攻防世界 MISC 新手练习区 writeup 001-006

原创

ChaoYue_miku 于 2021-09-03 23:59:07 发布 186 收藏 1

分类专栏： CTF # 攻防世界 # Misc 文章标签： 算法 c++ 概率论

本文链接：https://blog.csdn.net/ChaoYue_miku/article/details/120092550

版权

CTF 同时被 3 个专栏收录

127 篇文章 5 订阅

订阅专栏

攻防世界

6 篇文章 0 订阅

订阅专栏

Misc

2 篇文章 0 订阅

订阅专栏

攻防世界 MISC 新手练习区 题目解答

文章目录

001 this_is_flag

难度系数：

题目来源： 暂无

题目描述： Most flags are in the form flag{xxx}, for example:flag{th1s_!s_a_d4m0_4la9}

0x01 题目描述即为flag

0x02 得到flag： **flag{th1s_!s_a_d4m0_4la9}**

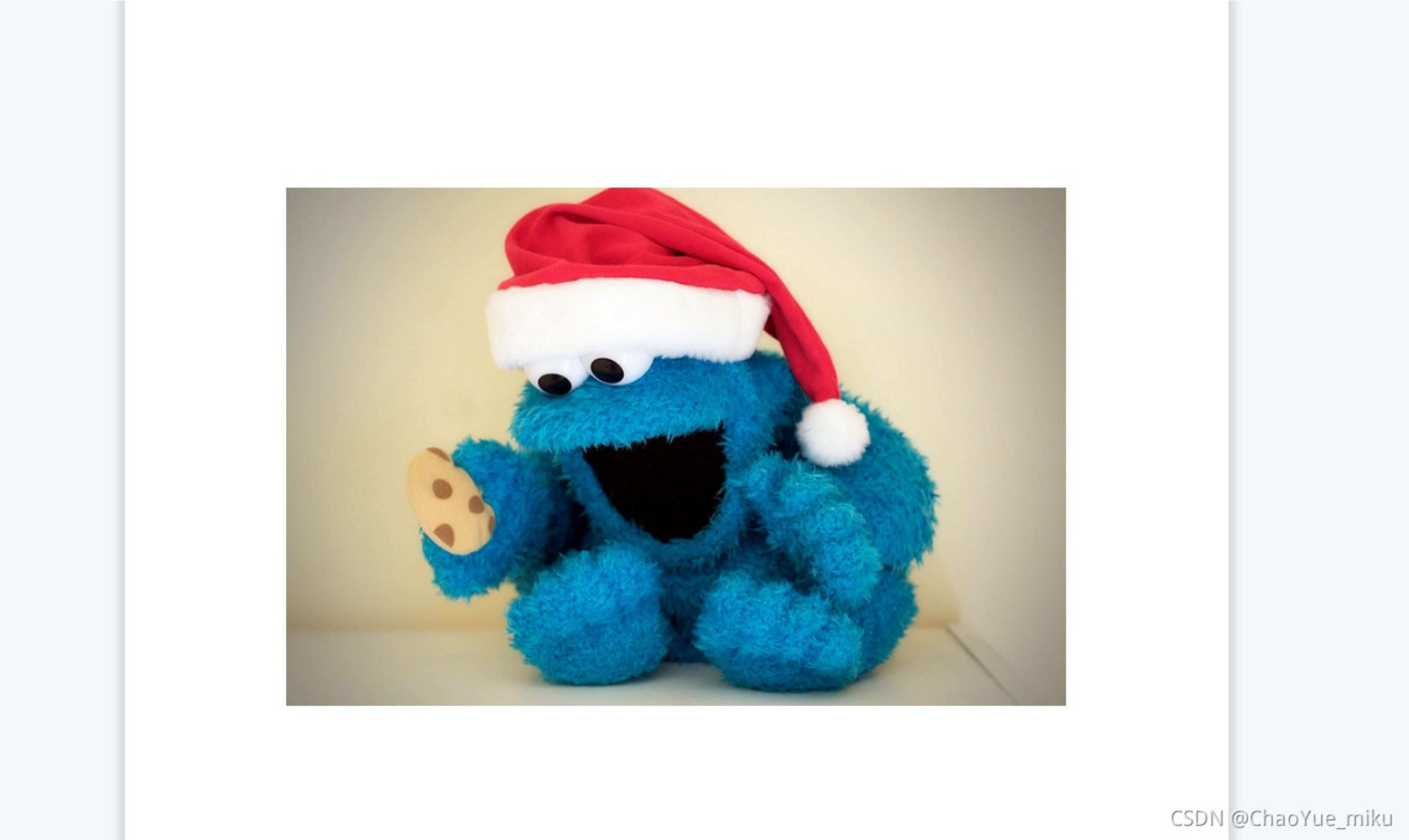
002 pdf

难度系数： 3.0

题目来源： csaw

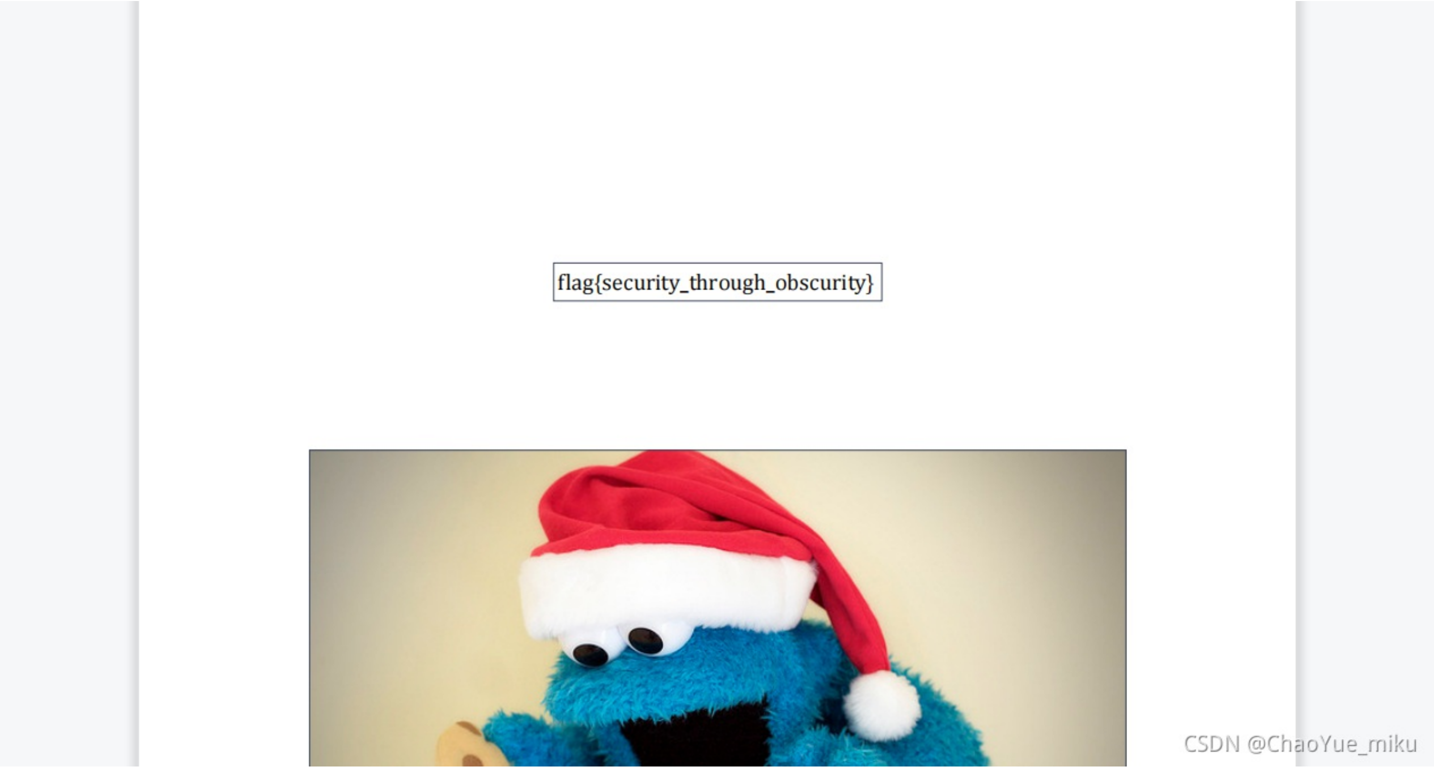
题目描述： 菜猫给了菜狗一张图，说图下面什么都没有

0x01 下载并打开附件，是一个pdf格式文件



题目描述说图下面什么都没有，那就看看图下面到底有没有猫腻

0x02 拖动上层图片，检查图片覆盖的部分



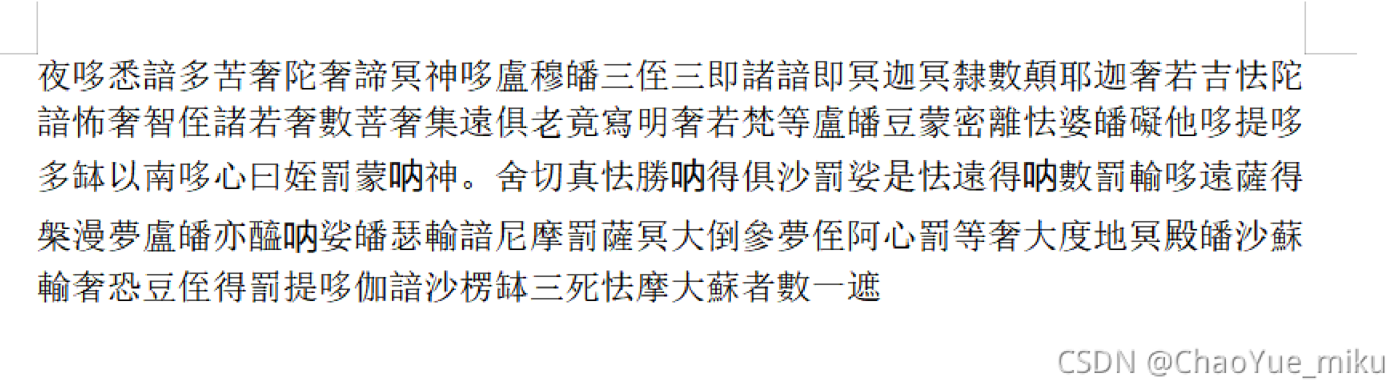
flag{security_through_obscurity}

0x03 得到flag： flag{security_through_obscurity}

003 如来十三掌

难度系数： 3.0
题目来源： 暂无
题目描述： 菜狗为了打败菜猫，学了一套如来十三掌。

0x01 下载并打开附件



夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

熟悉密码的同学可以看出来，这是一种叫做与佛论禅的编码

0x02 进行“与佛论禅”解码

打开网页与佛论禅

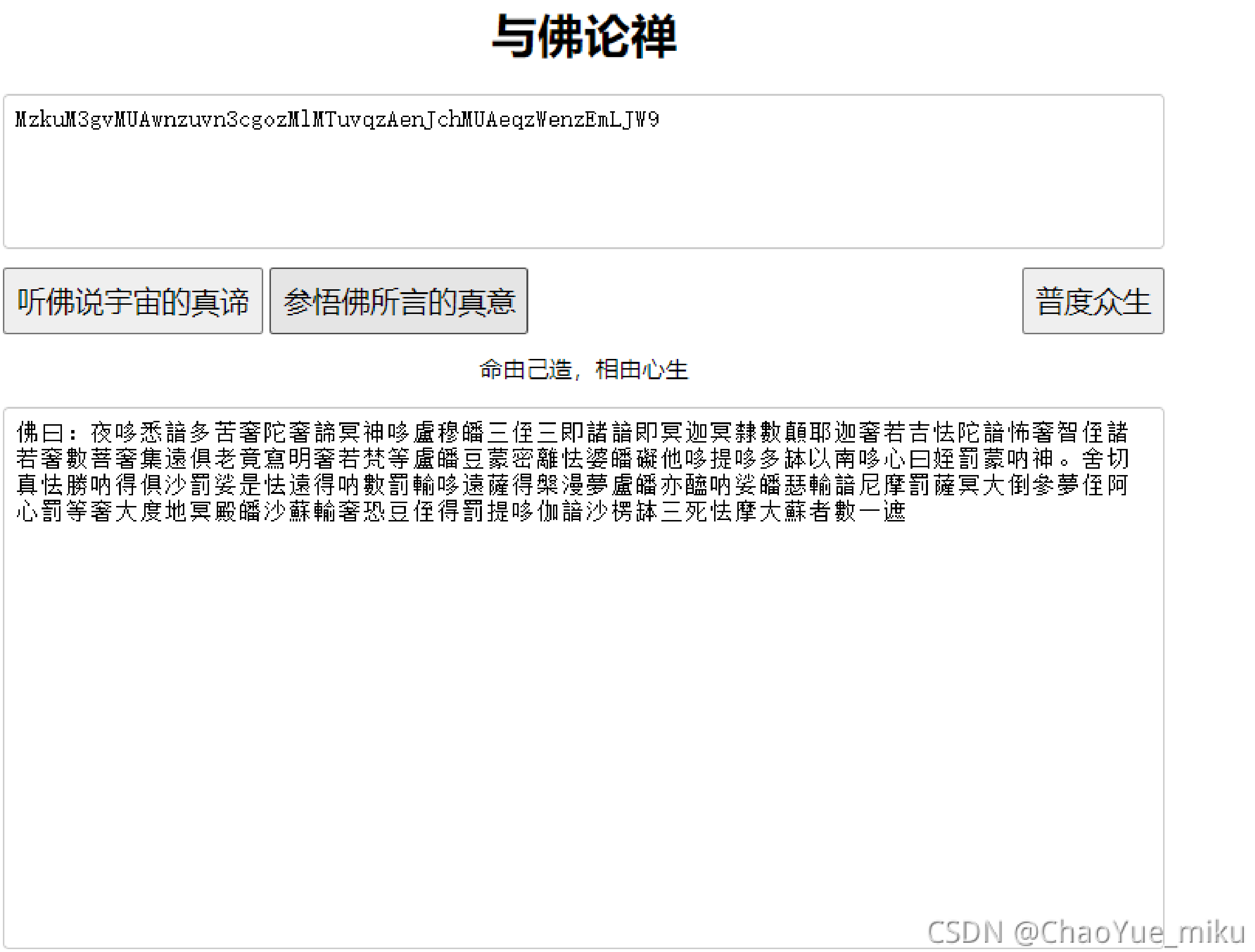
解码时要注意在开头加上`佛曰：`这是标准格式，任何字符串经过与佛论禅加密后都会在开头带上`佛曰：`两个字

Encode：

```
佛曰：夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮
```

Decode：

```
MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9
```



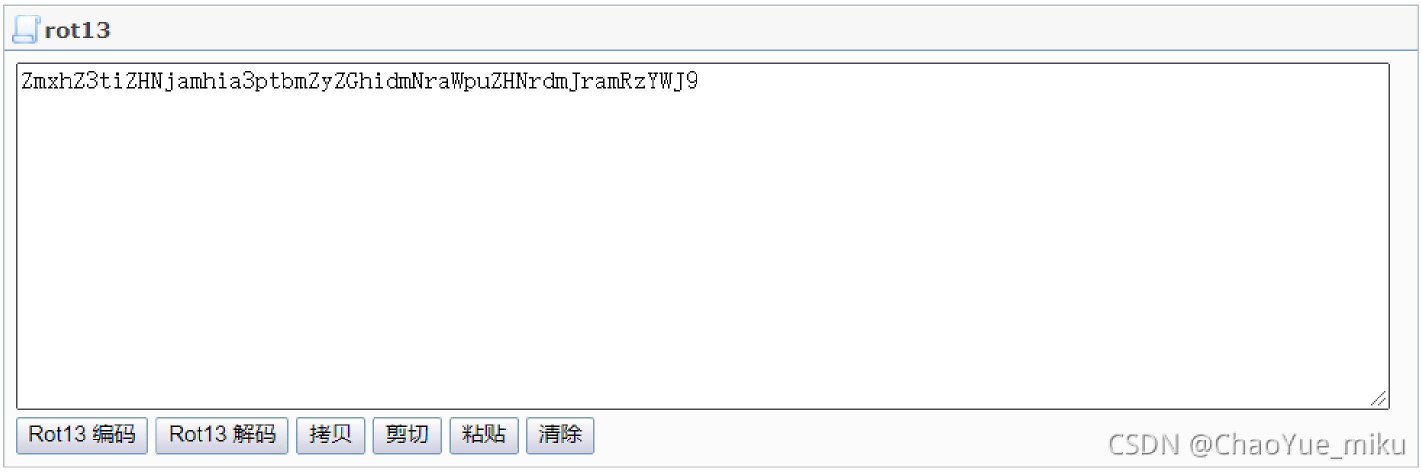
MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

佛曰：夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

0x03 进行rot-13解码

上一步与佛论禅解码得到的结果非常像base64加密后的内容，但是尝试base64解码却失败了。

结合题目“如来十三掌”，我们联想到ROT-13这种加密方式，这是一种凯撒密码的变体。



ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

Encode：

```
MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9
```

Decode：

```
ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9
```

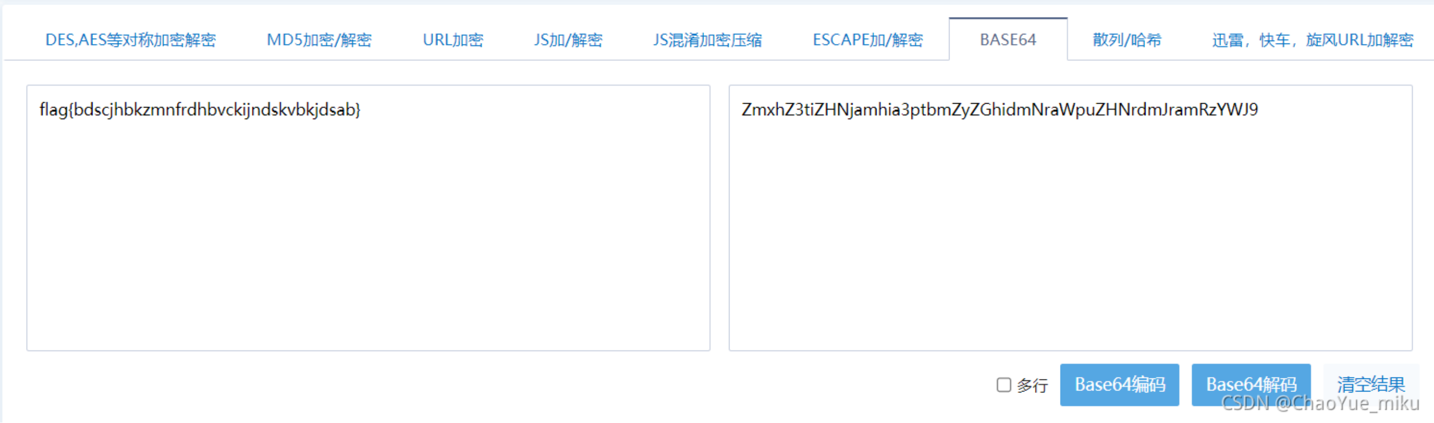
0x04 进行base64解码

Encode：

```
ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9
```

Decode：

```
flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}
```



flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

0x05 得到flag： flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

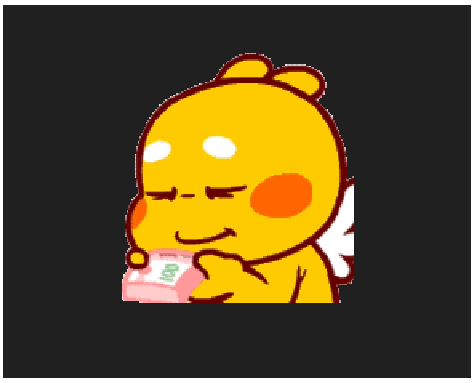
004 give_you_flag

难度系数：4.0

题目来源： 暂无

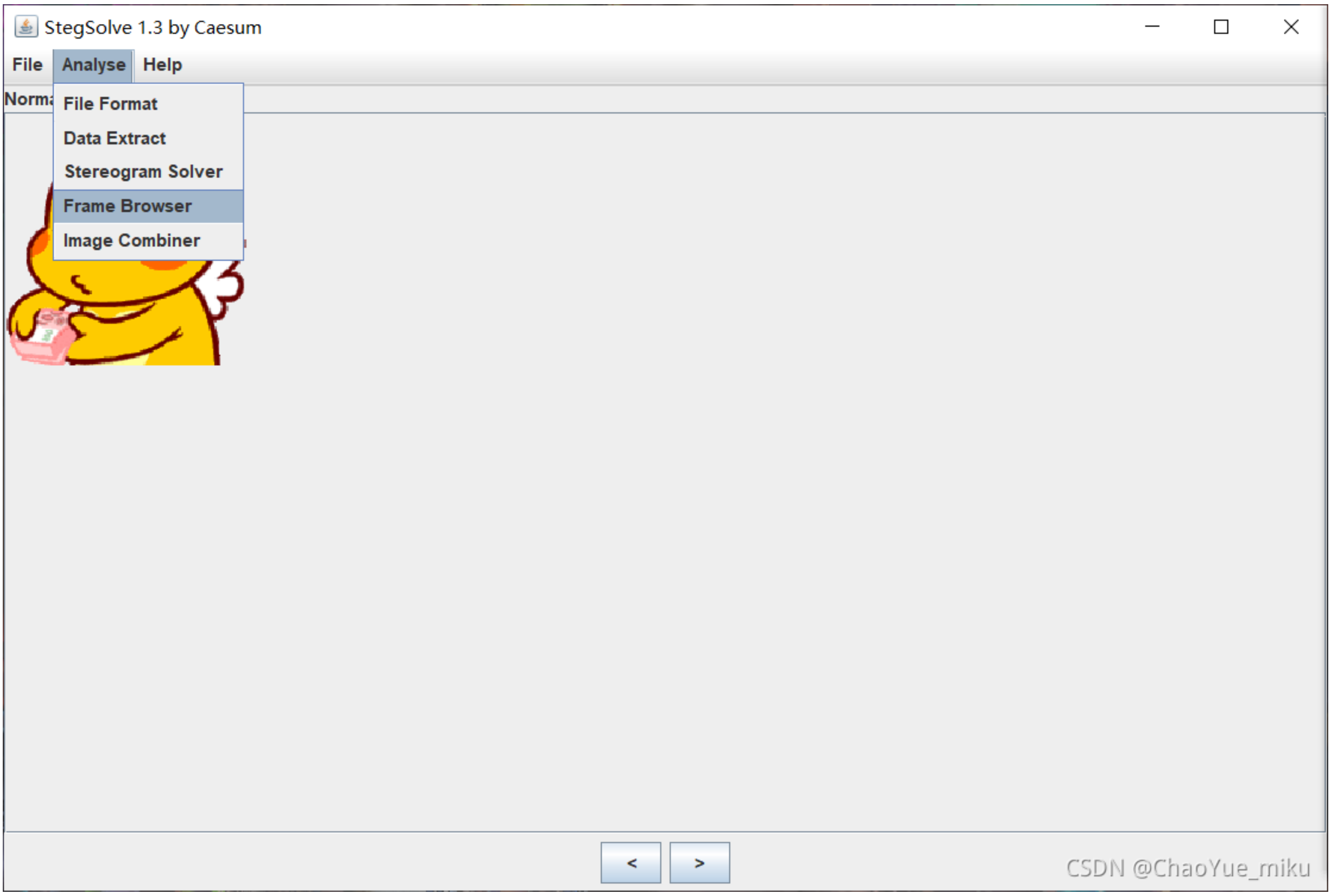
题目描述： 菜狗找到了文件中的彩蛋很开心，给菜猫发了个表情包

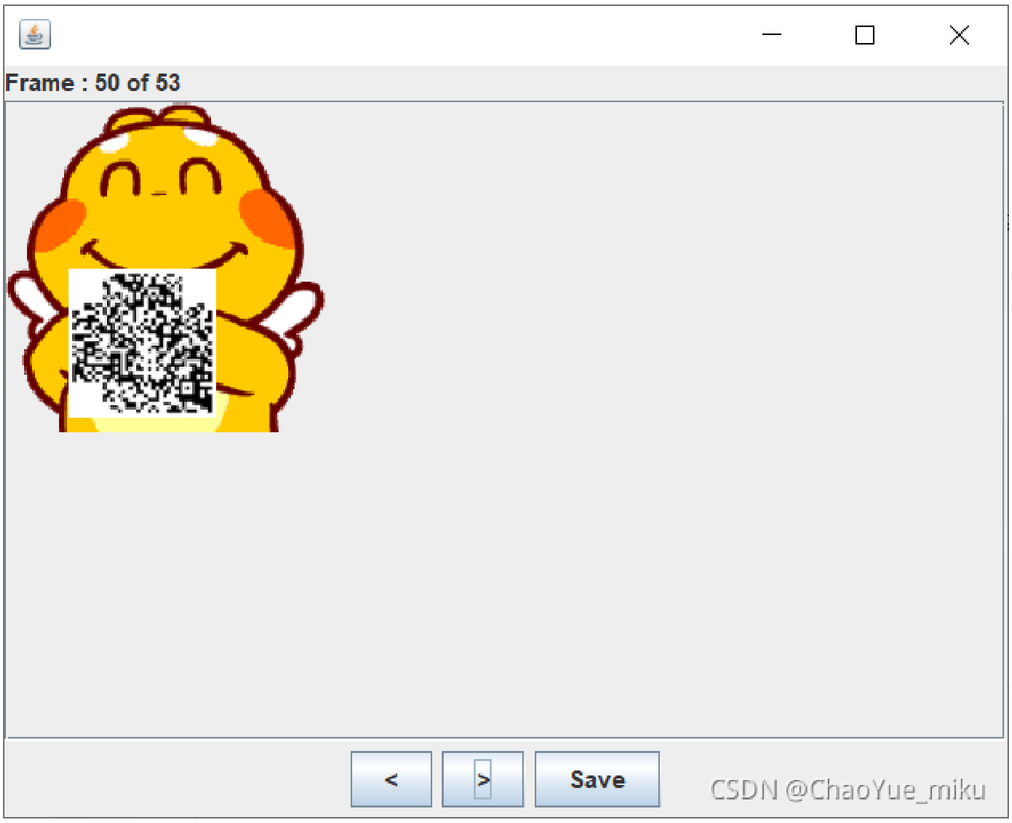
0x01 下载附件，打开后发现是一张GIF图片



可以看到gif动图结尾处闪过一张二维码

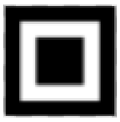
0x02 使用Stegsolve中的Frame Browser逐帧提取gif



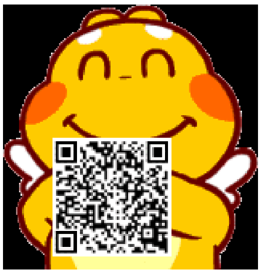


该gif图片共有53帧，在第50帧发现了二维码，但是该二维码缺失了三个定位符，所以需要我们手动补充上去。

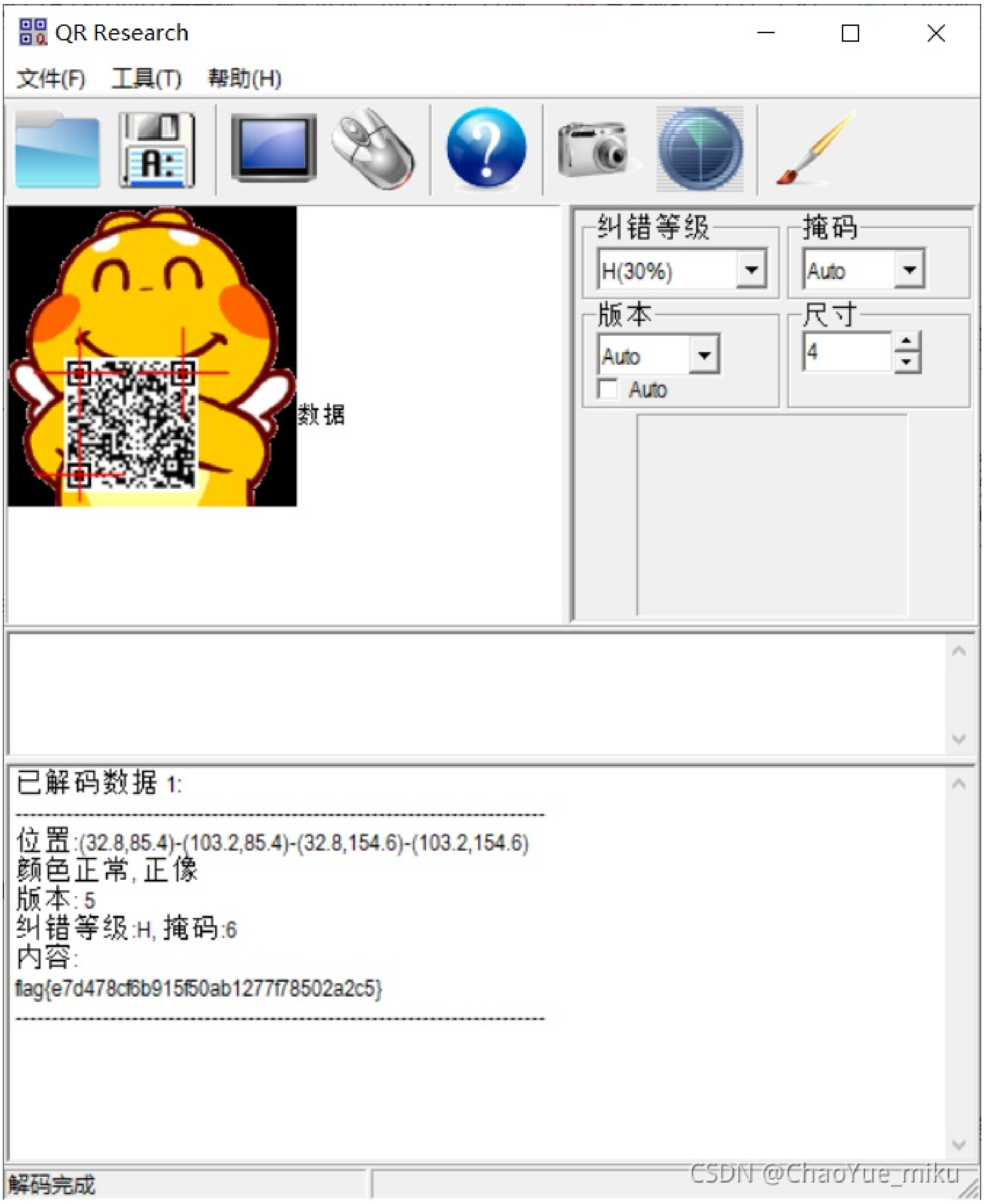
0x03 使用PS手动补全二维码



最终结果：



0x03 使用CQR扫描二维码



纠错等级 H(30%)　掩码 Auto

版本 Auto　□ Auto　尺寸 4

```
已解码数据 1:
------------------------------------------------------------
位置:(32.8,85.4)-(103.2,85.4)-(32.8,154.6)-(103.2,154.6)
颜色正常, 正像
版本: 5
纠错等级:H, 掩码:6
内容:
flag{e7d478cf6b915f50ab1277f78502a2c5}
------------------------------------------------------------
```

解码完成

0x04 得到flag： **flag{e7d478cf6b915f50ab1277f78502a2c5}**

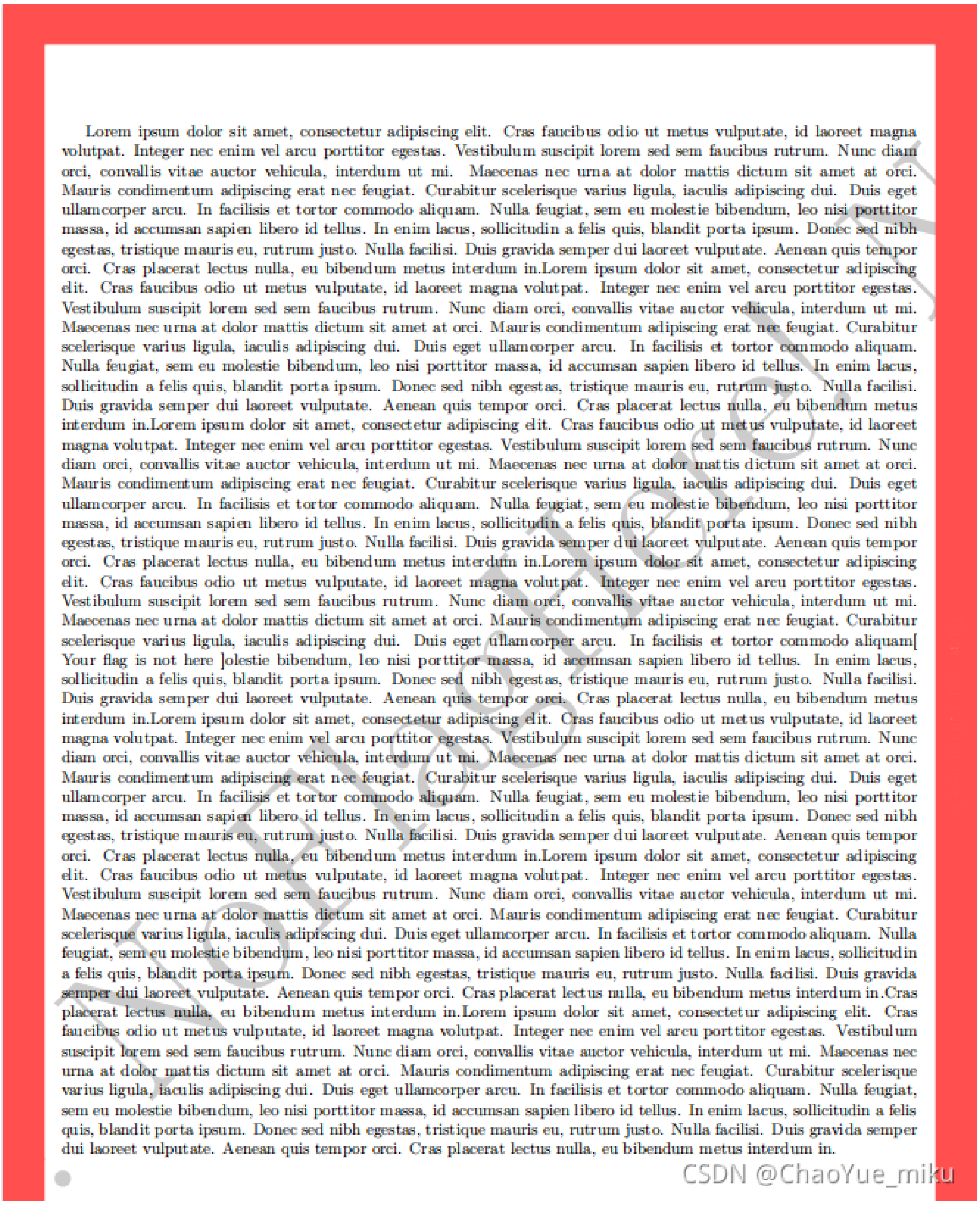
005 stegano

难度系数：4.0

题目来源： CONFidence-DS-CTF-Teaser

题目描述： 菜狗收到了图后很开心，玩起了pdf 提交格式为flag{xxx}，解密字符需小写

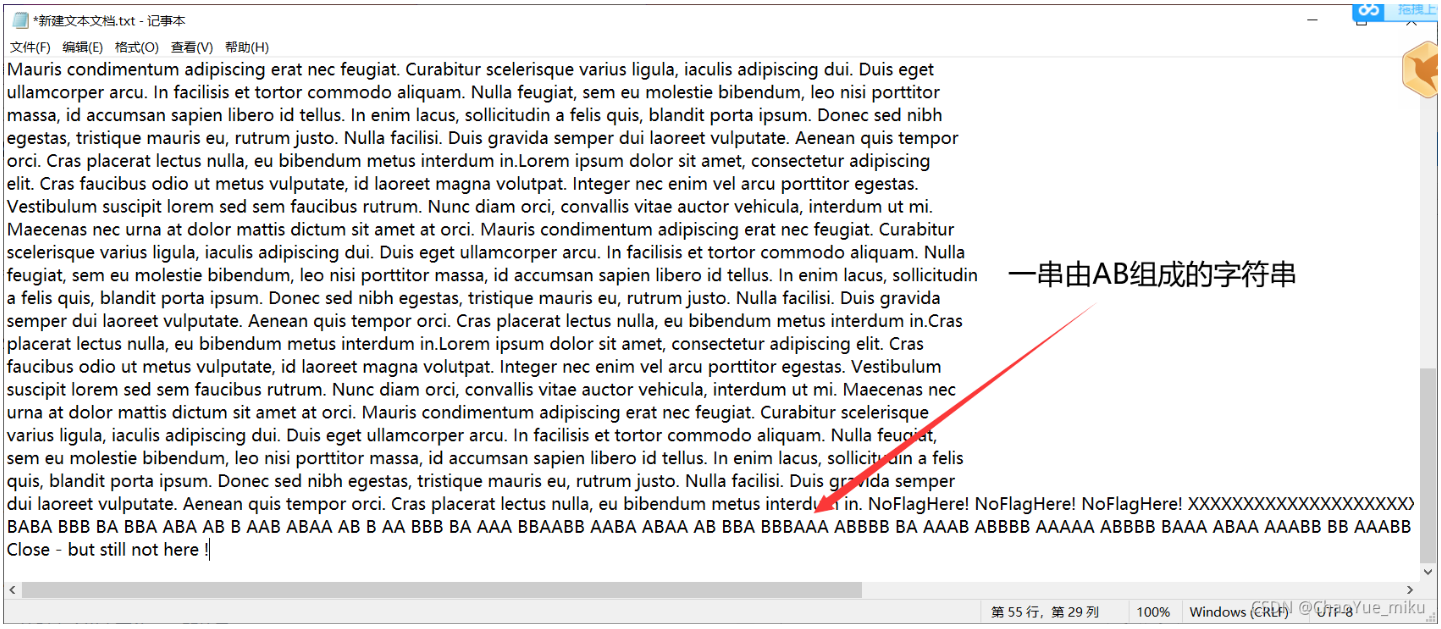
0x01 下载附件,打开后发现是一个pdf文件



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam[Your flag is not here]olestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.

暂时看不出来有关flag的信息

0x02 Ctrl+A全选pdf文件内容，粘贴到文本文档中查看


*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)
第 55 行，第 29 列
100%
Windows (CRLF)
UTF-8

Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in. NoFlagHere! NoFlagHere! NoFlagHere! XXXXXXXXXXXXXXXXXXX
BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB
Close - but still not here !

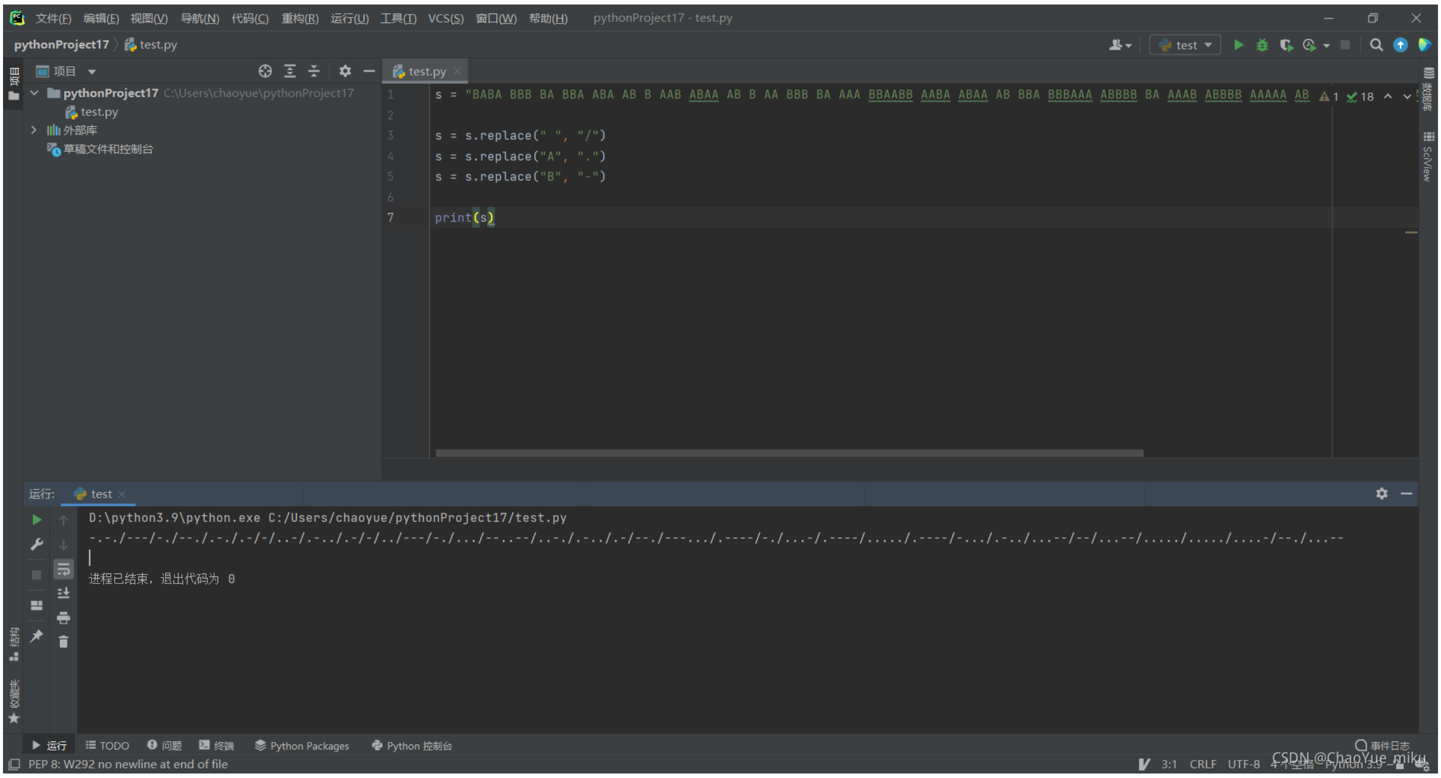
一串由AB组成的字符串

疑似为培根密码，但是却没有进行分组。

由于AB对应两种字符，所以也有可能是摩斯电码。

0x03 将AB字符串转换为摩斯密码

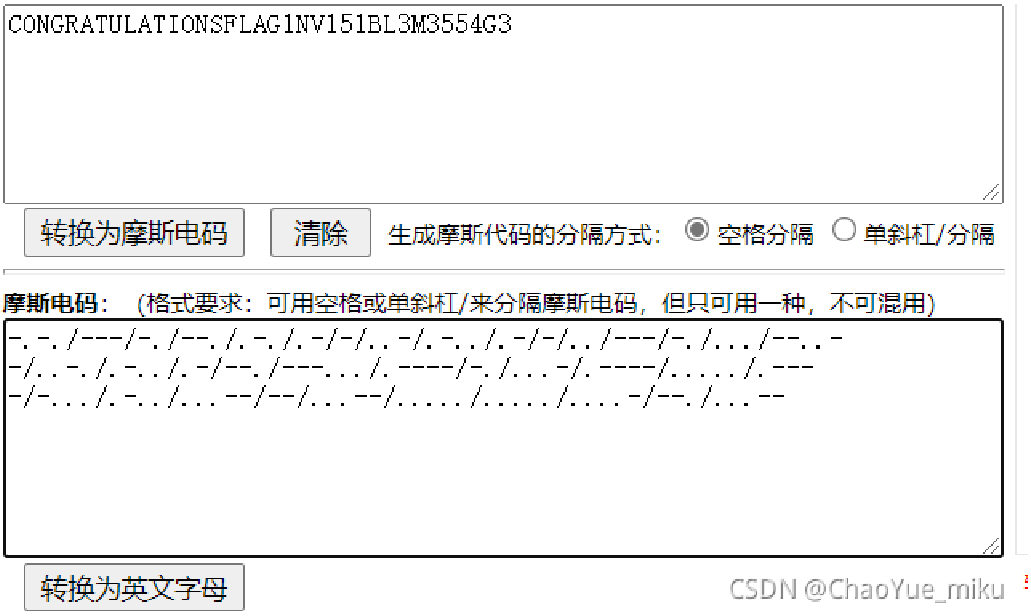
```python
s = "BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB"

s = s.replace(" ", "/")
s = s.replace("A", ".")
s = s.replace("B", "-")

print(s)
```



```python
s = "BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA AB

s = s.replace(" ", "/")
s = s.replace("A", ".")
s = s.replace("B", "-")

print(s)
```

```
D:\python3.9\python.exe C:/Users/chaoyue/pythonProject17/test.py
-.-./---/-./--./.-./.-/-/..-/.-../.-/-/../---/-./.../--..--/..-./.-../.-/--./---.../.----/-./...-/.----/...../.----/-.../.-../...--/--/...--/...../...../....-/--./...--

进程已结束，退出代码为 0
```

0x04 摩斯密码解密



CONGRATULATIONSFLAG1NV151BL3M3554G3

转换为摩斯电码　清除　生成摩斯代码的分隔方式：● 空格分隔 ○ 单斜杠/分隔

摩斯电码：（格式要求：可用空格或单斜杠/来分隔摩斯电码，但只可用一种，不可混用）

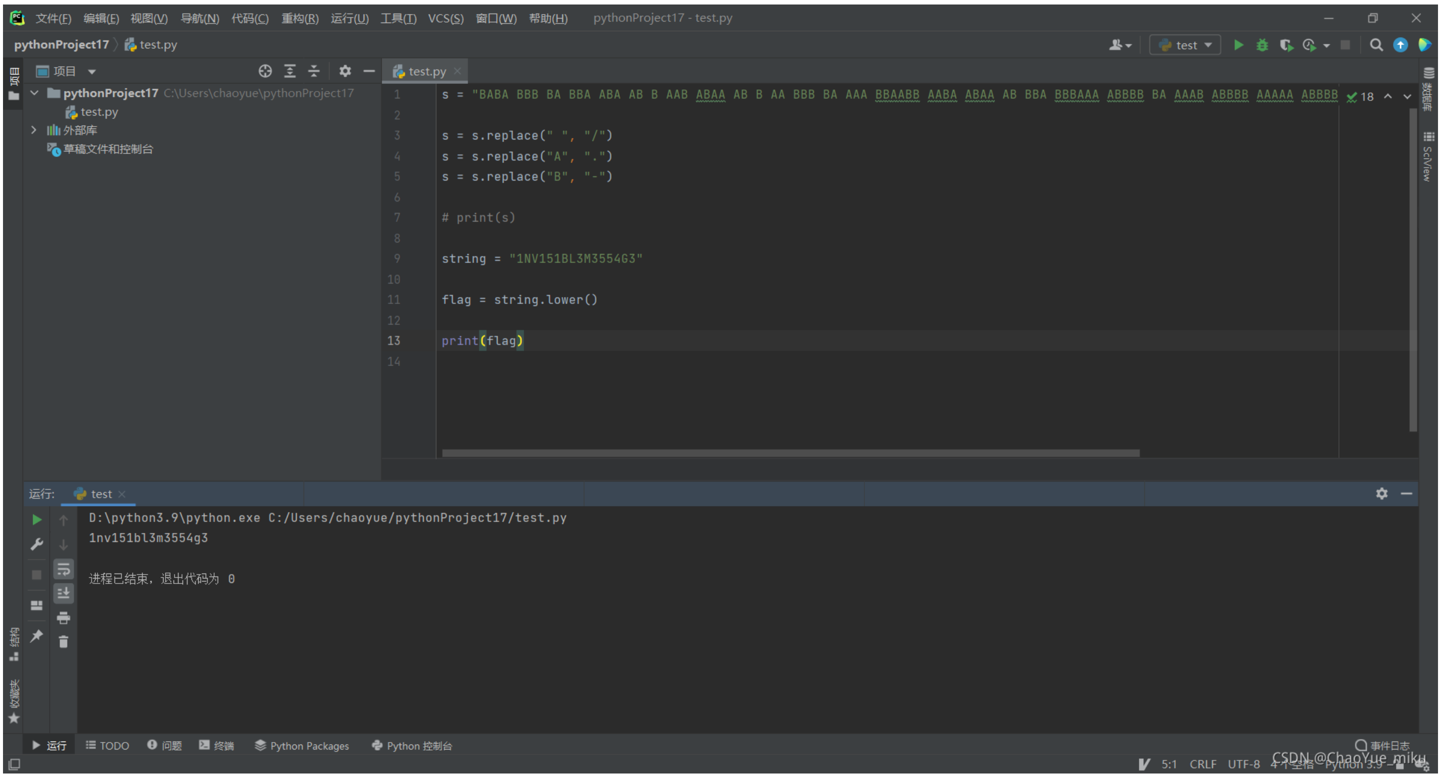
```
-.-./---/-./--./.-./.-/-/..-/.-../.-/-/../---/-./.../--..-
-/..-./.-../.-/--./---.../.----/-./...-/.----/...../.---
-/-.../.-../...--/--/...--/...../...../....-/--./...--
```

解密结果：

CONGRATULATIONSFLAG1NV151BL3M3554G3

0x05 根据题目要求，将解密字符转化为小写形式

```python
string = "1NV151BL3M3554G3"

flag = string.lower()

print(flag)
```



```
s = "BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB

s = s.replace(" ", "/")
s = s.replace("A", ".")
s = s.replace("B", "-")

# print(s)

string = "1NV151BL3M3554G3"

flag = string.lower()

print(flag)
```

```
D:\python3.9\python.exe C:/Users/chaoyue/pythonProject17/test.py
1nv151bl3m3554g3

进程已结束，退出代码为 0
```

0x06 得到flag： flag{1nv151bl3m3554g3}

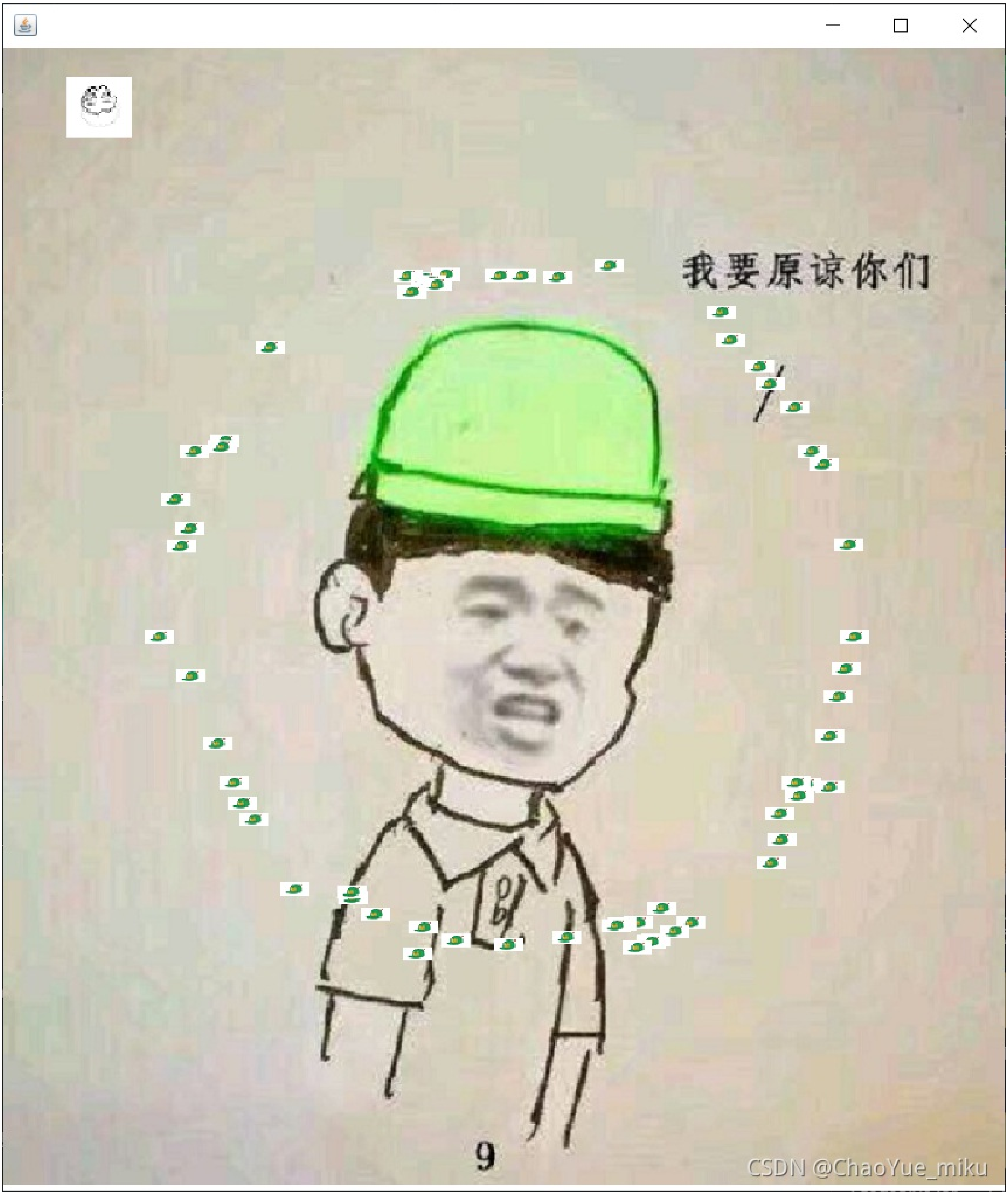
006 坚持60s

难度系数：4.0

题目来源： 08067CTF

题目描述： 菜狗发现最近菜猫不爱理他，反而迷上了菜鸡

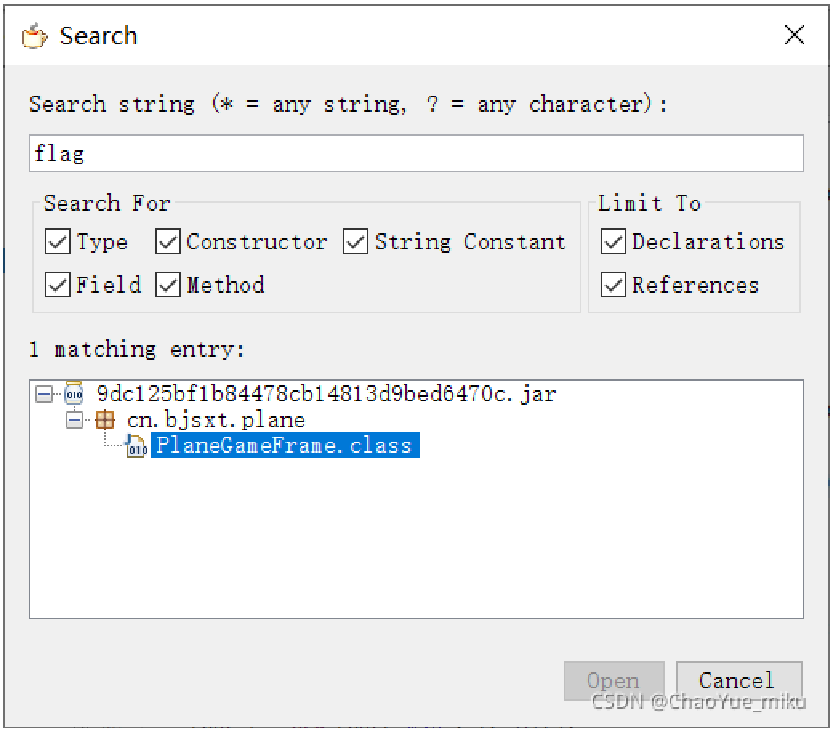
0x01 下载附件,是一个jar文件,打开后发现是一个小游戏



当然可以完成游戏任务得到flag，接下来讲解常规做法

0x02 使用Java反编译软件jd-gui（需要jdk1.7）打开jar文件

按Ctrl+Shift+S进入搜索界面，查找带有flag的字符串



Search

Search string (* = any string, ? = any character):

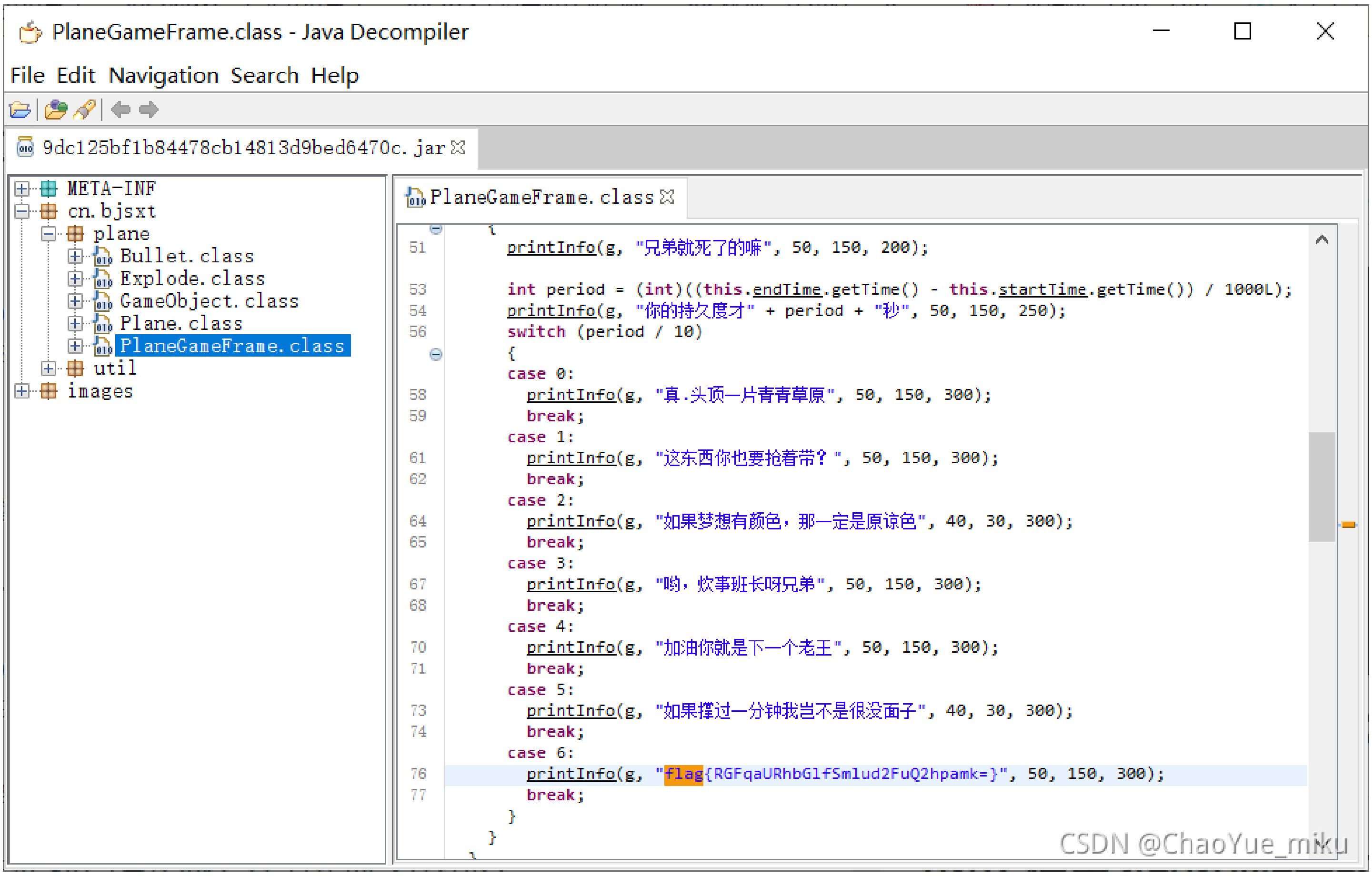
flag

Search For: ☑ Type ☑ Constructor ☑ String Constant ☑ Field ☑ Method

Limit To: ☑ Declarations ☑ References

1 matching entry:

```
9dc125bf1b84478cb14813d9bed6470c.jar
  cn.bjsxt.plane
    PlaneGameFrame.class
```



PlaneGameFrame.class - Java Decompiler

File Edit Navigation Search Help
9dc125bf1b84478cb14813d9bed6470c.jar
PlaneGameFrame.class

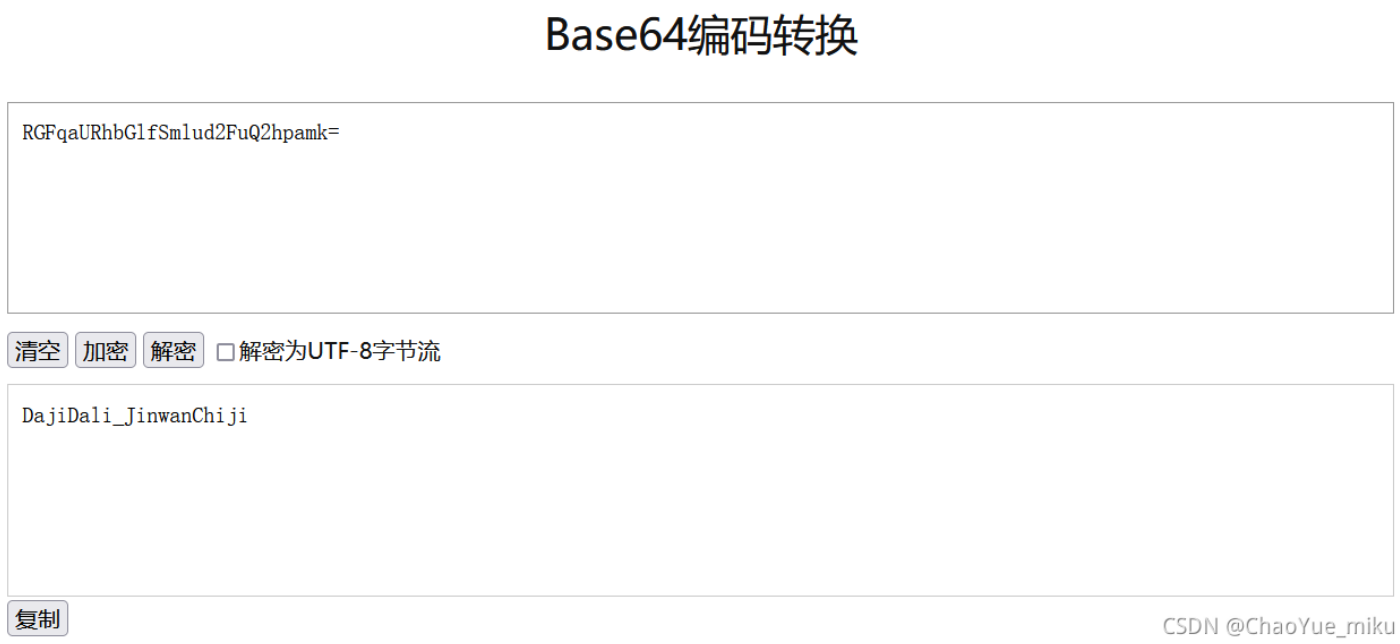
```
META-INF
cn.bjsxt
  plane
    Bullet.class
    Explode.class
    GameObject.class
    Plane.class
    PlaneGameFrame.class
  util
images
```

```
    {
      printInfo(g, "兄弟就死了的嘛", 50, 150, 200);

      int period = (int)((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
      printInfo(g, "你的持久度才" + period + "秒", 50, 150, 250);
      switch (period / 10)
      {
      case 0:
        printInfo(g, "真.头顶一片青青草原", 50, 150, 300);
        break;
      case 1:
        printInfo(g, "这东西你也要抢着带？", 50, 150, 300);
        break;
      case 2:
        printInfo(g, "如果梦想有颜色，那一定是原谅色", 40, 30, 300);
        break;
      case 3:
        printInfo(g, "哟，炊事班长呀兄弟", 50, 150, 300);
        break;
      case 4:
        printInfo(g, "加油你就是下一个老王", 50, 150, 300);
        break;
      case 5:
        printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
        break;
      case 6:
        printInfo(g, "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);
        break;
      }
    }
```

flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}

flag显然经过了base64加密，所以需要一次解码

0x03 对flag进行base64解密



Base64编码转换

```
RGFqaURhbGlfSmlud2FuQ2hpamk=
```

□解密为UTF-8字节流

```
DajiDali_JinwanChiji
```

0x04 得到flag： flag{DajiDali_JinwanChiji}