

攻防世界crypto中 banana-princess的 writeup，真是坑啊

原创

隐藏起来 于 2020-03-29 20:34:14 发布 2832 收藏 5

分类专栏: [CTF # crypto](#)

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/dchua123/article/details/105185194>

版权



[CTF 同时被 2 个专栏收录](#)

20 篇文章 3 订阅

订阅专栏



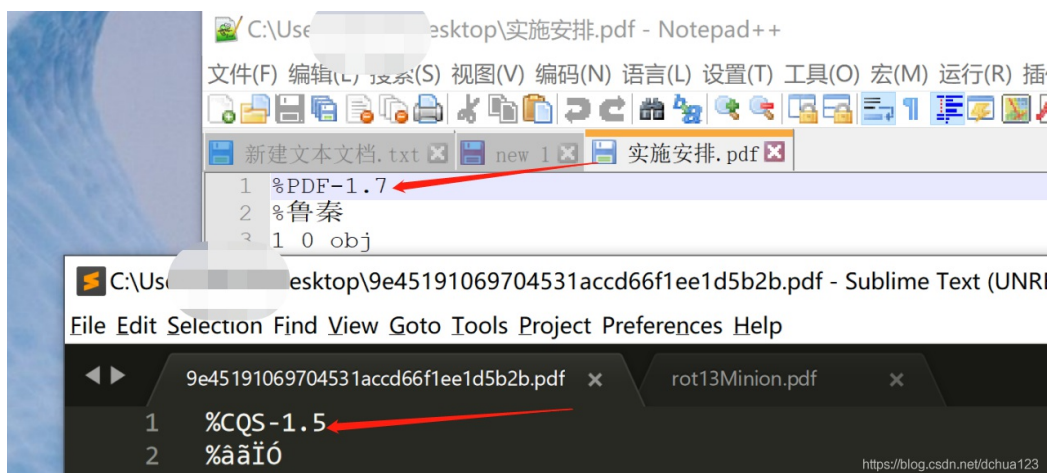
[crypto](#)

15 篇文章 0 订阅

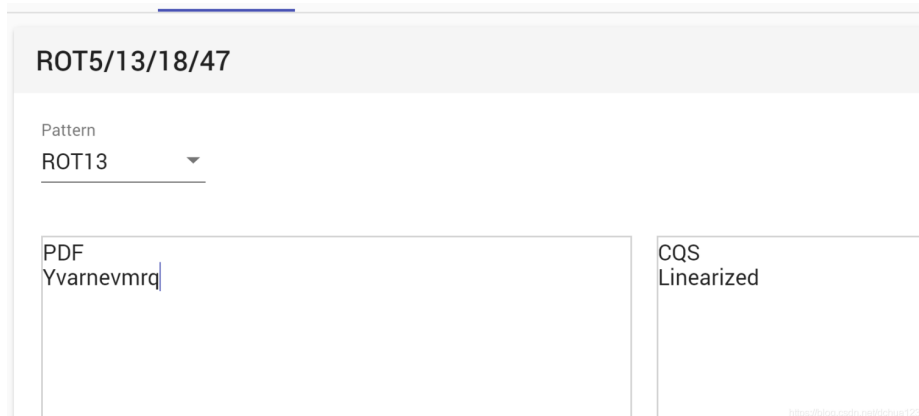
订阅专栏

这个题折腾了好久都没有思路, pdf打不开, 也没有任何的提示, 后来实在没辙了, 找了个pdf来对比, 终于有了发现:

1、对比一个正常能打开的pdf和题目的pdf头, 发现如下 (notepad++打开的是正常的):



一个是%PDF-1.7, 另外一个为%CQS-1.5。形式完全一样啊, 数字可以理解为版本号。那就思路来了, 估计是进行了位移? 尝试后发现:



随便抓了一段在前面的字符, 解密也可得一个看着是有意义的单词。

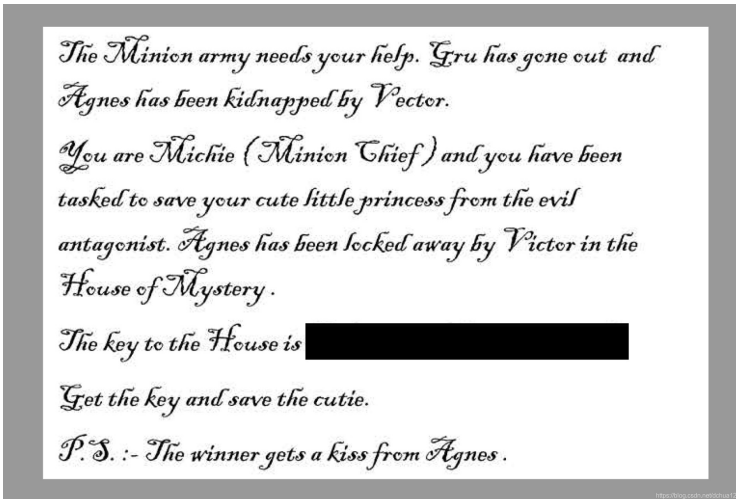
2、通过上述描述, 进行rot13解密:

```
cat 9e45191069704531accd66f1ee1d5b2b.pdf | tr 'A-Za-z' 'N-ZA-Mn-za-m' > new.pdf
```

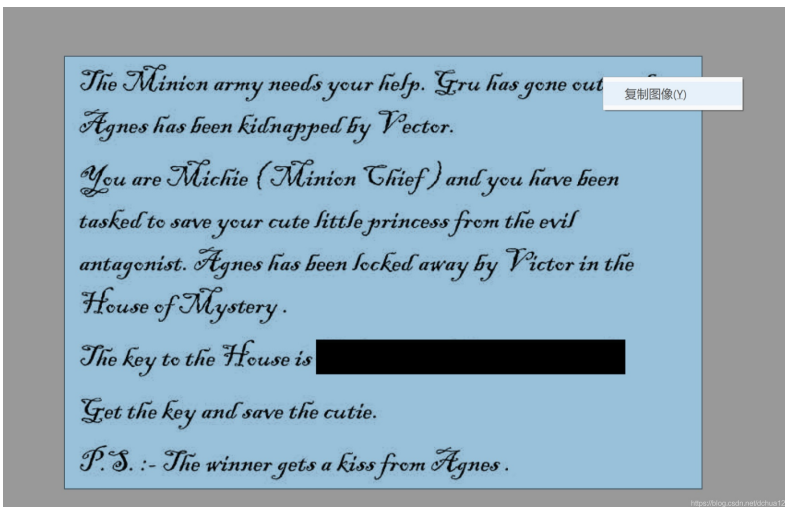
```
root@kali:~/Desktop# cat 9e45191069704531accd66f1ee1d5b2b.pdf | tr 'A-Za-z' 'N-ZA-Mn-za-m' > new.pdf  
root@kali:~/Desktop#
```

<https://blog.csdn.net/dchua123>

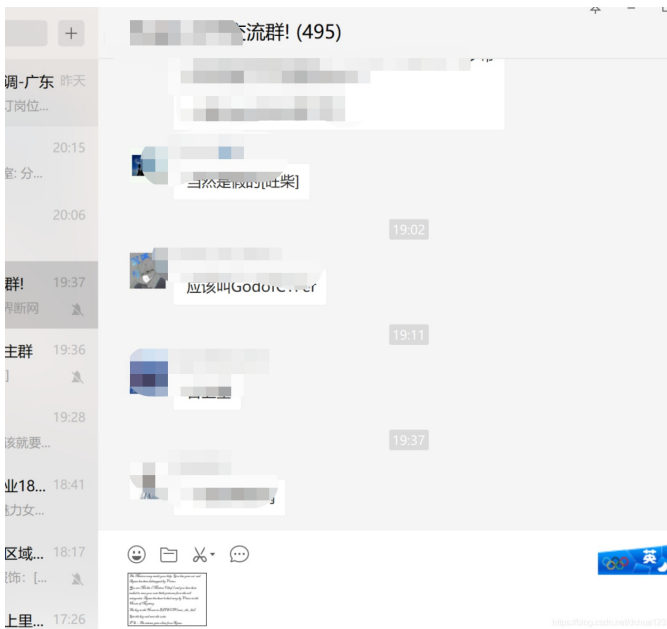
3、现在就可以打开pdf了，如下：



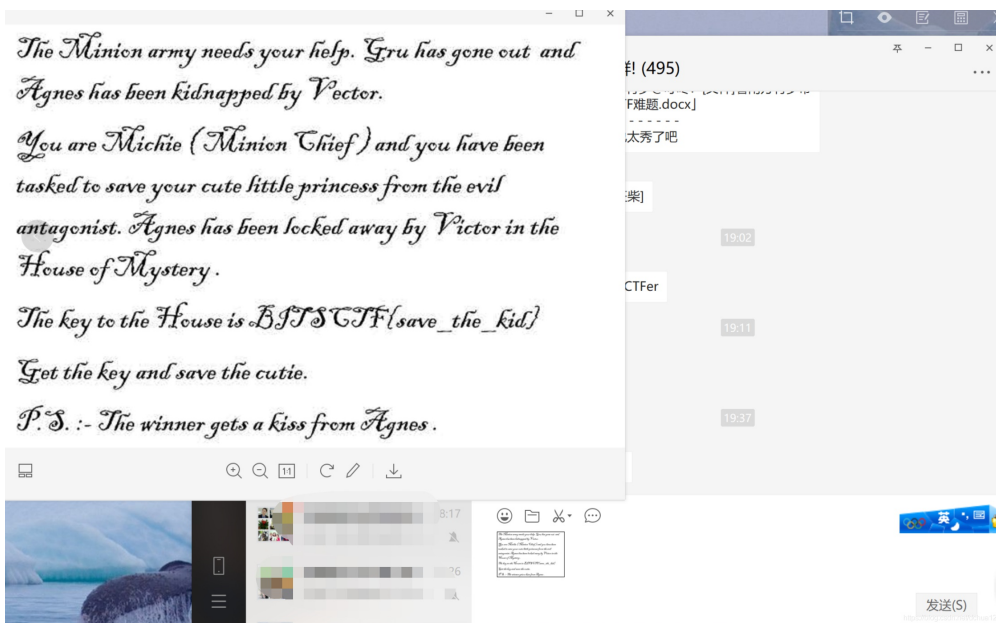
4、坑啊，flag被遮盖了，好在直接复制就能出来，方法如下：



5、将图片粘贴到绘图里面去，或者聊天窗口里去，即可看到flag啦，双击放大即可：



辨认了好久，flag如下：



BITSCTF{save_the_kid}