




2021年大学生网络安全邀请赛暨第七届上海市大学生网络安全大赛“东华杯”Misc（全）-Writeup

原创

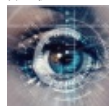
塞纳河畔的春水  于 2021-11-01 21:27:18 发布  6102  收藏 1

分类专栏: [CTF_Writeup](#) 文章标签: [安全](#) [网络安全](#) [python](#) [pycharm](#) [c++](#)

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_42815161/article/details/121076575

版权



[CTF_Writeup](#) 专栏收录该内容

8 篇文章 2 订阅

订阅专栏

文章目录

MISC

[checkin](#)

[project](#)

[JumpJumpTiger](#)

[where_can_find_code](#)

MISC

checkin

题目:

```
+AGYAbABhAGcAewBkAGgAYgBfADcAdABoAH0-
```

Magic一把梭, UTF-7编码

Input
length: 37
lines: 1
+

```
+AGYAbABhAGcAewBkAGgAYgBfADcAdABoAH0-
```

Output
time: 0ms
length: 37
lines: 1

Recipe (click to load)	Result snippet	Properties
Decode_text('UTF-7 (65000)')	flag{dhb_7th}	Valid UTF8 Entropy: 3.55

CSDN @塞纳河畔的春水

```
flag{dhb_7th}
```

project

(脑洞题披上工控题的外衣)

附件解压打开，发现可疑压缩包

File Name	Modified	Type	Size
pic00017.pic	2011/3/28 15:09	PIC 文件	29 KB
pic00018.pic	2011/3/28 15:09	PIC 文件	127 KB
pic00019.pic	2011/3/31 9:25	PIC 文件	131 KB
pic00020.pic	2011/3/31 9:25	PIC 文件	168 KB
pic00021.pic	2011/3/31 9:25	PIC 文件	830 KB
pic00022.pic	2011/3/31 9:25	PIC 文件	3,466 KB
pic00023.pic	2011/3/31 9:25	PIC 文件	694 KB
pic00024.pic	2011/3/31 9:26	PIC 文件	8 KB
pic00025.pic	2011/3/28 15:09	PIC 文件	5 KB
PICMANAG.DAT	2011/3/31 9:25	DAT 文件	1 KB
problem_bak.zip	2021/10/31 9:46	WinRAR ZIP 压缩...	69 KB
PROJECT.INF	1998/6/14 23:52	安装信息	1 KB
project.pro	2011/3/31 9:25	PRO 文件	1 KB
ProjManage.dat	2011/3/31 9:24	DAT 文件	1 KB
R1.RTF	2000/9/9 9:55	RTF 格式	3 KB
R2.RTF	2000/9/9 9:55	RTF 格式	10 KB
RDRQueryServer.dat	2011/3/31 9:26	DAT 文件	1 KB

CSDN @塞纳河畔的春水

解压之后拿到疑似流量数据，共三段。

前两段：

```
Date: Sun, 19 Sep 2021 21:28:55 +0800
From: "mk1kxxx@yeah.net" <mk1kxxx@yeah.net>
To: mk1kxxx <mk1kxxx@yeah.net>
Subject: =?UTF-8?B?5L2g5p2l5LqGfg==?=
X-Priority: 3
X-Has-Attach: no
X-Mailer: Foxmail 7.2.20.273[cn]
Mime-Version: 1.0
Message-ID: <202109192128112273138@yeah.net>
Content-Type: multipart/related;
  boundary="-----_001_NextPart057850482324_-----"
```

This is a multi-part message in MIME format.

```
-----_001_NextPart057850482324_-----
Content-Type: multipart/alternative;
  boundary="-----_002_NextPart832058858335_-----"
```

```
-----_002_NextPart832058858335_-----
Content-Type: text/plain;
  charset="UTF-8"
Content-Transfer-Encoding: base64
```

```
6KGo5o0F5YyF5paH5YyW77yM5piv6ZqP552A572R57uc56S+5Lqk5rKf6YCa55qE5aKe5aSa5Ye6
546w55qE5LiA56eN5Li75rWB5paH5YyW44CC5LiA5LiQ5Lq655qE6KGo5o0F5YyF5piv5Yw26ZqQ
6JeP6LW35p2l55qE55yf5oiR77yM5LiA5LiQ5Zu95a6255qE6KGo5o0F5YyF6YeM6I0955yL5Yiw
6L+Z5LiQ5Zu95a6255qE6KGo5o0F44CC4oCM4oCM4oCM4oCM4oC4oCs4oCs4oCM5pyJ5pe25YcZ
77yM6KGo5o0F5YyF6KGo6L6+55qE5piv5LiN6I096YGT56C055qE55yf5a6e5o0z5r0V5ZKM5oSf
5Y+X77yM6K+t6KiA5ZKM5paH5a2X55qE5bC95aS077yM5bCx5piv6KGo5o0F5YyF5pa95bGV55qE
56m66Ze044CCDQrooajmg4XlJIXmmK/nvZHnu5zor63oqIDnmoTkuIDnp43ov5vljJbvVzIz1roPn
moTkuqfnlJ/lkozmtYHooYzkuI7lhbbnbnlprnmoTigJzigIzigIzigIzigI3vu7/igI3i
gI3n1J/lrZjnjq/loopigJ3mnInlhbPjgILlhbboV73msYLphlPnm67jgIHmlrDlpYfjgIHosJDo
sJHnrYnmlYjmnprnmoTnibnngrrnvIzigIzigIzigIzigI3vu7/igIzigKzkuI7lubTovbvK
urrlvKDmiazkuKrmgKflkozmkJ7mgKrnmoTlv4PnkIbnm7jnrKbigIzigIzigIzigIzigI3vu7/i
gIzigKzjgIINCuihqOaDheWmheS5i+aJgOS7peiDveWkn+Wkp+iMg+WbtOWcsOS8oOaSre+8jOKA
jOKAjOKAjOKAjOKAje+7v+KArOKAjeaYr+WboOS4uuWftuW8peiHpeS6huaWh+Wt1+S6p0a1geea
hOaer+eHpeWsjOaAgeW6puihqoi+vuS4jehWhuehrueahOW8seeCue+8jOacieaViOWcsOaPkOmr
mOS6huayn+mAmuaViOeOh+OAgumDqOWIhuihqOaDheWmheWft+acieabv+S7o+aWh+Wt1+eahOWK
n+iDve+8jOKAjOKAjOKAjOKAjOKAje+7v+KAjeKAjei/mOWPr+S7peiKguecgeaJk+Wt1+aXtumX
tOKAjOKAjOKAjOKAjOKAje+7v+KAjOKAjOOAgumaj+edgOaZuuIDveaJi+acuuEahOWFqOmdouaZ
ruWPiuWSjOekvuS6pOW6lOeUqO9r+S7tueahOWkp+mHj+S9v+eUqO+8jOihqOaDheWmheW3sue7
j+mrmOmikeeOh+WcsOWHuueOsOWcQOS6uuS7rOeahOe9kee7nOiBiuWkqeWvveivneW9k+S4reOA
gg0K
```

```
-----_002_NextPart832058858335_-----
Content-Type: text/html;
  charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
```

```
<html><head><meta http-equiv=3D"content-type" content=3D"text/html; charse=
t=3DUTF-8"><style>body { line-height: 1.5; }body { font-size: 14px; font-f=
amily: "Microsoft YaHei UI"; color: rgb(0, 0, 0); line-height: 1.5; }body =
{ font-size: 14px; font-family: "Microsoft YaHei UI"; color: rgb(0, 0, 0);=
line-height: 1.5; }</style></head><body>=0A<div><div>=E8=A1=A8=E6=83=85=
```

=E5=8C=85=E6=96=87=E5=8C=96=EF=BC=8C=E6=98=AF=E9=9A=8F=E7=9D=80=E7=BD=91=
=E7=BB=9C=E7=A4=BE=E4=BA=A4=E6=B2=9F=E9=80=9A=E7=9A=84=E5=A2=9E=E5=A4=9A=
=E5=87=BA=E7=8E=B0=E7=9A=84=E4=B8=80=E7=A7=8D=E4=B8=BB=E6=B5=81=E6=96=87=
=E5=8C=96=E3=80=82=E4=B8=80=E4=B8=AA=E4=BA=BA=E7=9A=84=E8=A1=A8=E6=83=85=
=E5=8C=85=E6=98=AF=E5=85=B6=E9=9A=90=E8=97=8F=E8=B5=B7=E6=9D=A5=E7=9A=84=
=E7=9C=9F=E6=88=91=EF=BC=8C=E4=B8=80=E4=B8=AA=E5=9B=BD=E5=AE=B6=E7=9A=84=
=E8=A1=A8=E6=83=85=E5=8C=85=E9=87=8C=E8=83=BD=E7=9C=8B=E5=88=B0=E8=BF=99=
=E4=B8=AA=E5=9B=BD=E5=AE=B6=E7=9A=84=E8=A1=A8=E6=83=85=E3=80=82=E2=80=8C=
=E2=80=8C=E2=80=8C=E2=80=8C=E2=80=8D=E2=80=AC=E2=80=AC=E2=80=8C=E6=9C=89=
=E6=97=B6=E5=80=99=EF=BC=8C=E8=A1=A8=E6=83=85=E5=8C=85=E8=A1=A8=E8=BE=BE=
=E7=9A=84=E6=98=AF=E4=B8=8D=E8=83=BD=E9=81=93=E7=A0=B4=E7=9A=84=E7=9C=9F=
=E5=AE=9E=E6=83=B3=E6=B3=95=E5=92=8C=E6=84=9F=E5=8F=97=EF=BC=8C=E8=AF=AD=
=E8=A8=80=E5=92=8C=E6=96=87=E5=AD=97=E7=9A=84=E5=B0=BD=E5=A4=B4=EF=BC=8C=
=E5=B0=B1=E6=98=AF=E8=A1=A8=E6=83=85=E5=8C=85=E6=96=BD=E5=B1=95=E7=9A=84=
=E7=A9=BA=E9=97=B4=E3=80=82</div><div>=E8=A1=A8=E6=83=85=E5=8C=85=E6=98=AF=
=E7=BD=91=E7=BB=9C=E8=AF=AD=E8=A8=80=E7=9A=84=E4=B8=80=E7=A7=8D=E8=BF=9B=
=E5=8C=96=EF=BC=8C=E5=AE=83=E7=9A=84=E4=BA=A7=E7=94=9F=E5=92=8C=E6=B5=81=
=E8=A1=8C=E4=B8=8E=E5=85=B6=E7=89=B9=E5=AE=9A=E7=9A=84=E2=80=9C=E2=80=8C=
=E2=80=8C=E2=80=8C=E2=80=8C=E2=80=8D=EF=BB=BF=E2=80=8D=E2=80=8D=E7=94=9F=
=E5=AD=98=E7=8E=AF=E5=A2=83=E2=80=9D=E6=9C=89=E5=85=B3=E3=80=82=E5=85=B6=
=E8=BF=BD=E6=B1=82=E9=86=92=E7=9B=AE=E3=80=81=E6=96=B0=E5=A5=87=E3=80=81=
=E8=B0=90=E8=B0=91=E7=AD=89=E6=95=88=E6=9E=9C=E7=9A=84=E7=89=B9=E7=82=B9=
=EF=BC=8C=E2=80=8C=E2=80=8C=E2=80=8C=E2=80=8C=E2=80=8D=EF=BB=BF=E2=80=8C=
=E2=80=AC=E4=B8=8E=E5=B9=B4=E8=BD=BB=E4=BA=BA=E5=BC=A0=E6=89=AC=E4=B8=AA=
=E6=80=A7=E5=92=8C=E6=90=9E=E6=80=AA=E7=9A=84=E5=BF=83=E7=90=86=E7=9B=B8=
=E7=AC=A6=E2=80=8C=E2=80=8C=E2=80=8C=E2=80=8C=E2=80=8D=EF=BB=BF=E2=80=8C=
=E2=80=AC=E3=80=82</div><div>=E8=A1=A8=E6=83=85=E5=8C=85=E4=B9=8B=E6=89=80=
=E4=BB=A5=E8=83=BD=E5=A4=9F=E5=A4=A7=E8=8C=83=E5=9B=B4=E5=9C=B0=E4=BC=A0=
=E6=92=AD=EF=BC=8C=E2=80=8C=E2=80=8C=E2=80=8C=E2=80=8C=E2=80=8D=EF=BB=BF=
=E2=80=AC=E2=80=8D=E6=98=AF=E5=9B=A0=E4=B8=BA=E5=85=B6=E5=BC=A5=E8=A1=A5=
=E4=BA=86=E6=96=87=E5=AD=97=E4=BA=A4=E6=B5=81=E7=9A=84=E6=9E=AF=E7=87=A5=
=E5=92=8C=E6=80=81=E5=BA=A6=E8=A1=A8=E8=BE=BE=E4=B8=8D=E5=87=86=E7=A1=AE=
=E7=9A=84=E5=BC=B1=E7=82=B9=EF=BC=8C=E6=9C=89=E6=95=88=E5=9C=B0=E6=8F=90=
=E9=AB=98=E4=BA=86=E6=B2=9F=E9=80=9A=E6=95=88=E7=8E=87=E3=80=82=E9=83=A8=
=E5=88=86=E8=A1=A8=E6=83=85=E5=8C=85=E5=85=B7=E6=9C=89=E6=9B=BF=E4=BB=A3=
=E6=96=87=E5=AD=97=E7=9A=84=E5=8A=9F=E8=83=BD=EF=BC=8C=E2=80=8C=E2=80=8C=
=E2=80=8C=E2=80=8C=E2=80=8D=EF=BB=BF=E2=80=8D=E2=80=8D=E8=BF=98=E5=8F=AF=
=E4=BB=A5=E8=8A=82=E7=9C=81=E6=89=93=E5=AD=97=E6=97=B6=E9=97=B4=E2=80=8C=
=E2=80=8C=E2=80=8C=E2=80=8C=E2=80=8D=EF=BB=BF=E2=80=8C=E2=80=8C=E3=80=82=
=E9=9A=8F=E7=9D=80=E6=99=BA=E8=83=BD=E6=89=8B=E6=9C=BA=E7=9A=84=E5=85=A8=
=E9=9D=A2=E6=99=AE=E5=8F=8A=E5=92=8C=E7=A4=BE=E4=BA=A4=E5=BA=94=E7=94=A8=
=E8=BD=AF=E4=BB=B6=E7=9A=84=E5=A4=A7=E9=87=8F=E4=BD=BF=E7=94=A8=EF=BC=8C=
=E8=A1=A8=E6=83=85=E5=8C=85=E5=B7=B2=E7=BB=8F=E9=AB=98=E9=A2=91=E7=8E=87=
=E5=9C=B0=E5=87=BA=E7=8E=B0=E5=9C=A8=E4=BA=BA=E4=BB=AC=E7=9A=84=E7=BD=91=
=E7=BB=9C=E8=81=8A=E5=A4=A9=E5=AF=B9=E8=AF=9D=E5=BD=93=E4=B8=AD=E3=80=82</=
div></div><img src=3D"cid:_Foxmail.1@e1a633df-2fe4-f85c-7270-ca78308ac1c5"=
border=3D"0"></body></html>
-----_002_NextPart832058858335_-----

提取第一串base64解码，解密得到一段话，

表情包文化，是随着网络社交沟通的增多出现的一种主流文化。一个人的表情包是其隐藏起来的真我，一个国家的表情包里能看到这个国家。表情包是网络语言的一种进化，它的产生和流行与其特定的“生存环境”有关。其追求醒目、新奇、谐谑等特点，表情包之所以能够大范围地传播，是因为其弥补了文字交流的枯燥和态度表达不准确的弱点，有效地提高了沟通效率。部分表情包

```

input
length: 484    lines: 21
6KGo5o0F5YyF5paH5YyW77yM5piv6ZqP552A572R57uc56S+5Lqk5rKf6YCa55qE5aKe5aSa5Ye6
546w55qE5LiA56eN5Li75rWB5paH5YyW44CC5LiA5Liq5Lq655qE6KGo5o0F5YyF5piv5Yw26ZqQ
6Jep6LW35p2l55qE55yf5oiR77yM5LiA5Liq5Zu95a6255qE6KGo5o0F5YyF6YeM6IO955yL5Yiw
6L+Z5Liq5Zu95a6255qE6KGo5o0F44CC4oCM4oCM4oCM4oCM4oCs4oCs4oCM5pyJ5pe25YCZ
77yM6KGo5o0F5YyF6KGo6L6+55qE5piv5LiN6IO96YGT56C055qE55yf5a6e5o0z5r0V5ZKM5oSf
5Y+X77yM6K+t6KiA5ZKM5paH5a2X55qE5bc95aS077yM5bcx5piv6KGo5o0F5YyF5pa95bGV55qE
56m66Ze044CCDQrooajmg4XlJiXmmK/nvZHnu5zor63oqIDnmoTkuIDnp43ov5vljJbvvlzroPn
moTkuqfnlJ/lkozmtYHooYzkuI7lhbbnbnlRprnmoTigJzigIzigIzigIzigIzigI3vu7/igI3i
gI3nlJ/lrZjnjq/looPigJ3mnInlhbPjgILlhbbov73msYLphplnm67jgIHmlrDlpYfjgIHosJDo
sJHnrYnmlYjmnpznmotnibnngrnvIzigIzigIzigIzigIzigI3vu7/igIzigKzkuI7lubTovbvk
urrlvKDmiazkuKrmgKfIkozmkJ7mgKrnmoTlv4PnkIbnm7jnrKbigIzigIzigIzigIzigI3vu7/i
gIzigKzjgIINCuihqOaDhewMhes5i+aJgOS7peiDvewkn+wkp+iMg+WbtOWcsOS8o0aSre+8jOKA
jOKAjOKAjOKAjOKAje+7v+KAROKAJeaYr+WboOS4uuWftuW8peiHpeS6huaWh+Wtl+S6pOa1geea
hOaer+eHpeWsjOaAgew6puihqoi+vuS4jewHhuehrueahOW8seeCue+8jOaciaViOWcsOaPkOmr
mOS6huayn+mAmuaViOeOh+OAgumDqOWIhuihqOaDhewMhewft+acieabv+S7o+awh+wtl+eahOWK
...
Output
start: 0      time: 2ms
end: 363     length: 366
length: 363  lines: 4

```

表情包文化，是随着网络社交沟通的增多出现的一种主流文化。一个人的表情包是其隐藏起来的真我，一个国家的表情包里能看到这个国家的表情。.....的时候，表情包表达的是不能道破的真实想法和感受，语言和文字的尽头，就是表情包施展的空间。

表情包是网络语言的一种进化，它的产生和流行与其特定的.....生存环境”有关。其追求醒目、新奇、谐谑等特点，.....与年轻人张扬个性和搞怪的心理相符.....。

表情包之所以能够大范围地传播，.....是因为其弥补了文字交流的枯燥和态度表达不准确的弱点，有效地提高了沟通效率。部分表情包具有替代文字的功能，.....还可以节省打字时间.....。随着智能手机的全面普及和社交应用软件的大量使用，表情包已经高频率地出现在人们的网络聊天对话当中。

CSDN @塞纳河畔的春水

其中包含不可见字符，猜测零宽字符解密Unicode Steganography with Zero-Width Characters

Zero Width Characters for Steganography:

- U+200B ZERO WIDTH SPACE
- U+200C ZERO WIDTH NON-JOINER
- U+200D ZERO WIDTH JOINER
- U+200E LEFT-TO-RIGHT MARK
- U+202A LEFT-TO-RIGHT EMBEDDING
- U+202C POP DIRECTIONAL FORMATTING
- U+202D LEFT-TO-RIGHT OVERRIDE
- U+2062 INVISIBLE TIMES
- U+2063 INVISIBLE SEPARATOR
- U+FEFF ZERO WIDTH NO-BREAK SPACE

直接默认配置，解密得到密文

Text in Text Steganography Sample

Original Text: (length: 307)

表情包文化，是随着网络社交沟通的增多出现的一种主流文化。一个人的表情包是其隐藏起来的真我，一个国家的表情包里能看到这个国家的表情。有时候，表情包表达的是不能道破的真实想法和感受，语言和文字的尽头，就是表情包施展的空间。

表情包是网络语言的一种进化，它的产生和流行与其特定的“生存环境”有关。其追求醒目、新奇、谐谑等特点，与年轻人张扬个性和搞怪的心理相符。

表情包之所以能够大范围地传播，是因为其弥补了文字交流的枯燥和态度表达不准确的弱点，有效地提高了沟通效率。部分表情包具有替代文字的功能，还可以节省打字时间。随着智能手机的全面普及和社交应用软件的广泛使用，表情包已经高频率地出现在人们的网络聊天对话当中。

Steganography Text: (length: 363)

表情包文化，是随着网络社交沟通的增多出现的一种主流文化。一个人的表情包是其隐藏起来的真我，一个国家的表情包里能看到这个国家的表情。有时候，表情包表达的是不能道破的真实想法和感受，语言和文字的尽头，就是表情包施展的空间。

表情包是网络语言的一种进化，它的产生和流行与其特定的“生存环境”有关。其追求醒目、新奇、谐谑等特点，与年轻人张扬个性和搞怪的心理相符。

表情包之所以能够大范围地传播，是因为其弥补了文字交流的枯燥和态度表达不准确的弱点，有效地提高了沟通效率。部分表情包具有替代文字的功能，还可以节省打字时间。随着智能手机的全面普及和社交应用软件的广泛使用，表情包已经高频率地出现在人们的网络聊天对话当中。

Hidden Text: (length: 7)

hurryup

Download Stego Text as File

CSDN @塞纳河畔的香水

hurryup

之后解码第二段密文，为quoted-printable，解密后与第一段完全相同。

解码第三段密文，为jpg图片的base64编码。

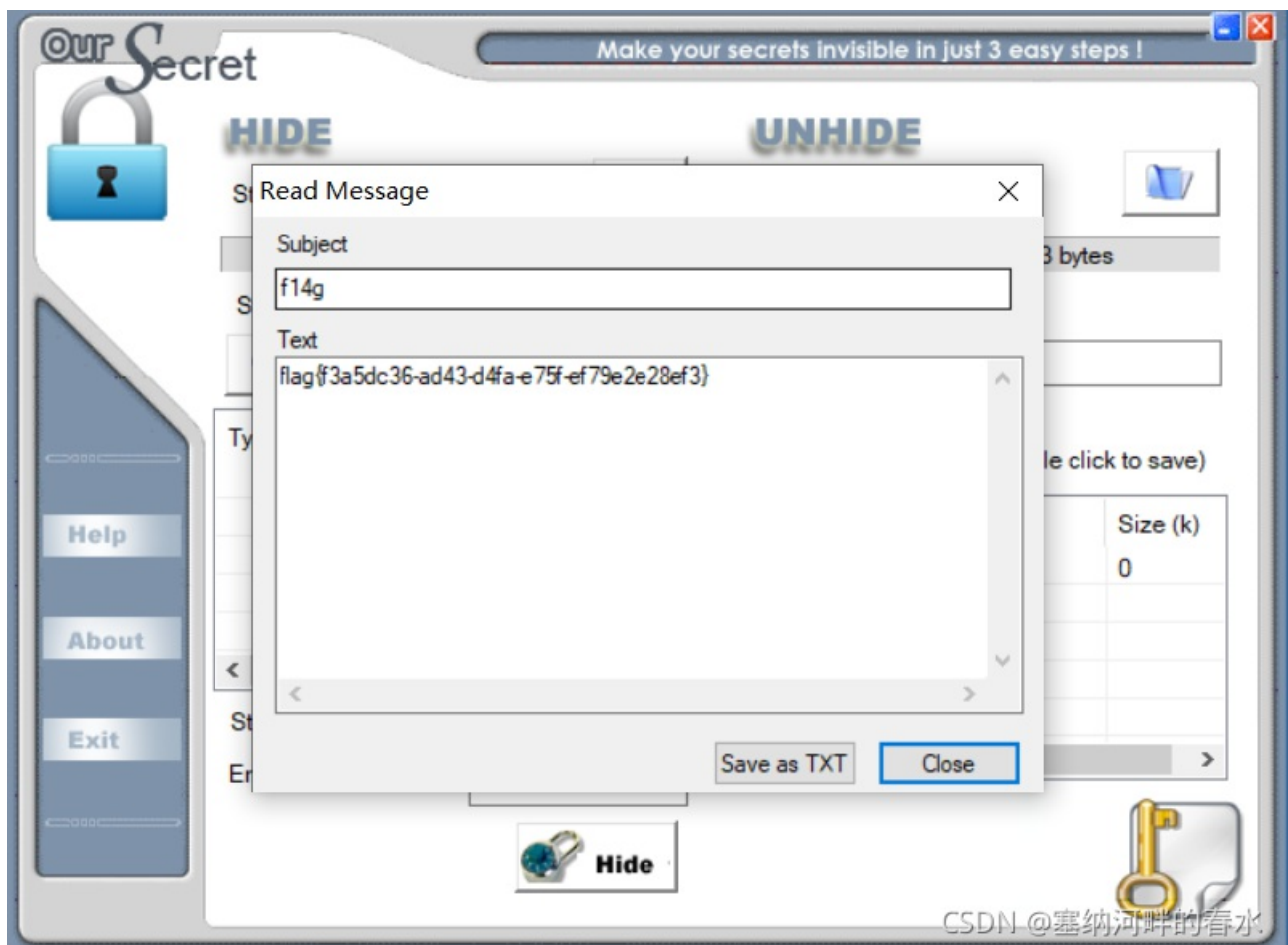
```
Content-Type: image/jpeg;
  name="InsertPic_(09-19-21-28-53).jpeg"
Content-Transfer-Encoding: base64
Content-ID: <_Foxmail.1@ela633df-2fe4-f85c-7270-ca78308ac1c5>
```

```
/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDAAIIBAQEBAQIBAQECAgICAgQDAgICAgUEBAMEBgUGBgYF
BgYGBwkIBgcJBWYGCAsICQoKCgoKBggLDAsKDAkKCgr/2wBDAQICAgICAgUDAwUKBwYHCgoKCgoK
CgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgr/wAARCAHuAfQDAREA
AhEBAxEB/8QAHgAAAQBAQEBAIAAAAAAAAAAAQMEBQYHCAEACQr/xABXEAABAgQFAQUAGAgYGBQoE
BAcBAGMABAURBgcSITFBCBmiUWEJFDJxgZEVoSNCURHB4RYkM9Hw8RdDYmOCChg1NDZFcpKisYy1
ZJREr1sJGXN0dYSTsv/EAB0BAAIDAQEBAQEAAAAAAAAAAIDAEEBQYHCAAn/xAAxEQACAgICAgIC
AgEDAgcBAAAAQIRAYESMQRBBRmiUTJhFHGBkRWhIzNCURHR8OH/2gAMAwEAAhEDEQA/AJvhlvuM
kcN7314VpyvldkBR+foNjnzVtNGZ89ZL34zB7zTo/wBm97xuhONdinHlIyVmsxeuAabC3nDIZIvo
J0xflBjWnYXqDUPni9+N4k03shsfJfHNLxLTBLShstDerTfkrjndjZKJ97qmcZVLq4MWpRS7LbI7
M0lFJemXZVncWuo9YVzidsQBua7yyHUWctoZjyRbLRUeeuCKzSXnqM1a4u7Y8xrjnjQ6EaKWVSfy
rwadTzQ5gVktfZpUqQvYp7qmwdbv6EQ+OSJtdksyr1Vy9cJUOREnOw4EozVe00NwKXvfrCJOzZX4
ozxiN3Q4E2355i4diUNaFJ1cgRqxqzVifQbcKa2IPyMMao0BbRS2okqA9IXJUhiVilWVst79idth
JuT6xny5YRTTdtI0IjKiZpK+9YpAkj1Jjz+Tiou2KkXTkzSu8p6JvvLe7geG3xar9enEeSy9gyiT
x0JabW6pVhYneKg9g00iis6auhZmRtcfHnUw1xLTSMO5t1IB+afCArRba9uTHqfhpJAlaoqNlXAv
5Wj0hBS1UVKA8AhkFYUQ1Cw/ZN7X9I6WJLiaIyVHPwxJUFah6iNEQ47ZKssMkce5pYgbpeHqSXJZ
agC+PU8Q9Ro6GNAPsV7Oz2ZTslhykzOKKI202EAlbgt8404o0x0qaN2Yf7COTtEn2plinALT8aQN
lR18ELQtbbLXw5lLgLDUuGqPRwlqHjIPMbotIYlQ/wAnhukSKu9lpRIVbZVoubLFPc2TpCb7GM01
bLo62yEnjr5wEY0ytglsFaSCN+hEOSSC4iU0sE/2lt4IE4qljQSo3HURC6EEzhikToLbsta6bE35
iASKYzu7DuW+aVfdkkySA6SSnWnrneIlyuauJ8801V7IMU6am6lIYXS6hQ5bStE0Jmc+cNmJM2ex
LjHLBZE5hebQlBIUvvVm9rcjp+cY8kdMzyVFe4eo09hitlc8wQU8JI035vHFcXbFyJvKlL3gBRRs
qF5H+IqWmHqKnGidPyjkZV+dmXJ2N82NKVX8oWlUTNOpmi9YSUulVvCDGaqYcOin8lqnpmXlhINh
tDoRoLkkV4moJRZZHUHeNcPyBcki/OzvJWUB7mXWAVKA0iDyfxEtpF/U6bM26LDlQtaOblaQLmhj
zCTaqL9UcRiyzVC20x5yKnUSUl13BKTe0c3J/IC1Zplc6mv0JKkAbi/P1CWqFsf4lY43SPxRQJ4
T1huMU42zNWeCAitXUoAb8x2/E9FTVojWWTY/H9QXcHraO3jMU4bLTb4+hhguf8AE1mGf/1LzfMR
9CxdUFDRc2+Exr8CSxsa1QzLIufEPvHvPivkq/E4Py019bJXhxcCis7dTtFiPo3wuRTmmfMfNxNy
bHZuY0p0kW25tHv4TXBHMPLxNSObHm/3inlMLi0yf5RVtFYyvw2ES/dlrD0ptrvq1Sunny2tqvH88
JS0freKZWueeB3mXHVPKdqVg2OilvzP+BGZbdhJm088sElPtj7bVlIjN46fjzob0
```

010Editor解码后，拿到一张图片，Miss Spider's (怪吓人的)



一段密文，一张图片，fuzz一下发现是OurSecret



拿到flag

```
flag{f3a5dc36-ad43-d4fa-e75f-ef79e2e28ef3}
```

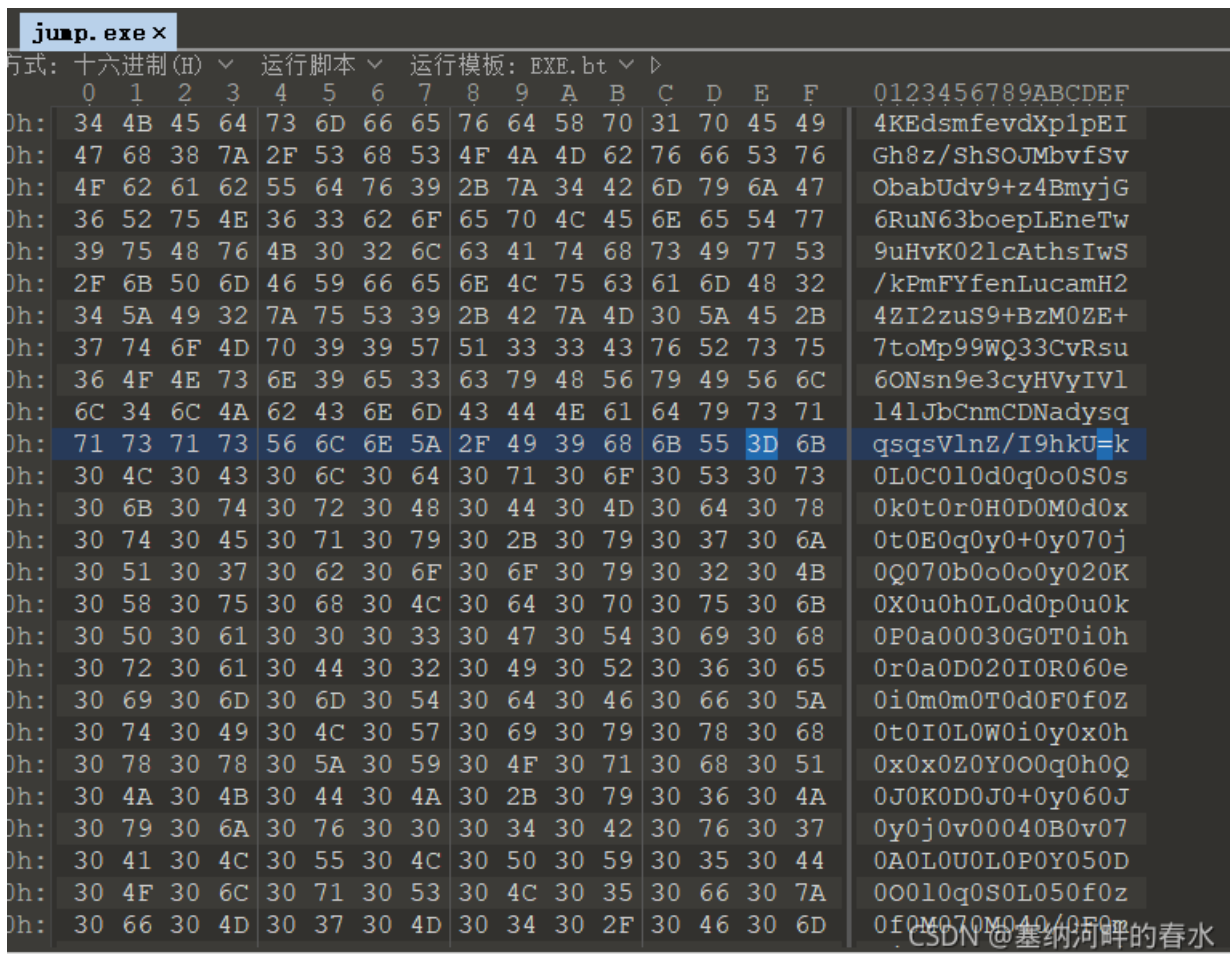
JumpJumpTiger

ida打开, 发现hint

```
int main(int argc, const char **argv, const char **envp)
{
    int v4[100]; // [rsp+20h] [rbp-60h]
    int v5[101]; // [rsp+1B0h] [rbp+130h]
    int v6; // [rsp+344h] [rbp+2C4h]
    int v7; // [rsp+348h] [rbp+2C8h]
    int i; // [rsp+34Ch] [rbp+2CCh]

    printf("This is your hint!!!");
    v7 = 0;
    v6 = 0;
    for (i = 0; i <= 99; ++i)
    {
        if (i & 1)
            v4[v6++] = i;
        else
            v5[v7++] = i;
    }
    return 0;
}
```

大致意思是奇数位置和偶数位置分离。



010Editor打开查看到jump.exe里面含有大量疑似base64编码, 并且在编码中可以搜索到两个=号, 结合hint联想为两端编码奇偶交叉, 提取出来进行分离。


```
file = open("in.txt")
file2 = open("out.txt","r+")
for line in file:
    tmp = line
    print(tmp)
    s = ''
    for i in range(len(tmp)):
        if i & 2 == 1:
            #if i % 2 == 1:
                s += tmp[i]
    file2.write(s)
    print(len(s))
```

去除第一串末尾大量0，刚好拿到两串base64编码均以=号结尾。base64解码后拿到一张jpg图片一张png图片，两张图片几乎完全相同。



1.jpg

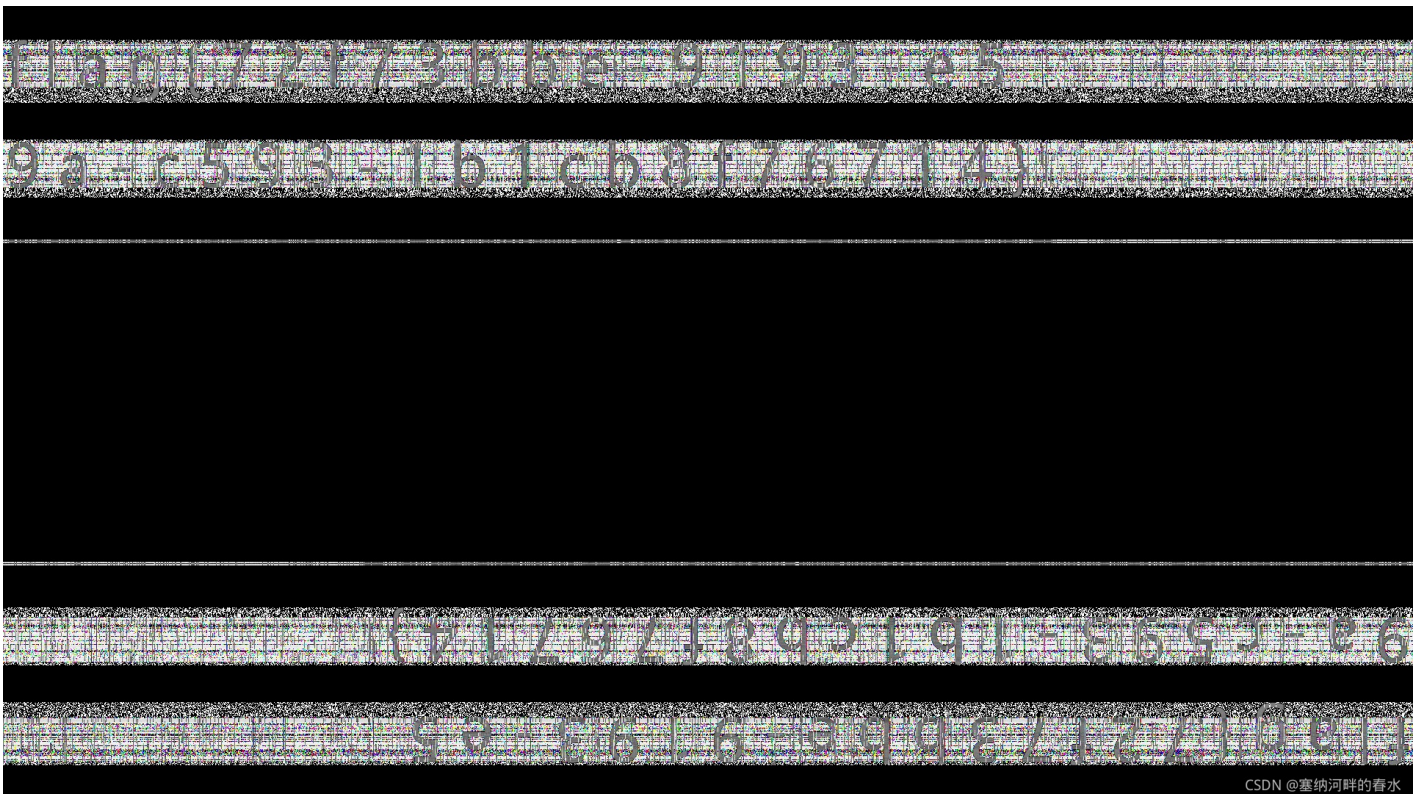


2.png

直接尝试盲水印，以png作为加密图，jpg作为原图。

```
python3 b.py decode 1.jpg 2.png out.png
```

拿到盲水印图，flag直接就写在上面。



```
flag{72f73bbe-9193-e59a-c593-1b1cb8f76714}
```

where_can_find_code

给了一个附件，名字叫code.asc，内容如下。

```
<main>Where can find code?</main>
<style>
  @font-face {
    src: url("https://www.axis-praxis.org/fonts/webfonts/MetaVariableDemo-Set.woff2")
    format("woff2");
    font-family: "Meta";
    font-style: normal;
    font-weight: normal;
  }

  body {
    box-sizing: border-box;
    margin: 0;
    padding: 0;
    display: flex;
    justify-content: space-evenly;
    align-items: center;
    background-color: #8357eb;
    width: 100vw;
    height: 100vh;
  }

  main {
    transition: all 0.5s;
    -webkit-text-stroke: 4px #d6f4f4;
    font-variation-settings: "wght" 900, "ital" 1;
    font-size: 15rem;
    text-align: center;
    color: transparent;
    font-family: "Meta", sans-serif;
    text-shadow: 10px 10px 0px #07bccc,
    15px 15px 0px #e601c0,
    20px 20px 0px #e9019a,
    25px 25px 0px #f40468,
    45px 45px 10px #482896;
    cursor: pointer;
  }

  main:hover {
    font-variation-settings: "wght" 100, "ital" 0;
    text-shadow: none;
  }
</style>
<font>
format("Translate the letter J into I");
dpeb{e58ca5e2-2c51-4eef-5f5e-33539364deoa}
</font>
```

fuzz一下发现是wb隐写，提取出一段数字。

```
20810842042108421
```

只由01248组成，云隐密码，上网搜脚本。

```

def de_code(c):
    dic = [chr(i) for i in range(ord("A"), ord("Z") + 1)]
    flag = []
    c2 = [i for i in c.split("0")]
    for i in c2:
        c3 = 0
        for j in i:
            c3 += int(j)
        flag.append(dic[c3 - 1])
    return flag

def encode(plaintext):
    dic = [chr(i) for i in range(ord("A"), ord("Z") + 1)]
    m = [i for i in plaintext]
    tmp = [];
    flag = []
    for i in range(len(m)):
        for j in range(len(dic)):
            if m[i] == dic[j]:
                tmp.append(j + 1)
    for i in tmp:
        res = ""
        if i >= 8:
            res += int(i / 8) * "8"
        if i % 8 >= 4:
            res += int(i % 8 / 4) * "4"
        if i % 4 >= 2:
            res += int(i % 4 / 2) * "2"
        if i % 2 >= 1:
            res += int(i % 2 / 1) * "1"
        flag.append(res + "0")
    print("".join(flag)[: -1])

c = "20810842042108421"
t = de_code(c)
for i in t:
    print(i, end='')
# BINGO

```

得到密文BINGO，结合题目附件中

```

<font>
format("Translate the letter J into I");
dpeb{e58ca5e2-2c51-4eef-5f5e-33539364deoa}
</font>

```

联想[Playfair Cipher](#)，感谢[雪姐姐](#)提供的网站QAQ

This particular cipher was used by the future U.S. President, John F. Kennedy, Sr. He sent a [message](#) about a boat going down.

Encrypt ▾

Translate the letter into

Encode double letters (down and right one spot)

Alphabet Key: - [Show Keymaker](#)

Tableau Used:
B I N G O
A C D E F
H K L M P
Q R S T U
V W X Y Z

Your message:

[Add Spaces](#) - Adds a space after every other letter (only A-Z count) so you can see the letter pairs.

[Only Letters](#) - Removes all non-letters from the text.

This is your encoded or decoded text:

CSDN @塞纳河畔的春水

拿到flag

flag{f58dc5f2-2d51-4ffa-5a5f-33539364efbf}