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





 CTF 同时被2个专栏收录

 20 篇文章3 订阅

订阅专栏



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):

SI M						
	文件(F) 编辑(L) 以天示(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插					
	[3]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]					
	🔚 新建文本文档.txt 🛛 🔚 new 1 🗵 📙 实施安排.pdf 🗵					
	1 %PDF-1.7					
	2 8 音 秦 3 1 0 obj					
C:\Us	esktop\9e45191069704531accd66f1ee1d5b2b.pdf - Sublime Text (UNRI					
Eile Edit Selection Find View Goto Tools Project Preferences Help						
۹ ۲۰	e45191069704531accd66f1ee1d5b2b.pdf × rot13Minion.pdf ×					
1 2	%CQS-1.5 %âãÏÓ https://blog.csdn.net/dchua123					

一个是%PDF-1.7,另外一个是%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:

ROT5/13/18/47	
Pattern ROT13 -	
PDF Yvarnevmrq	CQS Linearized

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:

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

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:

+	流群! (495)		수 - u
调-广东 昨天 丁岗位…	10000	- 1 Ja	
20:15 室: 分			
群! 19:37 早断网 🕱			
主群 19:36			
<u>x</u> [
19:28 该就要			
业18 18:41 訪女			
区域 18:17 }饰:[🖹	Image: State of the s		999) <mark>#</mark> _
<u>上里</u> 17:26	$\label{eq:rescaled} \begin{split} & \mathrm{Ke}_{\mathrm{S}} = \mathrm{A} \int \mathrm{Ke}_{\mathrm{S}} = \mathrm{A} \int \mathrm{S} \mathrm{P} (\mathrm{P} (\mathrm{P} (\mathrm{P} (\mathrm{P} (\mathrm{A} \mathrm{A} \mathrm{A} \mathrm{A} \mathrm{A} \mathrm{A} \mathrm{A} \mathrm{A} $		

辨认了好久, flag如下:

- 🗆 X		
The Minion army needs your help. Gru has gone out and Agnes has been kidnapped by Vector.	É! (495) F滩题.docxI	∓ - □ ×
You are Michie (Minion Chief) and you have been	太秀了吧	
tasked to save your cute little princess from the evil	[柴]	
antagonist. Agnes has been locked away by Victor in the		
Thouse of Mystery.	CTFer	
The key to the House is BITSCIF (save_the_kid)		
Get the key and save the cutie.		
P.S. :- The winner gets a kiss from Agnes .		
B17 B17 C B17 C C B17 C C C C C C C C C C C C C		<mark></mark>
		发送(S)

BITSCTF{save_the_kid}