CTF MP3音频隐写

原创

GunnerXiang 于 2019-02-10 02:53:20 发布 6728 收藏 8

分类专栏： CTF 文章标签： MISC CTF 隐写

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_41620646/article/details/86860656

版权

CTF 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

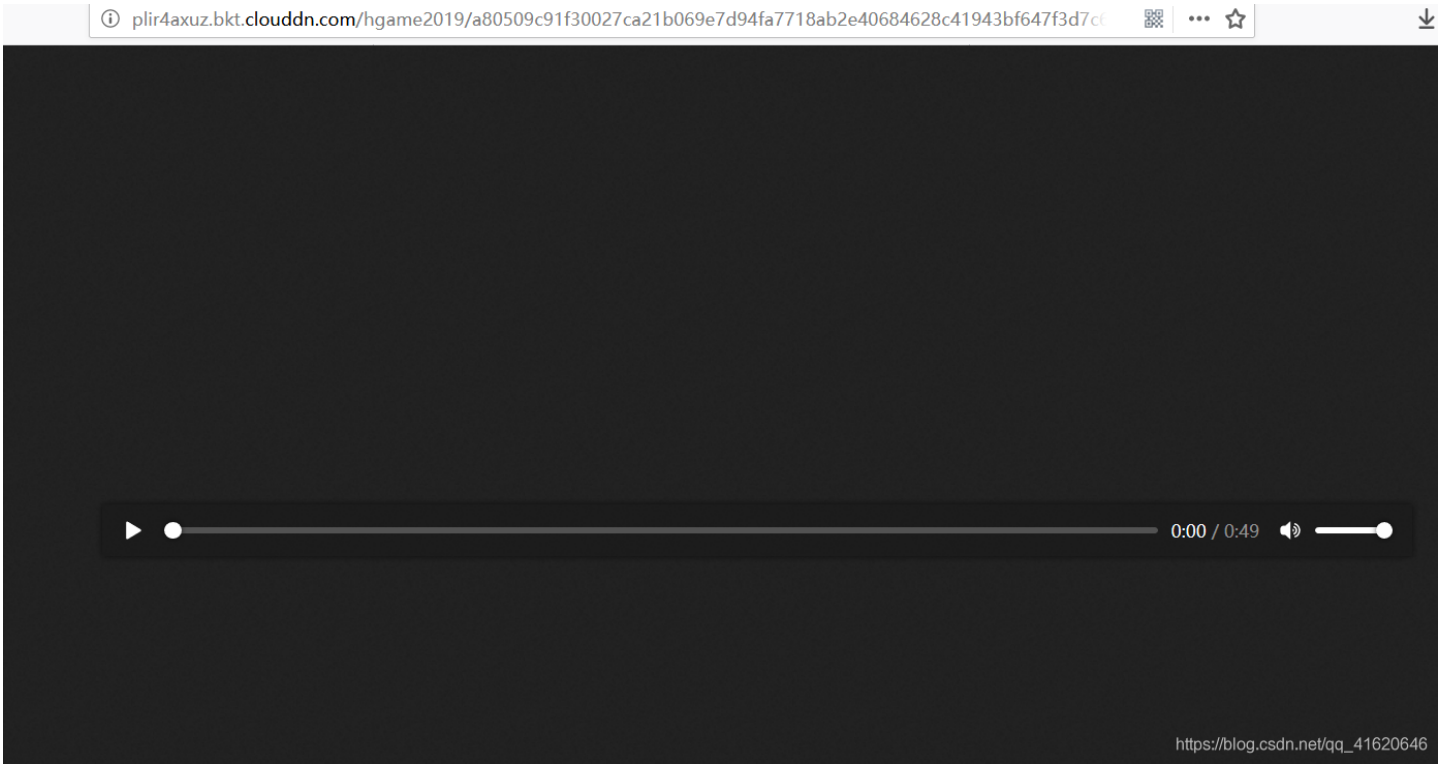
最近作为新人（=菜鸡）参加杭电vidar的hgame寒假ctf培训，碰到一道音频隐写题。

描述

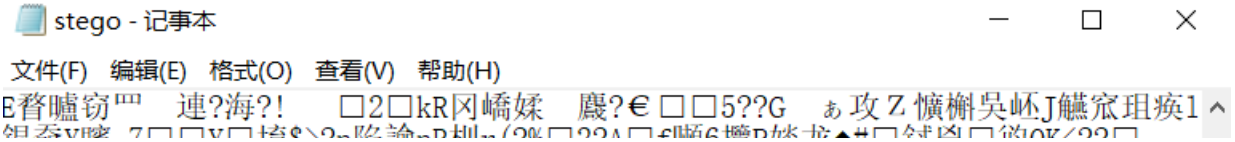
一首MP3,好好听哦，flag由大写英文字母、数字以及下划线组成，记得添加hgame{}

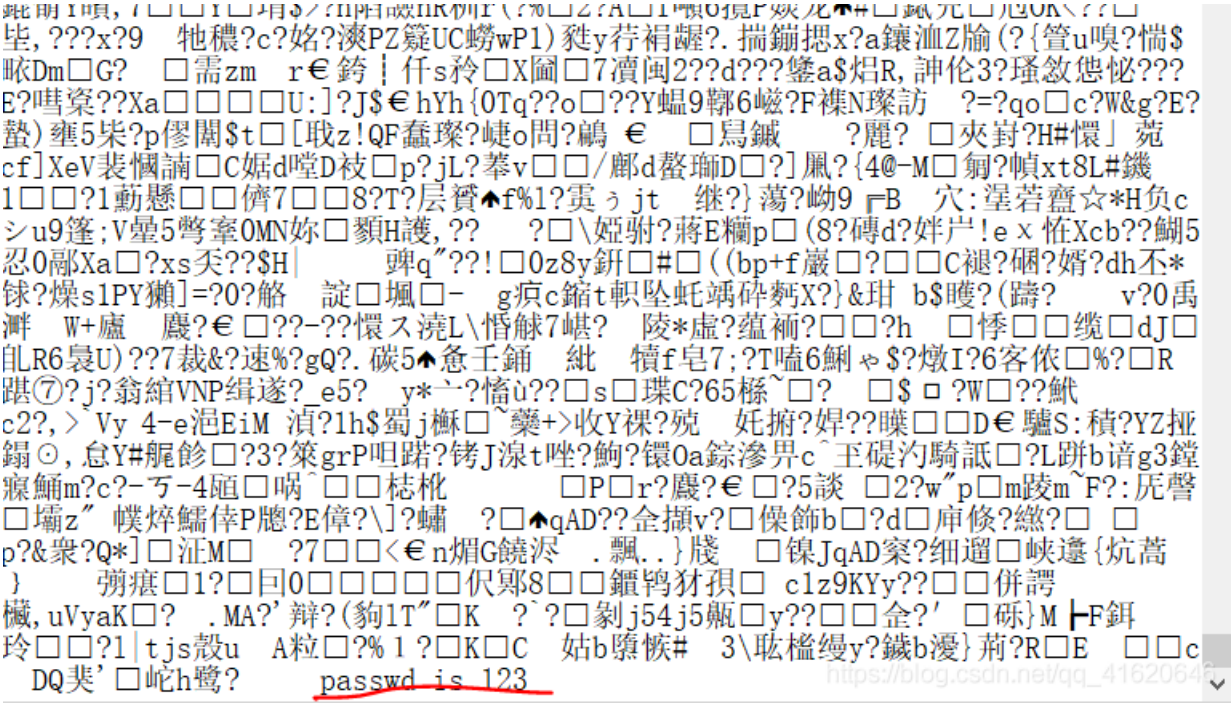
URL http://plir4axuz.bkt.clouddn.com/hgame2019/a80509c91f30027ca21b069e7d94fa7718ab2e40684628c41943bf647f3d7c6a/stego.mp3

打开url，发现是一个mp3文件：



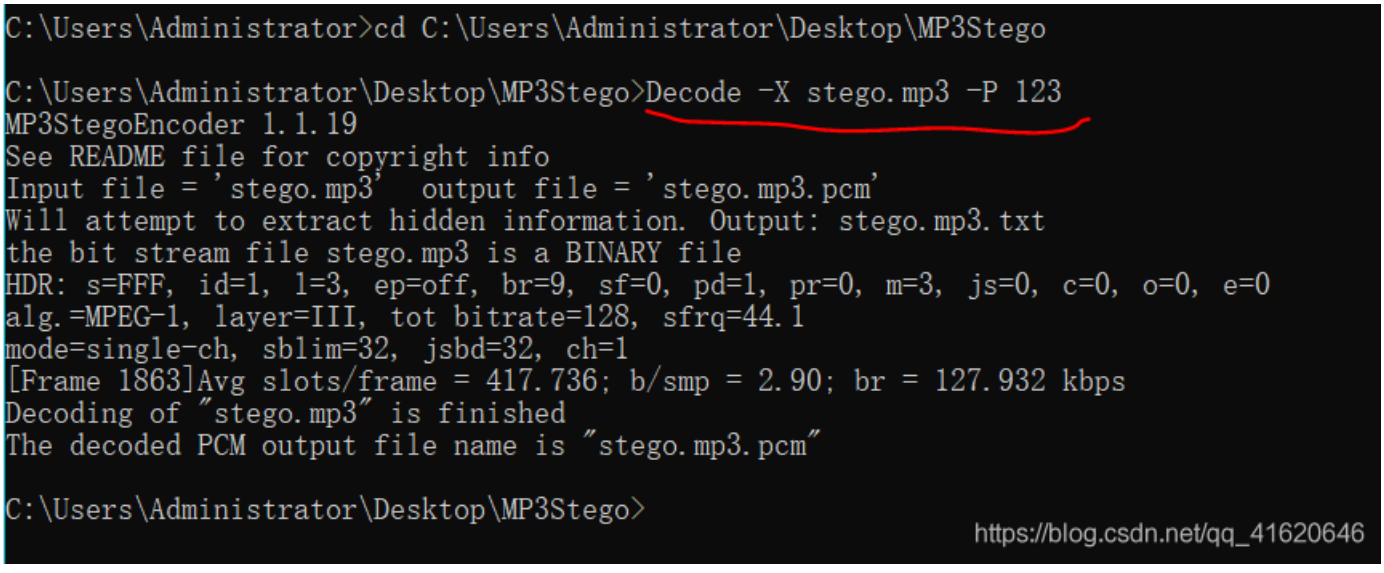
将其下载到本地。然后百度ctf mp3相关内容，下载工具MP3stego，并将下载来的音频文件放到MP3stego的文件目录下。然后以txt文件格式打开下载来的mp3文件，在最后发现：





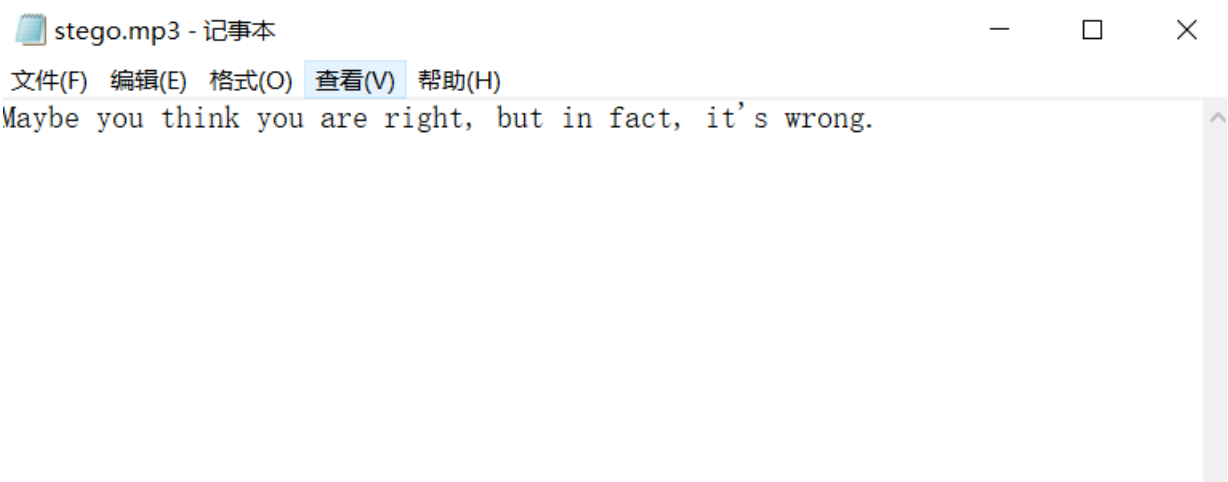
这个password我们马上会用到。

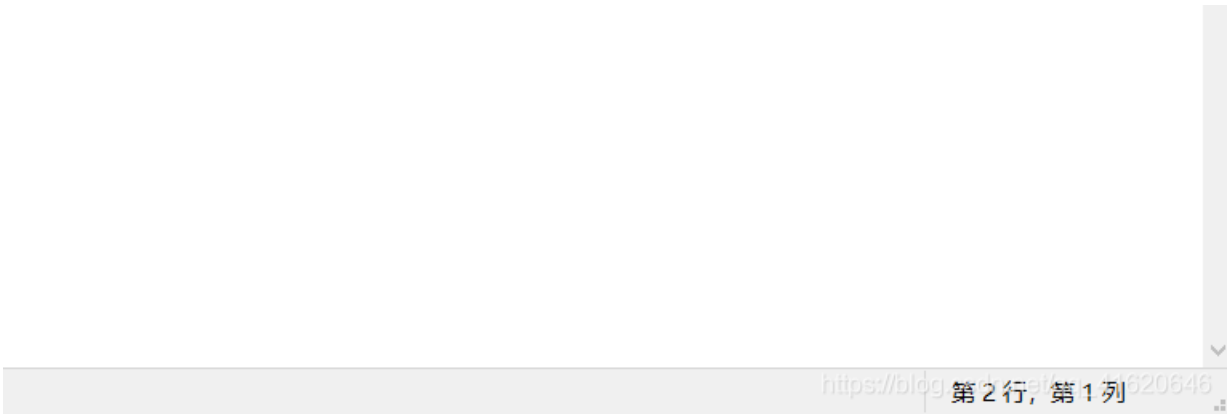
接下来打开cmd命令窗口，cd 进MP3stego的目录下，输入以下指令：`Decode -X stego.mp3 -P 123`
其中-X参数后跟同目录下的mp3文件名，-P后面跟密码，然后如图：



此时

会在同目录下生成1个txt文件，打开就应该能得到flag了（嗯，我本来是这样想的）



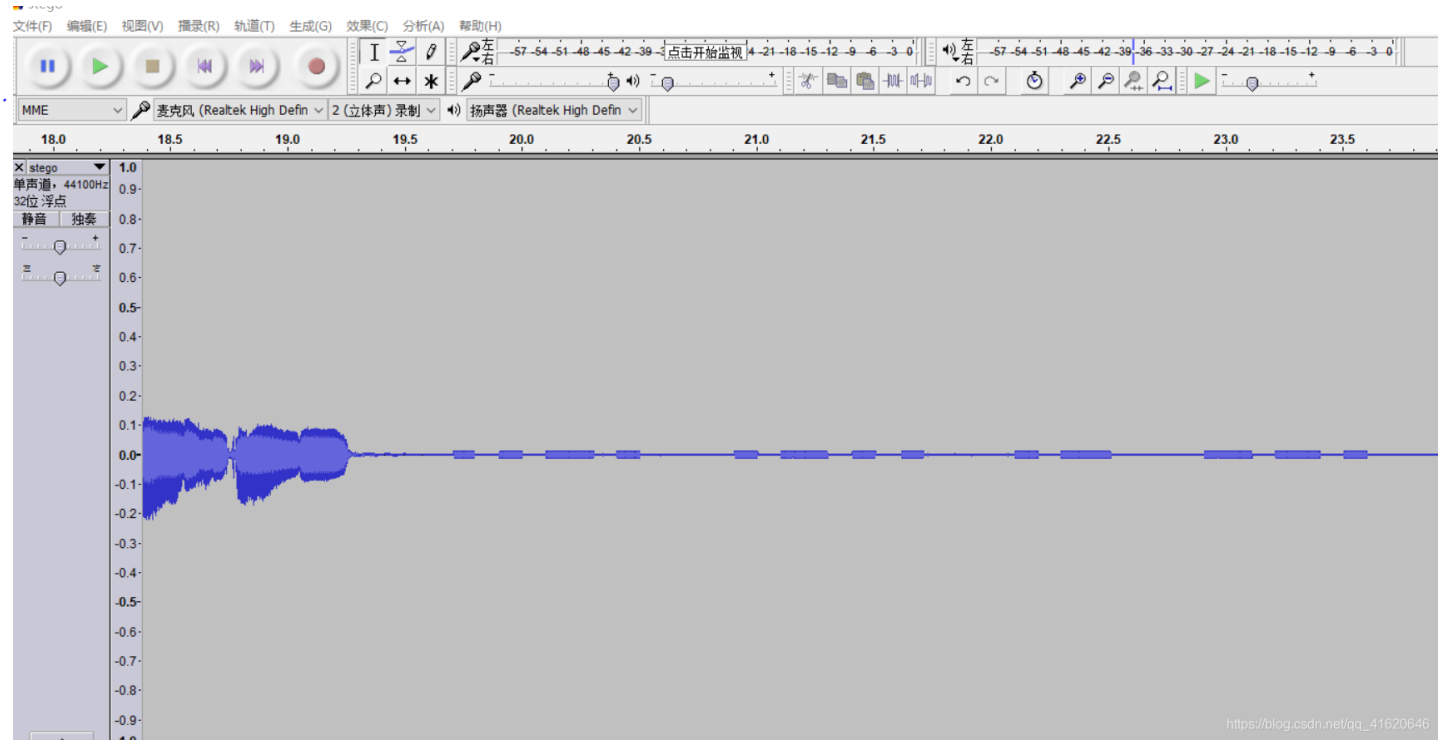


卧

槽！！！！！！！！！！！！！！！！完全被出题人套路了。。。~~好想打出题人~~

于是此方法行不通，另想出路。

想起来那个MP3文件我只听了一点，于是先把它听完。发现前面是歌声，后面却是“滴滴滴”的声音，猜想可能是摩尔斯电码。于是百度相关信息，下载工具Autacity,打开mp3文件：



前面的应该是歌声，后面的就是摩尔斯电码了。那些窄一点的就代表摩尔斯电码中的`.`,而宽的就代表摩尔斯电码中的`_`，长的

```
. . _.                  F
. _. .                  L
. _                     A
__.                     G
___. . .                :
. ____                  1
_                       T

. . __. _
. ___                   J
. . _                   U
. . . . .               5
_                       T

. . __. _
. . . . _               4
```

https://blog.csdn.net/qq_41620646

间隔将2个字符分开。于是查表，写出对应的字符：

其中，并没有在表中找到`..--.-`代表的字符，又因为flag包含大写字母，数字，下划线，所以猜想应该是下划线。于是最后的flag就应该是：`hgame{1T_JU5T_4_EASY_WAV}`。提交，发现正确。本题完。