鹤城杯杂项MISC部分WP

原创

HackerTenG 于 2021-10-09 17:11:29 发布 1917 收藏 2

分类专栏： CTF 文章标签： 信息安全 网络安全 web安全

本文链接：https://blog.csdn.net/qq_45615127/article/details/120674284

Preface

昨天的比赛又一次见识到了大师傅们多么厉害，疯狂上分，可怜如我，只做出了四个杂项。趁着比赛刚过就写下我的做题思路，也会去看下其他师傅的WP学习下，文中有我理解错误的思路烦请师傅们多多指教

Process

NEW_MISC

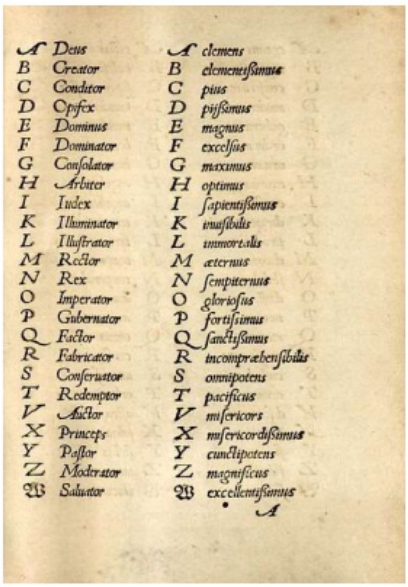
下载附件以后就是一个PDF

2021/8/23 Steganographie – Wikipedia

Nicetext verwandelt eine Binärdatei in pseudo-natürlichen Text. Dazu benutzt das Programm kontextfreie Grammatiken. Das Programm enthält ein Wörterbuch und Schreibstile. Das Wörterbuch enthält englische Wörter, die in fünf grammatische Typen klassifiziert sind (Artikel, Substantiv, Verb, Adjektiv, Präposition). Der Stil bestimmt die syntaktischen Regeln für verschiedene Satztypen. Ein einfacher Satz hat z. B. den Aufbau ART-SUBST-VERB-ART-SUBST.

Für die Transformation wählt der Kodierer einen Stil. Die Input-Bits dienen als Pointer auf die Wörter in den verschiedenen Klassen des Wörterbuchs. Die Dekodierung beruht auf einfacher reverser Codebook-Suche.

Beispiel zum Prinzip: Angenommen das Wörterbuch enthält vier Wörter in der Klasse ART (mit den binären Indizes 00 bis 11) und 32 Wörter in SUBST (mit den binären Indizes 00000 bis 11111). Die Eingabe sei die Bitfolge 0101110. Die ersten zwei Bit der Eingabe (01) werden durch das zweite Wort in ART ersetzt. Das nächste Wort entspricht dem 15. Wort in SUBST.

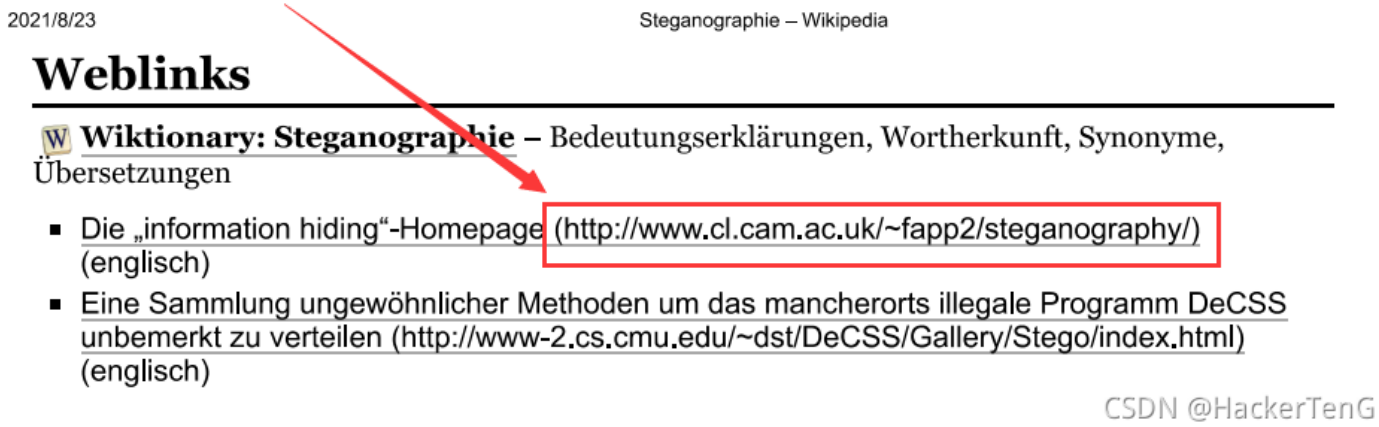


Buchstaben-Wort-Substitutionstabelle zu Beginn von Buch I der *Polygraphia* von Johannes Trithemius[6]

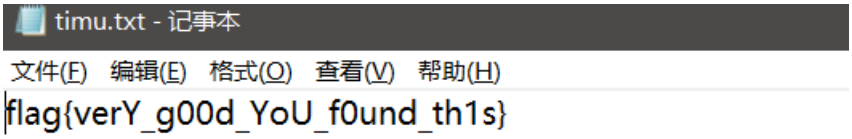
Semagramm

Eine Unterklasse der linguistischen Steganographie ist das Semagramm. Dabei werden durch kleine Details in einer an sich unverfänglichen Nachricht, einem Bild oder einer Zeichnung Informationen übertragen.

最开始我还以为有隐藏文件啥的，分离了下啥也没有。然后又换思路，开始看下PDF内容，发现这个单词表以后还以为是文章对应单词转换字母得出flag（不知道有没有师傅们跟我一样），看了好久以后都没找到这个表里面的单词，甚至还用百度翻译看了部分内容哈哈哈哈哈。然后发现有一个提示信息，咱也不知道是不是出题人的意图

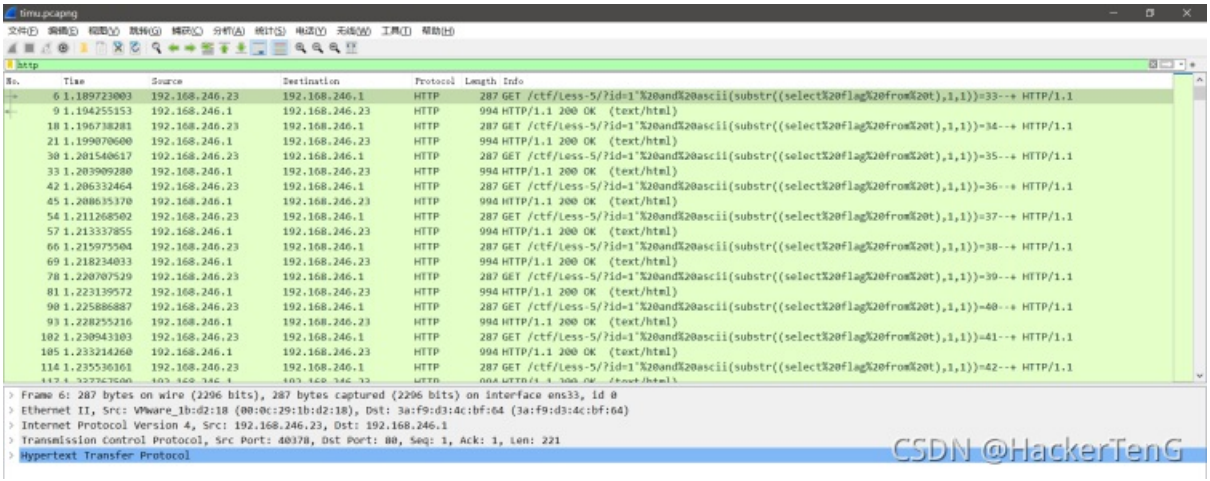


看到hiding这个单词就想着是不是线索，然后就打开网址看了下，是一篇介绍隐写术的文章，于是想到了隐写，但是之前没有接触到关于PDF隐写的知识（太菜了），然后就直接百度了下，竟然还找出来了，可以直接用**wbstego4.3open**查看PDF隐藏文件，下载以后直接导出一下PDF的隐藏信息就得到flag啦



流量分析

这个下载附件以后直接就是一个流量包，Wireshark打开就看到了sql注入的数据，筛选出http数据仔细查看是布尔盲注，也没有往其他地方想

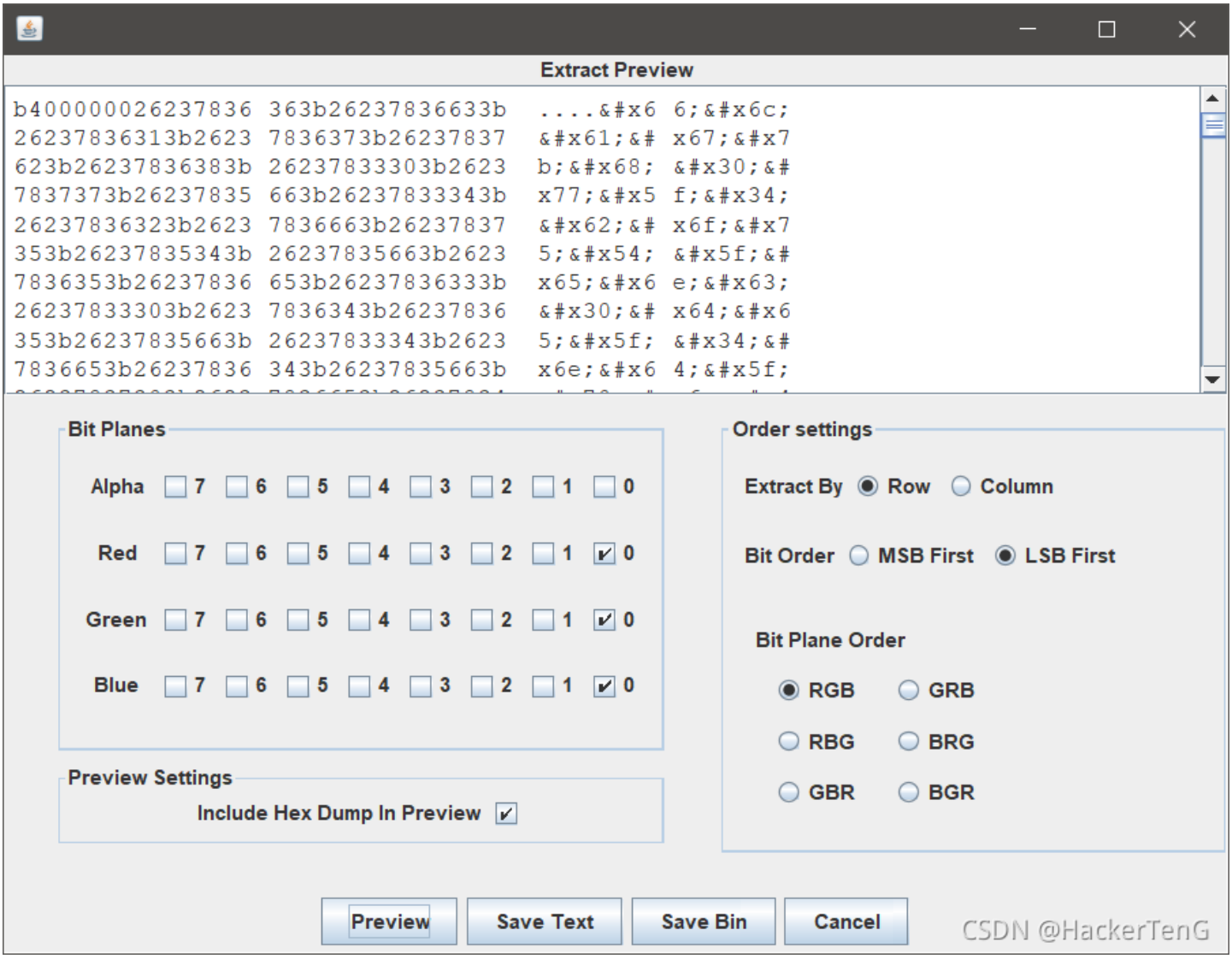


我是直接一条一条的往下翻爆破记录的最大ASCII码数字（求师傅们给个快捷的方法），然后记录下来直接用python转成对应的字符串就是flag

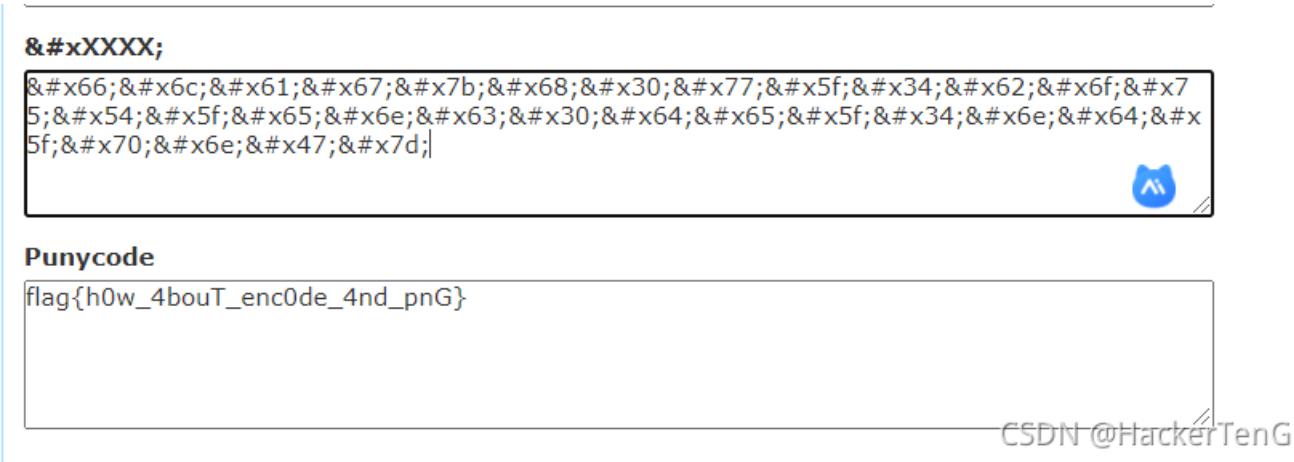
```
流量分析
102,108,97,103,123,119,49,114,101,115,104,65,82,75,95,101,122,95,49,115,110,116,105,116,125,126,126
flag{w1reshARK_ez_1sntit}
```

MISC2

下载附件只有一个check.png的图片，本来以为是常见的高度隐藏信息或者图片分离，结果都不是，查看文件属性发现位深度是32，于是想到了LSB隐写。而且用Stegsolve查看alpha通道为0时的图片是空白，所以判断alpha通道没有隐藏数据，然后就查看下红蓝绿最低位信息



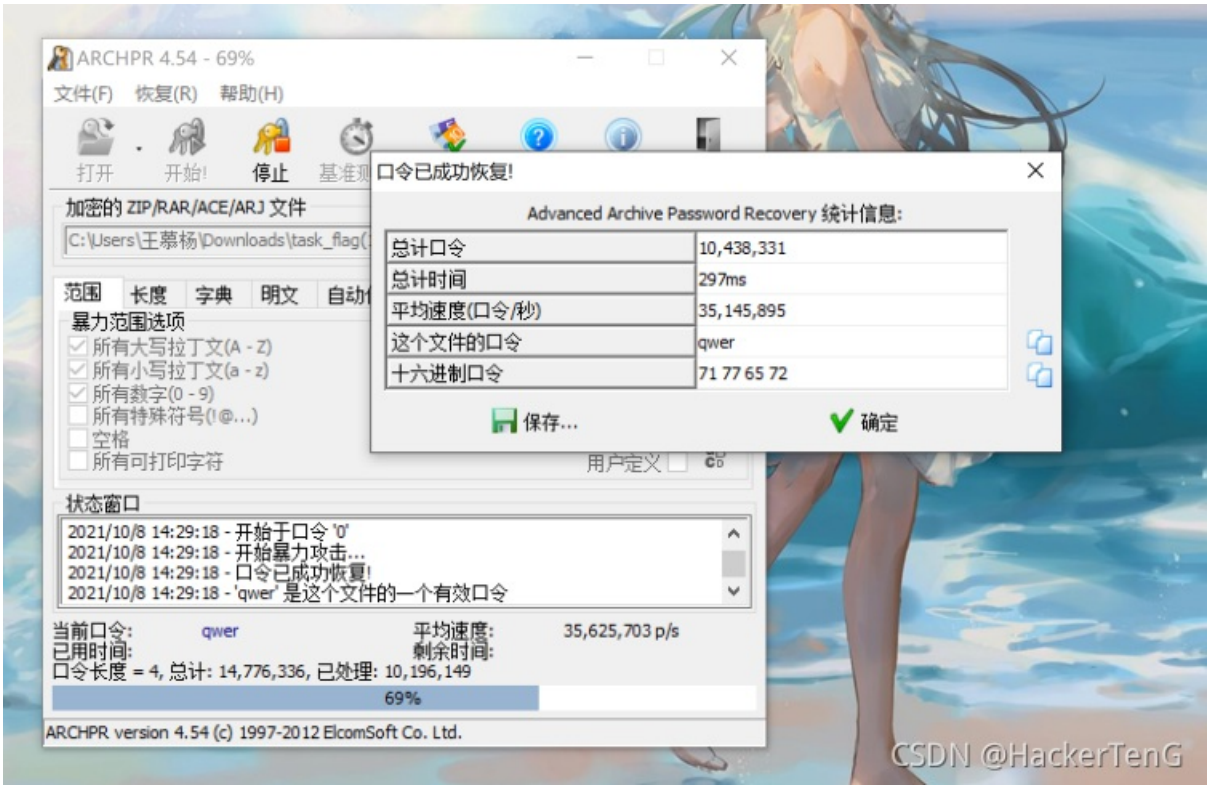
前面发现一堆编码，但是同样之前还没有做过一样的题，可是直觉感觉这就是flag了，发给学长看了下，刚想试下是不是16进制编码，学长解出来了已经



而且我也试了下提取出的每段数字就是16进制编码

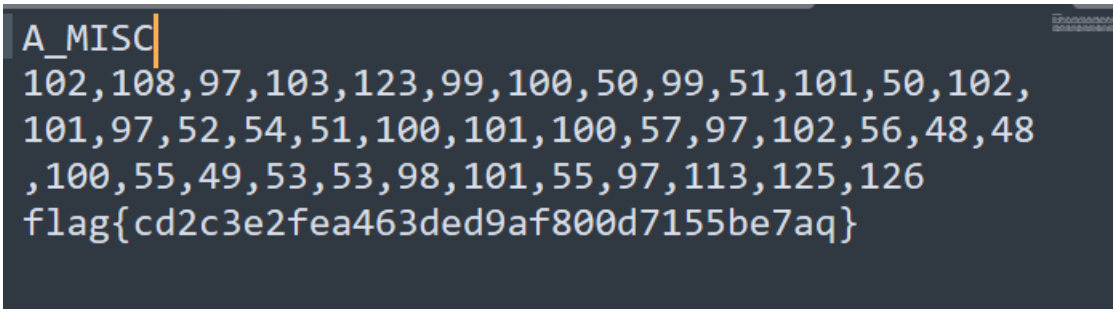
A_MISC

这个是我感觉这几个题目中最麻烦的了，附件下载后发现压缩包需要密码，我就去看是不是压缩包伪加密，自己看了下不是但是有点不太确定，于是又专门百度了下伪加密头，确定以后又分离了下压缩包依然没有线索。然后就试下爆破，问题是也没给提示，我看了下爆破时间以后就关闭了，本来不打算做这个题了，过了一会儿学弟说他爆破出来密码了，当时自己都没想到真是爆破。



压缩包密码是qwer（出题人一定没少打LOL），然后就开始往下进行。打开压缩包以后只有一张图片，图片内容就是一个云盘链接，啥也没管先打开链接看看，发现需要密码。然后又回过头看，感觉图片高度有问题，修改高度以后发现提取码

然后提取出来还是一个流量包，Wireshark打开以后一看还是sql注入流量，只不过换成了时间盲注，方法与前面流量解析一样，提取出ASCII码以后转换为字符串得到flag



之所以说这道题麻烦是并没有太难，而且太复杂了，一层套一层，无限套娃，到比赛结束也就做了这几道题。Web那个Spring是原题，学长给我发了下链接我复现了下，没什么写的。

Ending

暑假这三个月都没有做CTF题，明年就要专升本了，所以一直在看高数英语（嗐，高中贪玩儿的后果）。CTF很多知识都忘了，看来以后还是要抽时间做CTF题了，最后欢迎各位师傅多多指教哦