

BUUCTF Crypto部分题总结

原创

qiushuo29 于 2021-08-10 20:26:58 发布 141 收藏

分类专栏: [CTF密码学](#)

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/qiushuoxiaobai/article/details/119577349>

版权



[CTF密码学 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

1.Quoted-printable

题目 解题快手榜

Quoted-printable

1

注意: 得到的 flag 请包上 flag{} 提交

8114846c-d...

Flag

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
=E9=82=A3=E4=BD=A0=E4=B9
=9F=E5=BE=88=E6=A3=92=E5=
93=A6
100% Windows (CRLF) UTF-8 shuo/xiaobai
```

首先看到题目所给的密码并非常见的密码, 搜索一下题目Quoted-printable, 查看一下相关信息

quoted-printable 就是说用一些**可打印常用字符**, 表示一个字节 (8位) 中所有非打印字符方法! . **Quoted-printable**编码方法. 任何一个8位的字节值可编码为3个字符: 一个等号" =" 后跟随两个十六进制数字 (0-9或A-F)表示该字节的数值.例如, ASCII码换页符 (十进制值为12) 可以表示为" =0C" , 等号" =" (十进制值为61) 必须表示为" =3D" . 除了可打印ASCII字符与换行符以外, 所有字符必须表示为这种格式.

Quoted-printable编码

quoted-printable

=E9=82=A3=E4=BD=A0=E4=B9=9E=E5=BE=E6=A3=92=E5=93=A6

字符集 utf8(unicode编码)

编码 解码

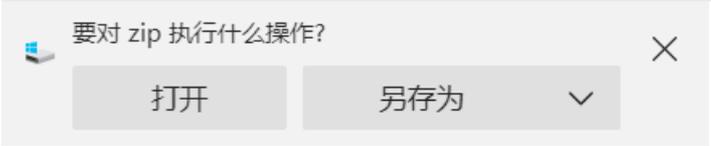
那你也很棒哦 <https://blog.csdn.net/qiushuoxiaobai>

了解了相关信息后，搜索相关工具

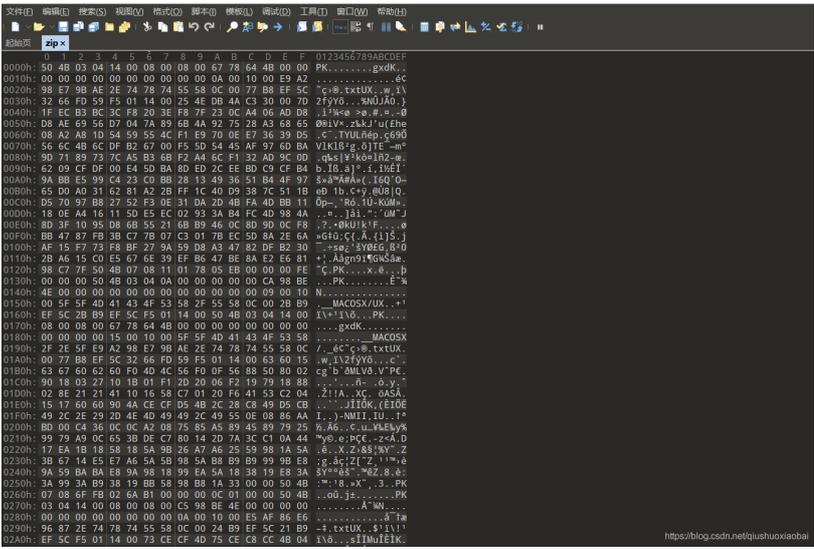
解码后发现flag“那你也很棒哦”

小结：遇到英文字母和数字两两混合且用“=”连接，要想起Quoted-printable编码。

2.大帝的密码武器

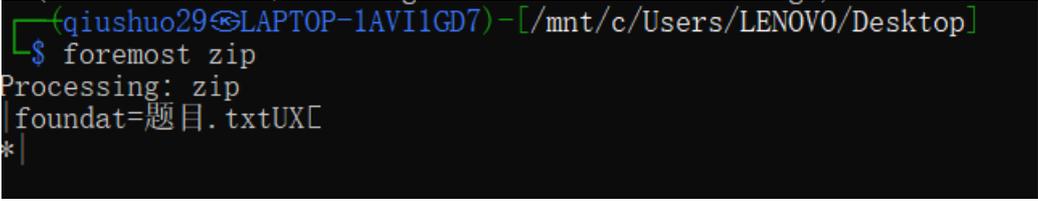


下载题目，得到zip文件无法打开，使用010editor



查看文件头为 50 4B 为zip文件的文件头，无法得到压缩包

尝试使用kali Linux的foremost功能分离文件



可分离出 题目.txt 在output文件夹中



得到flag: ComeChina

小结: 根据提示的zip文件, 无法得到更多的题目信息, 可以尝试使用foremost分离, 得到更多信息。

3.信息化时代的步伐

题目 解题快手榜

信息化时代的步伐

1

也许中国可以早早进入信息化时代, 但是被清政府拒绝了。附件中是数十年后一位伟人说的话的密文。请翻译出明文(答案为一串中文!)注意: 得到的 flag 请包上 flag{} 提交

a9bbf4f5-ef...

Flag

信息化时代的步伐 - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

606046152623600817831216121621196386

https://blog.csdn.net/qiushuoxiaobai

题目中提示答案为 一串中文, 所给的密码是一串数字, 着手数字转化为中文, 此时作者第一时间想到的是九键输入, 观察其中多有0, 00等应无法得出较好的中文的信息, 转换思路

附件是清政府拒绝的数十年后，年代较早，想起了中文电码一说，查找中文电码工具，

中文电码反查汉字结果:

- 6060: 计
- 4615: 算
- 2623: 机
- 6008: 要
- 1783: 从
- 1216: 娃
- 1216: 娃
- 2119: 抓
- 6386: 起

<https://blog.csdn.net/qjushuoxiaobai>

使用工具转化后，得到flag：计算机要从娃娃抓起

小结：中文与数字间的转换，要记得中文电码。

4.世上无难事

世上无难事

1

以下是某国现任总统外发的一段指令，经过一种奇异的加密方式，毫无规律，看来只能分析了。请将这段语句还原成通顺语句，并从中找到key作为答案提交，答案是32位，包含小写字母。注意：得到的flag请包上flag{}提交

[d5e7c907-a...](#)

Flag

提交

```
VIZZB IFIUQJBWO NVXAP OBC XZZ UKHVN IFIUQJBWO  
HB XVIXW XAW VXFI X QIXN VBD KQ IFIUQJBWO  
WBKAH NBWYO VBD XJBCN NKG QLKEIU DI XUJ VIUI  
DKNV QNCWIANQ XN DXPIMKIZW VKHV QEVBBZ KA  
XUZKAHNBA FKUHKAIX XAW DI VXFI HBN QNCWIANQ  
NCAKAH KA MUBG XZZ XEUBQQ XGIUKEX MUBG  
PKAWIUHXUNIA NVUBCHV 12NV HUXWI XAW DI XUJ  
SCQN QB HZXW NVXN XZZ EBCZW SBKA CQ NBWYO  
XAW DI DXAN NB NVXAP DXPIMKIZW MBU JIKAH  
QCEV XA BCNQNXAWKAH VBQN HKFI OBCUQIZFIQ X  
JKH UBCAW BM XLLZXCQJ XAW NVI PIO KQ  
64011012805M211J0XJ24MM02X1IW09
```

观察密码发现，此密码不同于base密码，观察其中英文字母间有间隔，像是用凯撒加密过的英文语段，使用凯

AmanCTF - 凯撒(Caesar)加密/解密

在线凯撒(Caesar)加密/解密

VIZZB IFIUQJBWO NVXAP OBC XZZ UKHVN IFIUQJBWO HB XVIXW XAW VXFI X QIXN VBD KQ IFIUQJBWO WBKAH NBWYO VBD XJBCN NKG QLKEIU DI XUJ VIUI DKNV QNCWIANQ XN DXPIMKIZW VKHV QEVBBZ KA XUZKAHNBA FKUHKAIX XAW DI VXFI HBN QNCWIANQ NCAKAH KA MUBG XZZ XEUBQQ XGIUKEX MUBG PKAWIUHXUNIA NVUBCHV 12NV HUXWI XAW DI XUJ SCQN QB HZXW NVXN XZZ EBCZW SBKA CQ NBWYO XAW DI DXAN NB NVXAP DXPIMKIZW MBU JIKAH QCEV XA BCNQNXAWKAH VBQN HKFI OBCUQIZFIQ X JKH UBCAW BM XLLZXCQJ XAW NVI PIO KQ 64011012805M211J0XJ24MM02X1IW09

偏移量

VIZZB IFIUQJBWO NVXAP OBC XZZ UKHVN IFIUQJBWO HB XVIXW XAW VXFI X QIXN VBD KQ IFIUQJBWO WBKAH NBWYO VBD XJBCN NKG QLKEIU DI XUJ VIUI DKNV QNCWIANQ XN DXPIMKIZW VKHV QEVBBZ KA XUZKAHNBA FKUHKAIX XAW DI VXFI HBN QNCWIANQ NCAKAH KA MUBG XZZ XEUBQQ XGIUKEX MUBG PKAWIUHXUNIA NVUBCHV 12NV HUXWI XAW DI XUJ SCQN QB HZXW NVXN XZZ EBCZW SBKA CQ NBWYO XAW DI DXAN NB NVXAP DXPIMKIZW MBU JIKAH QCEV XA BCNQNXAWKAH VBQN HKFI OBCUQIZFIQ X JKH UBCAW BM XLLZXCQJ XAW NVI PIO KQ 64011012805M211J0XJ24MM02X1IW09

UHYVA HEHTNIAVN MUWZO NAB WYY TJGUM HEHTNIAVN GA WUHWV WZY UWEH W PHWM UAC JP HEHTNIAVN VAJZG MAVWN UAC WIABM MJF PKJDHT CH WTH UHTH CJMU PMBVHZMP WM CWOHLJHYV UJGU PDUUAY JZ

撒(Caesar)加密/解密 - Bugku CTF工具枚举后

并未发现结果，尝试使用quipqiup工具爆破quipqiup - cryptoquip and cryptogram solver

将密文输入

```
0 -1.534 HELLO EVERYBODY THANK YOU ALL RIGHT EVERYBODY GO AHEAD AND HAVE A SEAT HOW IS EVERYBODY DOING TODAY HOW ABOUT TIM SPICER WE ARE HERE WITH STUDENTS AT WAKEFIELD HIGH SCHOOL IN ARLINGTON VIRGINIA AND WE HAVE GOT STUDENTS TUNING IN FROM ALL ACROSS AMERICA FROM KINDERGARTEN THROUGH 12TH GRADE AND WE ARE JUST SO GLAD THAT ALL COULD JOIN US TODAY AND WE WANT TO THANK WAKEFIELD FOR BEING SUCH AN OUTSTANDING HOST GIVE YOURSELVES A BIG ROUND OF APPLAUSE AND THE KEY IS 640E11012805F211B0AB24FF02A1ED09

1 -4.126 MILLO ITIKYBODY EMANC YOR ALL KUGME ITIKYBODY GO AMIAD AND MATI A SIAE MOP US ITIKYBODY DOUNG BODAY MOP ABORE EUV SZUWIK PI AKI MIKI PUEM SERDINES AE PACIJUILD MUGM SWMOOL UN AKLINGEON TUKGUNIA AND PI MATI GOE SERDINES BRNUNG UN JKOV ALL AWKOSS AVIKUWA JKOV CUNDIKGAKESIN EMKORGH 12EM GKADI AND PI AKI FRSE SO GLAD EMAB ALL WORLD FOUN RS BODAY AND PI PANE EO EMANC PACIJUILD JOK BIUNG SRWM AN ORESEANDUNG MOSE GUTI YORKSILTIS A BUG KORND OJ AZZLARS I AND EMI CIY US 640I11012805J211B0AB24JJ02A1ID09

2 -4.157 HILLO IMITERODE SHANK EOW ALL TUGHS IMITERODE GO AHIAD AND HAMI A KIAS HOP UK IMITERODE DOUNG SODAE HOP AROWS SUV KYUCIT PI ATI HITI PUSH KSWDINSK AS PAXIFUULD HUGH KCHOOL UN ATLINGEON MUTGUNIA AND PI HAMI GOE KSWDINSK SWNUNG UN FTOV ALL ACTOKK AVITUCA FTOV XUNDITGATSIN SHTOWGH 12SH GTADI AND PI ATI BWKS KO GLAD SHAS ALL COWLD BOUN WK SODAE AND PI PANS SO SHANK PAXIFUULD POT RIUNG KWCH AN OWSEKANDUNG HOKS GUMI BOWTRILMIK A RUG TOWND OF AYLLAWKI AND SHI XIE UK 640I11012805F211R0AR24FF02A1ID09

3 -4.162 MOLLU OKORYBUDY EMANC YUX ALL RIGME OKORYBUDY GU AMOAD AND MAKO A SOAE MUT IS OKORYBUDY DUNG EUDAY MUT ABUXE EIZ SFIHOR TO ARO MORO TIEM SEXDONES AE TACOPIOLD MIGM SHMUUL IN ARLINGEON KIRGINIA AND TO MAKO GUE SEXDONES EXNING IN PRUZ ALL AHRUSS AZORIIA PRUZ CINDORGAREON EMRUXGM 12EM GRADO AND TO ARO QXSE SU GLAD EMAB ALL HUXLD QUIN XS EUDAY AND TO TANE EU EMANC TACOPIOLD PUR BOING SXHM AN UXESEANDUNG MUSE GIKO YUXRSOLKOS A BIG RUXND UP AFFLAXSO AND EMO COY IS 640O11012805P211B0AB24PP02A1OD09

4 -4.178 HECCA EVERYZAKY THING YAP ICC ROSHT EVERYZAKY SA IHEIK INK HIVE I LEIT HAD OL EVERYZAKY KAONS TAKIY HAD IZAPT TOM LJOUER DE IRE HERE DOTH LTPKENTL IT DIGEBOECK HOSH LUHAAC ON IRCONSTAN VORSONOI INK DE HIVE SAT LTPKENTL TPWONS ON BRAM ICC IURALL IMEROUI BRAM GONKERSIRTEN THRAPHSH 12TH SRIKE INK DE IRE WPLT LA SCIK THIT ICC UAPCK WAON PL TARIY INK DE DINT TA THING DIGEBOECK BAR ZEONS LPUH IN APTLTIKONS HALT SOVE YAPRECVEL I ZOS RAPNK AB IJJCIPLA INK THE GEY OL 640E11012805E211Z0I224BB021EK09
```

<https://blog.csdn.net/qiushuoiaoba>

得到文段，THE KEY IS 640E11012805F211B0AB24FF02A1ED09

即可得到flag

小结：对特殊加密的英文语段，可以使用quipqiup工具进行爆破，观察是否可以得出结果。