

淮工CTF——crypto部分wp

原创

柳尘笙 已于 2022-04-21 22:28:47 修改 112 收藏

文章标签: [经验分享](#)

于 2022-04-21 15:48:45 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_42820704/article/details/124323400

版权

目录

Crypto

[天上掉馅饼](#)

[Ez凯撒](#)

[好的大学, 没有___](#)

[呃呃呃](#)

[Ez_Mixed](#)

[一杯再一杯~](#)

[简单简单超简单](#)

天上掉馅饼

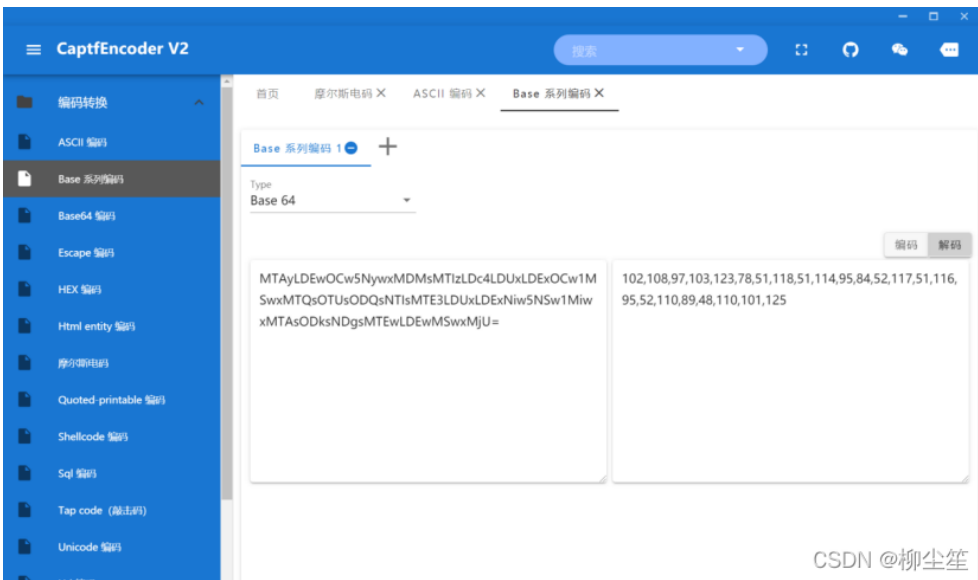
下载得c++文件, 用Notepad++打开得:



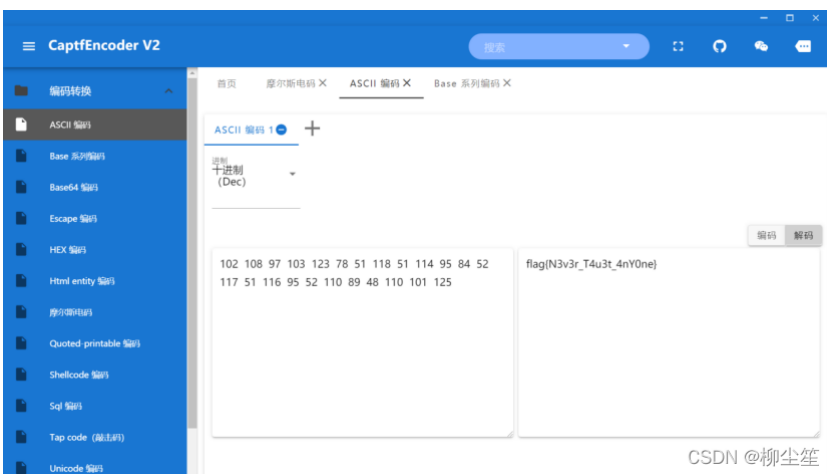
```
1 #include <iostream>
2 using namespace std;
3 int main()
4 {
5     //Let me tell you a secret: flag is in m2
6     char m1[]="MTAyLDEwOCw5NywzMjMzLDE0LDEwOCw1MSwzMTQsOTUsODQsMTIeMTE3LDEwOCw1NSwzMTIwMTAsODkzNDQsMTEwLDEwMScwMjU=";
7     int m2[]={72,97,104,97,104,97,44,32,121,111,117,39,118,101,32,98,101,101,110,32,99,104,101,97,116,101,100,33};
8     return 0;
9 }
10
```

CSDN @柳尘笙

Base64解码m1字符串:



再用ascii编码得：

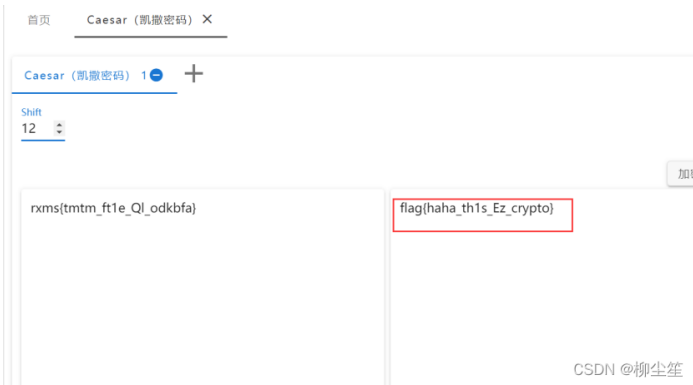


Ez凯撒

题目：



那就凯撒呗：



就在刚刚发生

题目：



看不懂，复制到度娘上查一下：



找到了一种语言：克苏鲁语（Cthuvian）词典



对照密文翻译即可：

-agl(后缀)	place	地方
ah	generic action, e.g. greet, eat, do	指称某类动作的一般形式, 如: 打招呼, 吃饭, 做
'ai	speak / call	说话, 呼叫, 称, 召唤
athg	sign (contract) / agree to	签订 (契约), 同意, 达成共识
'bthnk	body / essence	身体、躯体, 本质、存在、实质
bug	go	走、退散
c-(前缀)	we / our	我们, 我们的
ch'	cross over / travel	跨越、交叉, 旅行、驾驶
chtenff	brotherhood / society	兄弟关系, 社会
ebumna	pit	陷阱、矿坑
ee	answers	答案
ehye	cohesion / integrity	粘附、结合、凝聚, 统一、完整
ep	after; with hai, later / then	在……之后、与 hai 连用意为稍后,
f'-(前缀)	they / their	
'fhalma	mother	
fhtag	wait / sleep	
fm'latgh	burn	
ftaghu	skin / boundary	
geb	here	
gnaiih	father	
gof'nn	children	
goka	grant	
gotha	wish	
grah'n	lost one/ larva	
h'-	it/its	

新建文本文档.txt - 记事本
 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
 kn'a_ee_hupadgh_n'gha
 question_answers_born_of_death

CSDN @柳尘笙

好的大学，没有__

题目：



Base64解码得：



CSDN @柳尘笙

再用栅栏爆破：

```

===== RESTART: D:\桌面\venk.py =====
==
i=2
h1303gc_nf_0_1f0ry3nd_te3C0(HG4

i=3
hv0ngtNC)H1033c_3_[41y3dcef00Gf

i=4
h33g_f_f0ym_eC(G10ccN_01v3dt30H4

i=5
hyctf{1004_C0413ge_Hfv3_N0_3nc3}G

i=6
h0gN_103_3{413cf0fvntCH3c_ymde0G

i=7
h3cC_03t_G1n_01vce}43dN{fyg300_fH

i=8
h3_f0me{1cN0vd3H3gf_y_C00c_13t04

i=9
hmN0c3_1dfGvgC13_4yc0f0t}3_3e0

```

```

venk.py - C:\Users\venk\py (3.10.4)
File Edit Format Run Options Window Help

def fenceEncode(m, key):
    text = ''
    k = int(key)
    for i in range(k):
        text += m[i::k]
    return text

def fenceDecode(c, key):
    text = ''
    k = len(c) // int(key)
    for i in range(k):
        text += c[i::k]
    return text

if __name__ == '__main__':
    m = 'h01v3y033ncdg_ct_eN3fC_0{0H_G144'
    for i in range(2, 26):
        c = fenceEncode(m, i)
        print(f'i={i}d%i')
        print(c)
        print('\n')
        #print(fenceDecode(c, i))

```

CSDN @柳尘笙

呃呃呃

下载得题目文件：

```

No.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
^w^/= / m` / ~11 //^v` / [ _ ]; o=(^-) =_3; c=(^O) =(^-)-(^-); (^D) =(^O)
^)= (o^_o)/(o^_o); (^D) =(^O); w^/=(^=3) +_); [^O] ;^- /:(^w^ / +_ )
[o^_o-(^O)]; (^D) /:(^-)=3) +_); [^-]; (^D) [^O] =( (^w^ / =3) +_ ) [c^_o]; (^D)
[^c] =( (^D) +_ ) [ (^-)+(^-)-(^O) ]; (^D) [^o] =( (^D) +_ ) [^O] ; (^o) =( (^D)
[^c]+(^D) [^o]+(^w^ / +_ ) [^O] + ((^w^ / =3) +_ ) [^-] + ((^D) +_ ) [ (^-)+(^-)] +
((^-)=3) +_ ) [^O] + ((^-)=3) +_ ) [ (^-)- (^O) ] + (^D) [^c] + ((^D) +_ )
[ (^-)+(^-)] + (^D) [^o] + ((^-)=3) +_ ) [^O] ; (^D) [ _ ] =(o^_o) [^o] [^o]; (^e) =(
[ (^-)=3) +_ ) [^O] + (^D) ; (^D) /+( (^D) +_ ) [ (^-)+ (^-)] + ((^-)=3) +_ ) [o^_o-
^O] + ((^-)=3) +_ ) [^O] + (^w^ / +_ ) [^O] ; (^-)+ (^O) ; (^D) [^e] =\; (^D) ; ^O /
=( (^D) + (^-)) [o^_o-(^O)]; (o^-o) =( (^w^ / +_ ) [c^_o]; (^D) [^o] =\; (^D) [ _ ] ( (^D
^ ) [ _ ] (^e + ^v` ^ / (^D) [^o] + (^D) [^e] + (^O) + (^-)+ ((o^_o) + (o^_o) + (^D) [^e
^ ] + (^O) + ((^-) + (^O)) + (^-)+ (^D) [^e] + (^O) + (^-)+ (^O) + (^D) [^e] + (^O) + (^-
)+ (^-)+ (o^_o) + (^D) [^e] + (^O) + (^-)+ (o^_o) + (o^_o) + (^D) [^e] + (^
O) + (^O) + (c^_o) + (^D) [^e] + (^O) + (^-)+ (^-)+ (^O) + (^D) [^e] + (^O) + ((^-)
+ (^O)) + (^-)+ (^D) [^e] + (^O) + ((^-) + (^O)) + (^D) [^e] + ((o^_o)
+ (o^_o) + (c^_o) + (^D) [^e] + (^O) + (o^_o) + ((^-) + (o^_o) + (^D) [^e] + (^
O) + (o^_o) - (^O)) + ((^-) + (o^_o) + (^D) [^e] + ((o^_o) + (o^_o) + (c^_o) + (^D)
[ ^e] + (^O) + ((o^_o) + (o^_o) + (o^_o) - (^O)) + (^D) [^e] + ((o^_o)
+ (o^_o) + (^O) + (^D) [^e] + (^O) + (^-)+ (^-)+ (^D) [^e] + (^O) + ((^-) +
(o^_o) + ((^-) + (^O)) + (^D) [^o] ) (^O) ) (^-);

```

CSDN @柳尘笙

是颜文字AAEncode加密，在线解码得：

☆ www.atoolbox.net/Tool.php?id=703

好用的在线工具都在这里！

AAEncode加密/解密

```

^w^/= / m` / ~11 //^v` / [ _ ]; o=(^-) =_3; c=(^O) =(^-)-(^-); (^D) =(^O) =(o^_o)/(o^_o)
+_) [^-]; (^D) [^O] =( (^w^ / =3) +_ ) [o^_o]; (^D) [c] =( (^D) +_ ) [ (^-)+(^-)-(^O) ]; (^D) [^o]
[ (^-)+(^-)] + ((^-)=3) +_ ) [^O] + ((^-)=3) +_ ) [ (^-)- (^O) ] + (^D) [^c] + ((^D) +_ ) [ (^-)+(^-)] +
(^D) /+( (^D) +_ ) [ (^-)+ (^-)] + ((^-)=3) +_ ) [o^_o- ^O] + ((^-)=3) +_ ) [^O] + (^w^ / +_ ) [^O] ; (^-
o) =\; (^D) [ _ ] ( (^D) [ _ ] (^e + ^v` ^ / (^D) [^o] + (^D) [^e] + (^O) + (^-)+ ((o^_o) + (o^_o) + (^D)
(o^_o) + (^D) [^e] + (^O) + ((^-) + (o^_o) + (o^_o) + (^D) [^e] + (^O) + (^-)+ (^O) + (^D) [^e] + (^O)
(^-)+ (^D) [^e] + ((o^_o) + (o^_o) + (o^_o) + (^D) [^e] + (^O) + (o^_o) + ((^-) + (o^_o) + (^D) [^e] + (^
(o^_o) + (o^_o) + (c^_o) + (^D) [^e] + (^O) + ((^-) + (o^_o) + (o^_o) + (^D) [^e] + (^O) + ((^-) +
(o^_o) + (o^_o) - (^O)) + ((^-) + (o^_o) + (^D) [^e] + ((o^_o) + (o^_o) + (c^_o) + (^D) [^e] + (^O) + ((^-) +
(o^_o) + ((^-) + (^O)) + (^D) [^o] ) (^O) ) (^-);

```

加密

flag{Hello_W0rld};

CSDN @柳尘笙

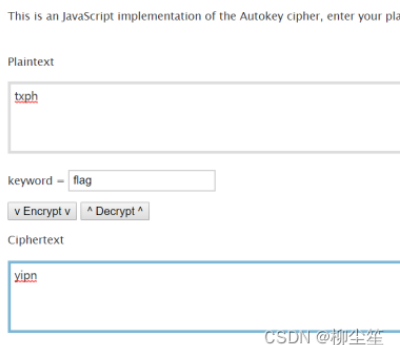
Ez_Mixed

题目:

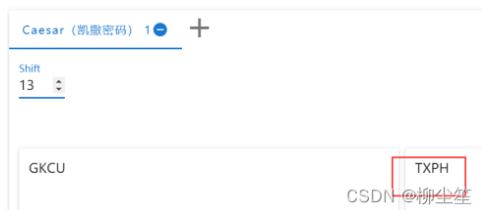


猜测是Vigenere加密, key也被加密了, 但显示是4位字母, 密文格式也符合flag{}

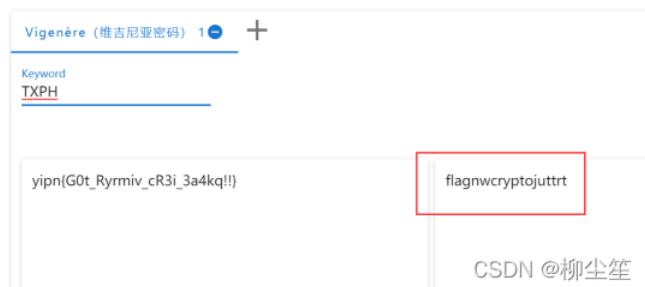
猜测密文中的yipn对应flag, 逆推出key:



尝试凯撒解密进行验证, 当偏移量为13时出现:



将其作为密钥key进行解密:



进行格式还原得:

flag{N0w_crypto_ju3t_3t4rt!!}

一杯再一杯~

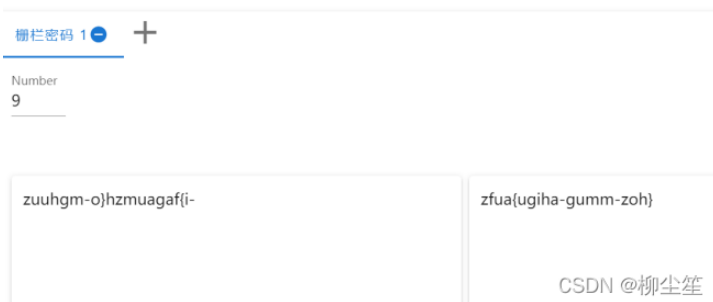
题目:



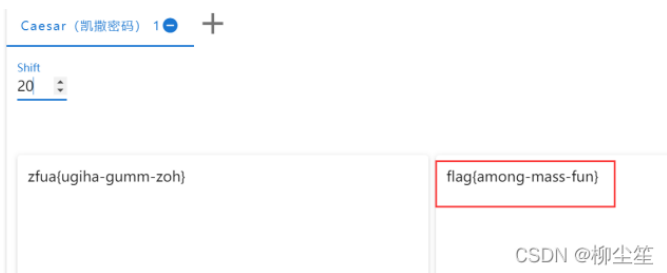
Base64解码得:



然后使用栅栏加密，将大括号弄到相应位置:

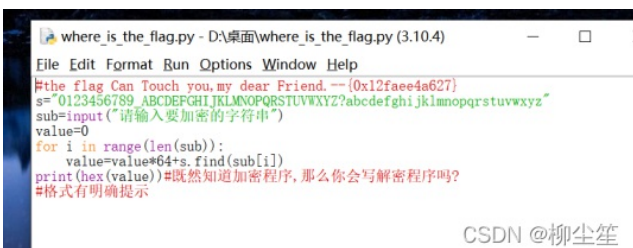


最后用凯撒解密:



简单简单超简单

下载得py脚本:



跑几次摸清计算过程，然后写逆运算程序:

(不擅长python,我还能写c?)

```
int main()
{
    char s[] = "0123456789_ABCDEFGHIJKLMNOPQRSTUVWXYZ?abcdefghijklmnopqrstuvwxyz";
    long long sum = 1304309311015;
    int i;

    for (;sum>0;)
    {
        for (i = 0; i < 64; i++)
        {
            if (((sum - i) % 64) == 0)
            {
                printf("%c", s[i]);
                sum = (sum - i) / 64;
                break;
            }
        }
    }

    printf("\n");
    return 0;
}
```

Microsoft Visual Studio 调试控制台
bN_tiyH
D:\编程\项目\Project1\Debug\Project1.e...
要在调试停止时自动关闭控制台, 请启用“...
按任意键关闭此窗口. . .

CSDN @柳尘笙

跑出flag。