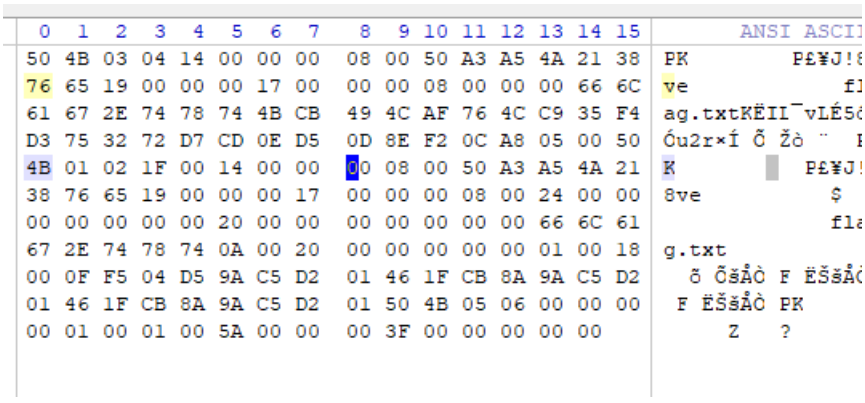
12：

倒数第六列 连起来，注意要换成小写

flag{xsxsbugkuadmin}

11.

这个就是伪加密，直接winhex改就好。



flag{Adm1N-B2G-kU-SZIP}

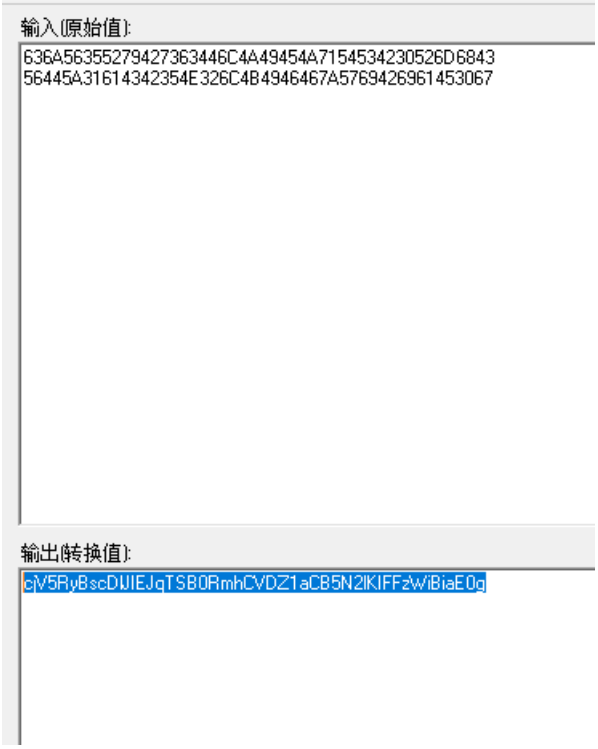
12.

告诉你个秘密(ISCCCTF)

100

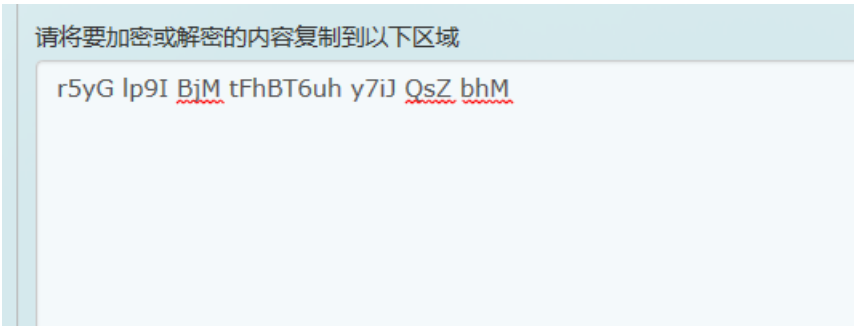
636A56355279427363446C4A49454A7154534230526D6843
56445A31614342354E326C4B4946467A5769426961453067

一看这个格式应该是十六进制，直接转成字符：



cjV5RyBscDlJlEJqTSB0RmhCVDZ1aCB5N2lKlFFzWiBiaE0g

试试base64：



r5yG lp9I BjM tFhBT6uh y7iJ QsZ bhM

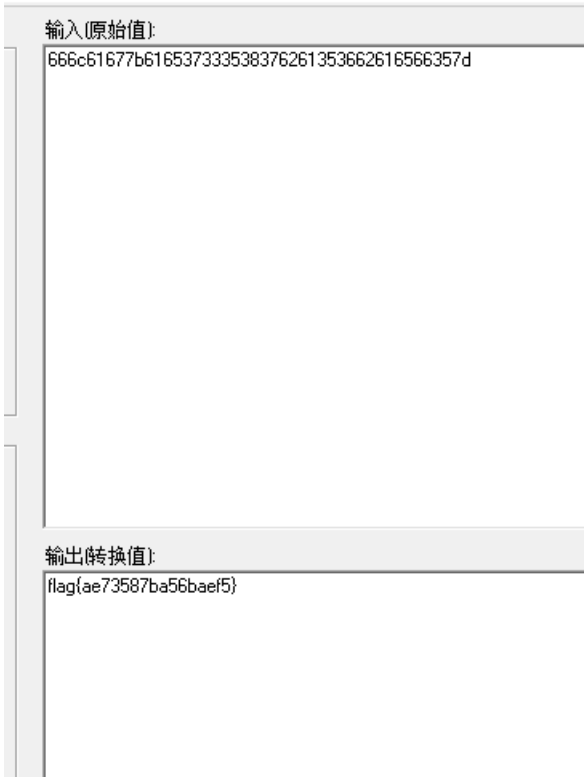
低头看键盘：

t o n g y u a n

这个提交的时候 直接提交 TONGYUAN就好

13.

不是MD5就是十六进制，。。没想到直接转换就搞出来了：



flag{ae73587ba56baef5}

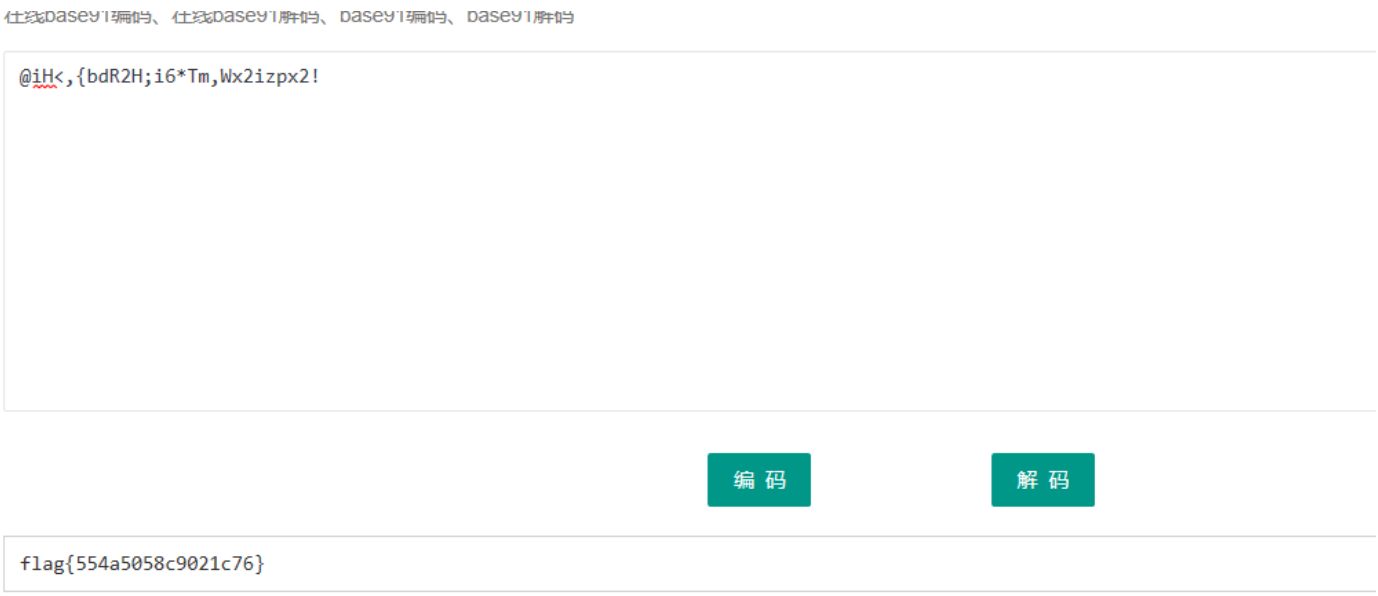
14.

base家族 16 32 64 都试过了。。。没想到还有什么 92 91.。。

结果是base91 真的牛批。

网址：

ctf.ssleye.com/base91.html



flag{554a5058c9021c76}

15.

社会主义核心价值观编码。。。。

还是那个网站：

http://ctf.ssleye.com/cvencode.html

flag{90025f7fb1959936}

16.


```
d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101 b1101100 o141 d105 x62 d101 b1101001 d46 o40 d71 x69
d102 d108 d97 o147 d123 x31 b1100101 b110100 d98 d102 b111000 d49 b1100001 d54 b110011 x39 o64 o144 o145 d53 x61 b1100010
d111 d111 x64 d32 o164 b1101001 x6d o145 x7e
```

有十进制(d开头的) 二进制(b开头) 八进制(o开头) 十六进制(x开头)

直接写脚本：

```
a = "d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101 b1101100 o141 d105 x62 d101 b1101001 d46 o40 d71 x69 d118 x65 x20 b1111001 o157 b1110101 d32 o141 d32 d102 o154 x61 x67 b100000 o141 d115 b100000 b1100001 d32 x67 o151 x66 d116 b101110 b100000 d32 d102 d108 d97 o147 d123 x31 b1100101 b110100 d98 d102 b111000 d49 b1100001 d54 b110011 x39 o64 o144 o145 d53 x61 b1100010 b1100011 o60 d48 o65 b1100001 x63 b110110 d101 o63 b111001 d97 d51 o70 d55 b1100010 d125 x20 b101110 x20 b1001000 d97 d118 o145 x20 d97 o40 d103 d111 d111 x64 d32 o164 b1101001 x6d o145 x7e"

b = a.split(" ")

print b

answer = ""

for i in b:

print i

if i[0] == 'b':

answer += chr(int(i[1:], 2))

if i[0] == 'o':

answer += chr(int(i[1:], 8))

if i[0] == 'd':

answer += chr(int(i[1:]))

if i[0] == 'x':

answer += chr(int(i[1:], 16))

print(answer)
```

```
Welcome to kelaibei. Give you a flag as a gift.  flag{1e4bf81a6394de5abc005ac6e39a387b} . Have a good time~
```

flag{1e4bf81a6394de5abc005ac6e39a387b}

17.

函数就是仿射密码了，直接脚本就行：

data = 'szzyfimhyzd'

```
res = ''
for x in data:
x = ord(x)
for i in range(0,26):
if x == (17*i-8)%26+97:
res += chr(i+97)
print res
```

```
affineshift
```

flag{affineshift}

18.

这个参考了别人的，这是linuxshadow文件。直接用john工具就好(linux才有)

```
root@kali:~/shadows# john shadow
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
hellokitty       (root)
1g 0:00:00:06 DONE 2/3 (2019-02-03 14:23) 0.1652g/s 830.2p/s 830.2c/s 830.2C
lovegod..celtic
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/shadows# john shadow --show
root:hellokitty:17770:0:99999:7:::
1 password hash cracked, 0 left
root@kali:~/shadows#
```

flag{hellokitty}

19.

来自宇宙的信号

110

银河战队出击

flag格式 flag{字母小写}

201710211808...

图片：

这个是什么。。标准银河字母：

flag{nopqrst}

这就把密码学的都写完了。。。今天再更别的。。这个写到这。