淮工CTF——crypto部分wp

原创

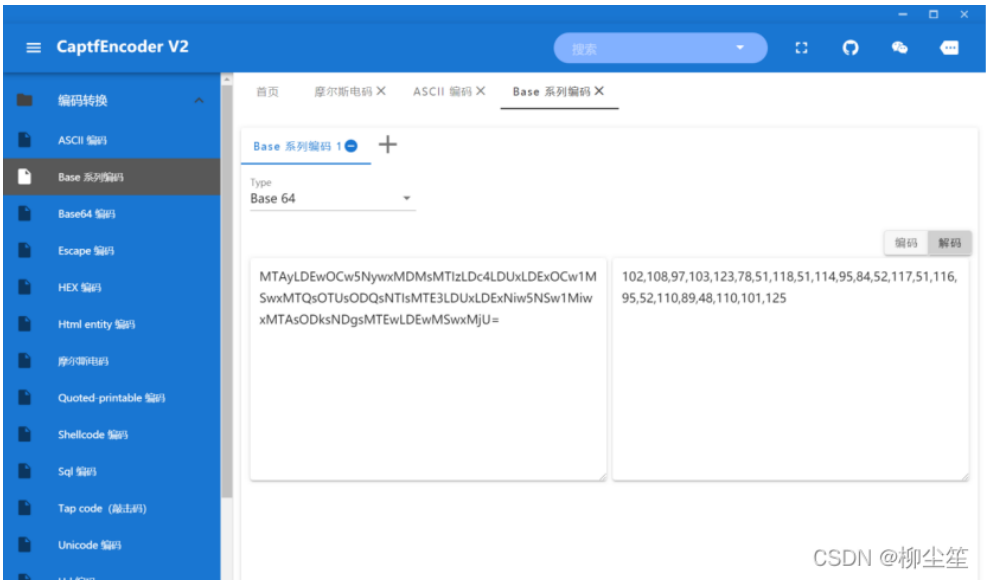
柳尘笙 已于 2022-04-21 22:28:47 修改 112 收藏
文章标签： 经验分享
于 2022-04-21 15:48:45 首次发布

目录

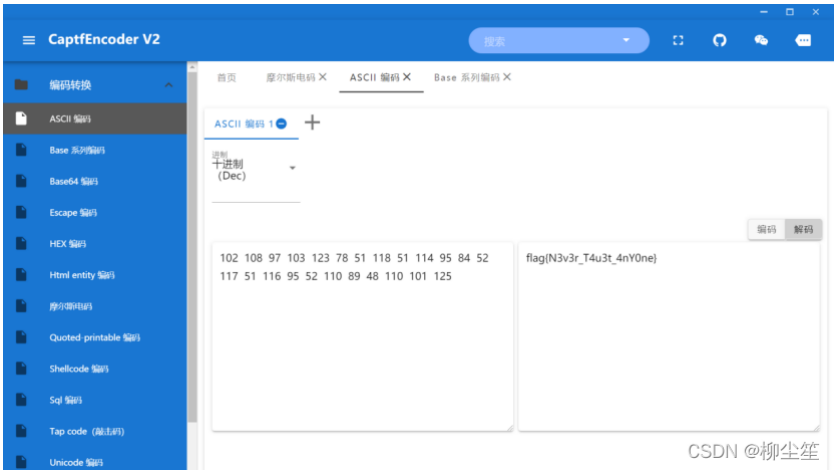
天上掉馅饼

下载得c++文件，用Notepad++打开得：

Base64解码m1字符串：

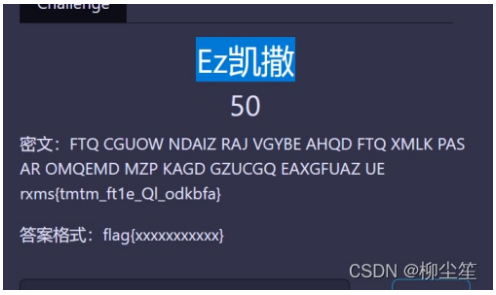


再用ascii编码得：

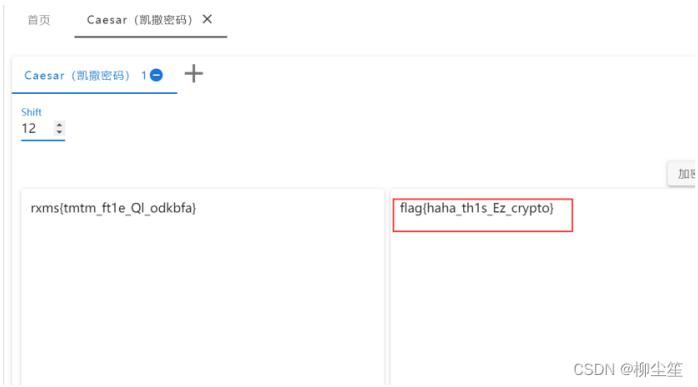


Ez凯撒

题目：



那就凯撒呗：



就在刚刚发生

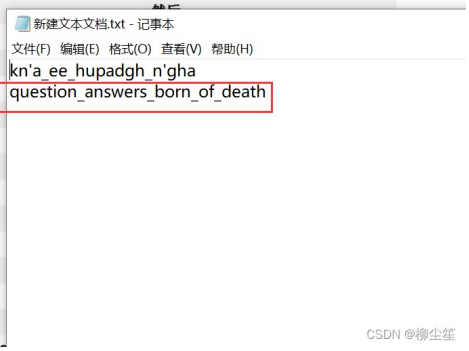
题目：

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，然后
f’-(前缀)	they / their	
‘fhalma	mother	
fhtagn	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	



好的大学，没有___

题目：

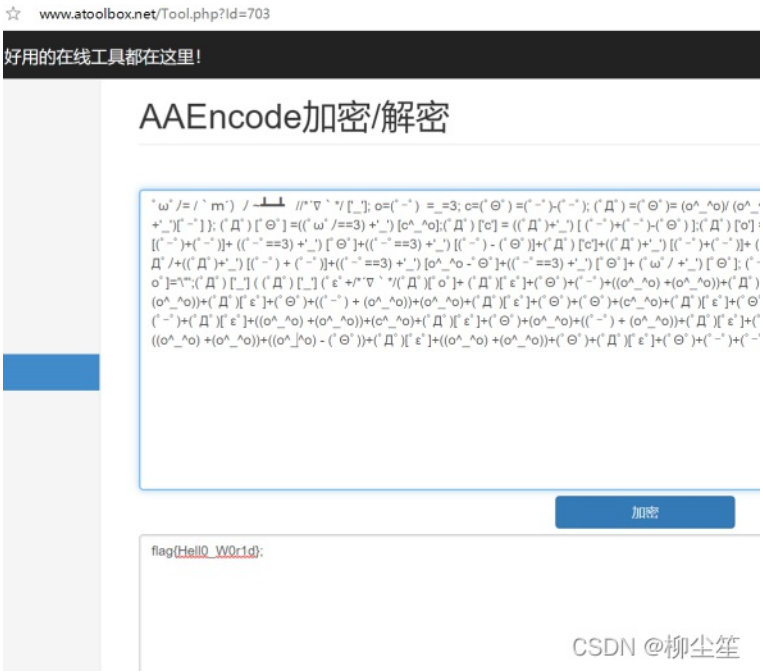
Base64解码得：

再用栅栏暴破：

呃呃呃

下载得题目文件：

是颜文字AAEncode加密，在线解码得：



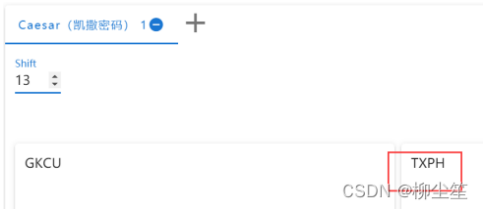
Ez_Mixed

题目：

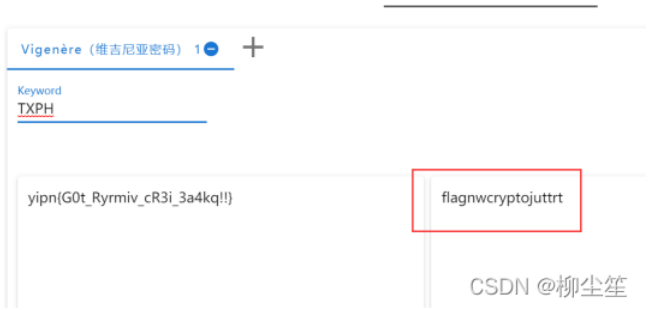
猜测是Vigenere加密，key也被加密了，但显示是4位字母，密文格式也符合flag{}，

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：



将其作为秘钥key进行解密：



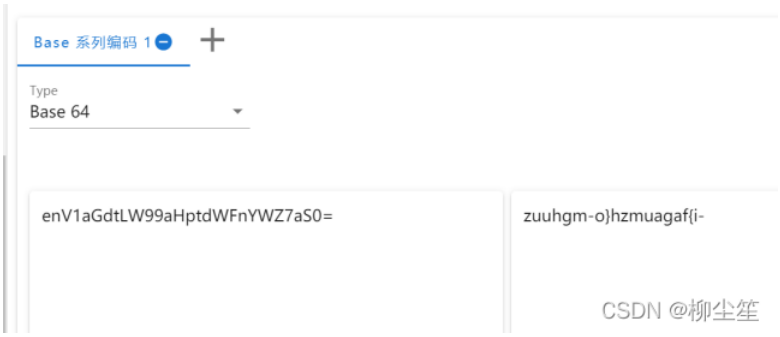
进行格式还原得：

flag{N0w_crypto_ju3t_3t4rt!!}

一杯再一杯~

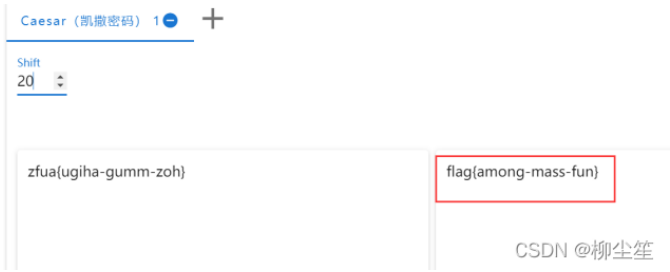
题目：

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：

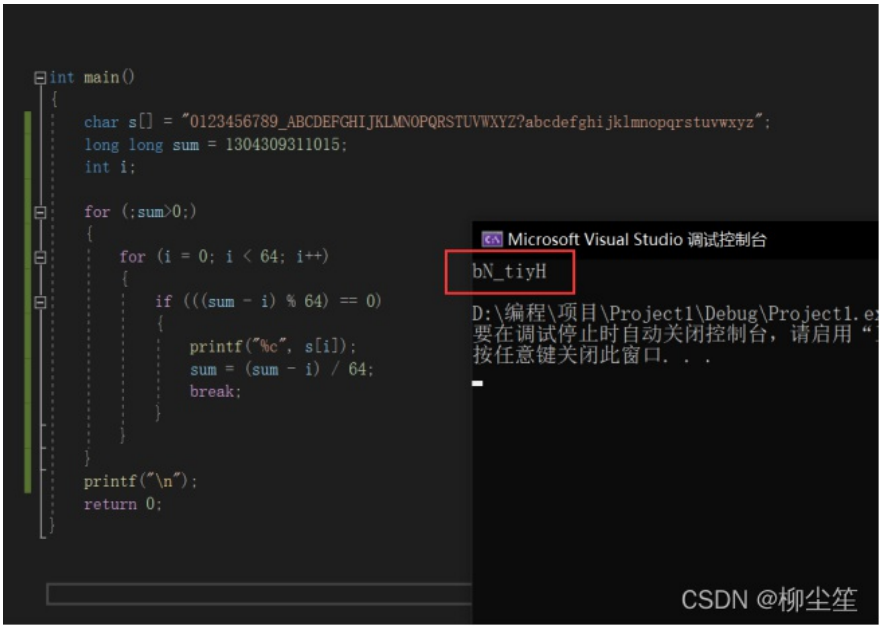


简单简单超简单

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,我还不能写c？）



跑出flag。