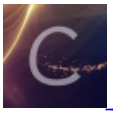
bugku-writeup-MISC-你想要的种子嘛

原创

dark2019 于 2021-07-22 10:30:54 发布 51 收藏
分类专栏： 信息安全 wp 文章标签： 杂项 bugku



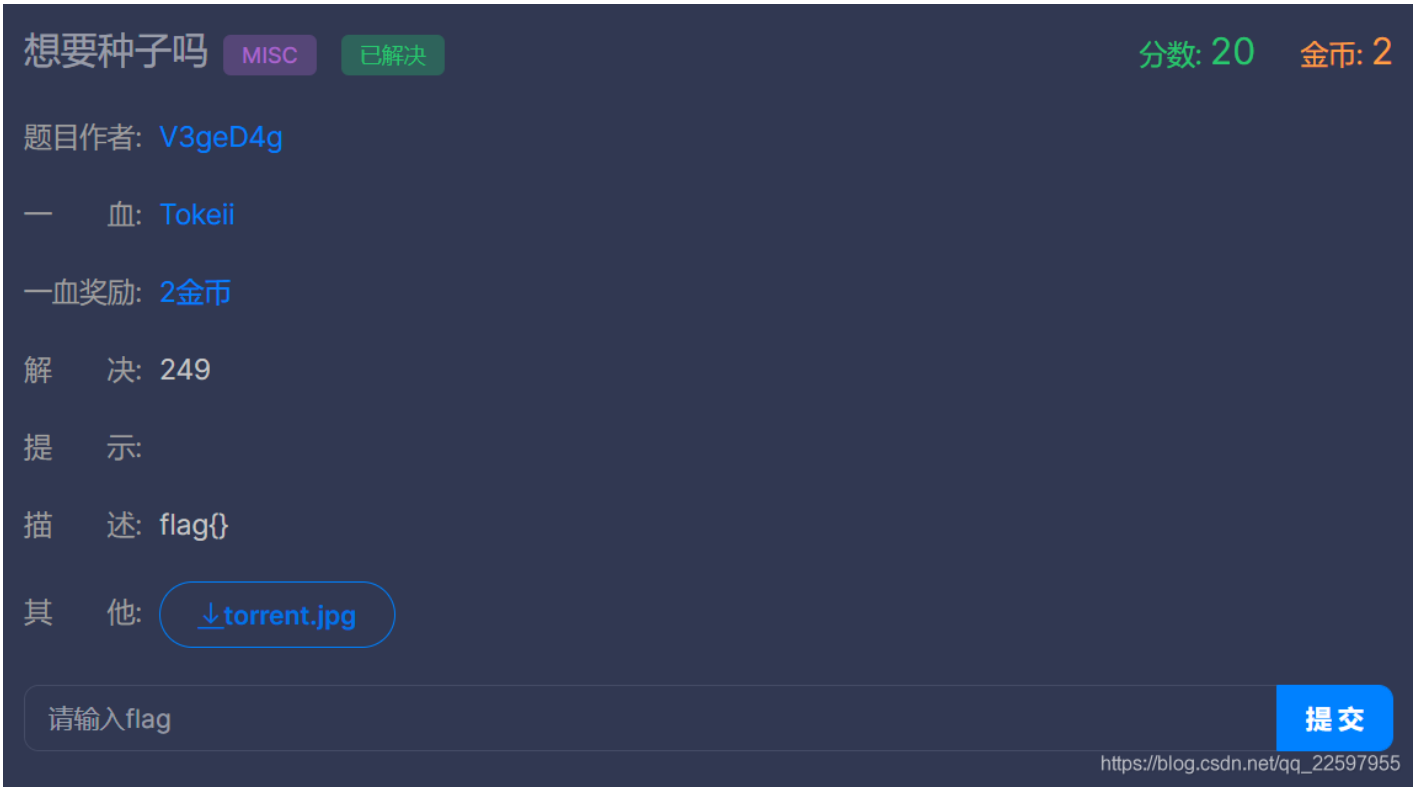
题目：你想要种子嘛

考察点：图片隐写

工具：steghide

binwalk

010 editor



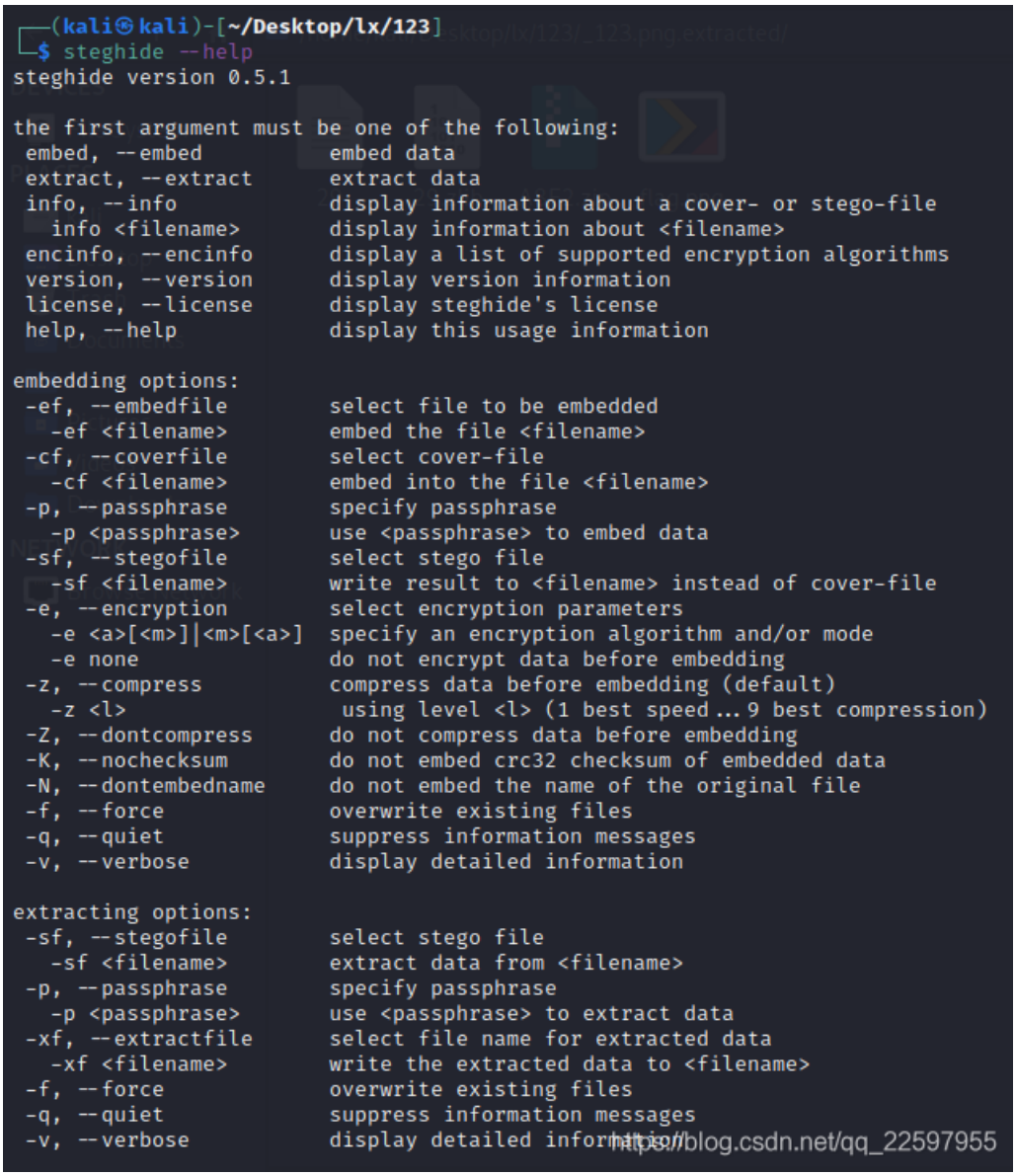
01—steghide

安装命令：

```
apt-get install steghide
```

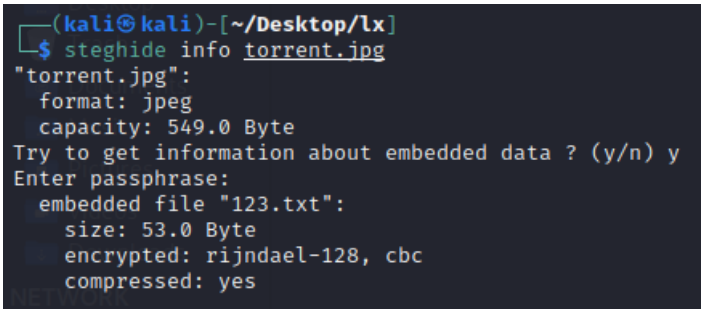
查看使用手册：

```
steghide --help
```



查看文件信息：

```
steghide info torrent.jpg
```

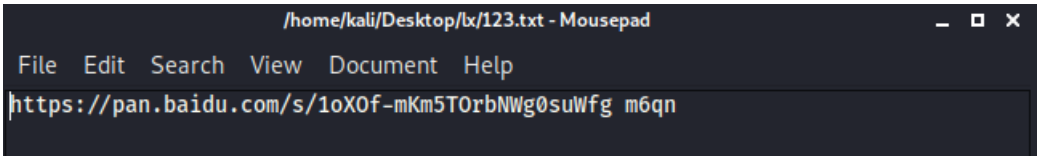


提取文件：

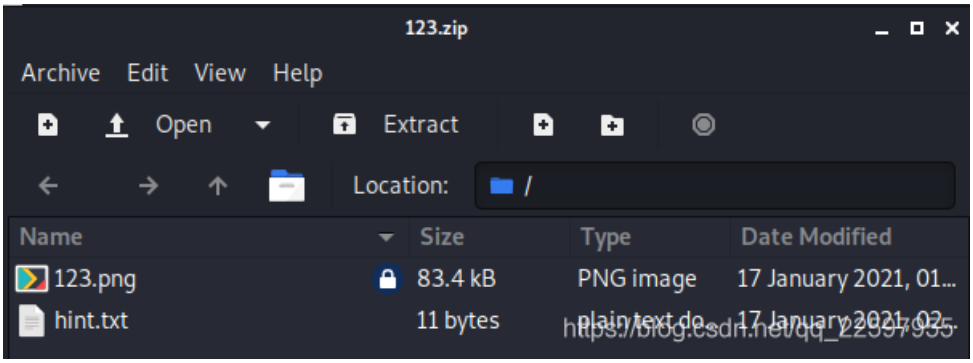
```
steghide extract -sf torrent.jpg
```

```
┌──(kali㉿kali)-[~/Desktop/lx]
└─$ steghide extract -sf torrent.jpg
Enter passphrase:
wrote extracted data to "123.txt".
```

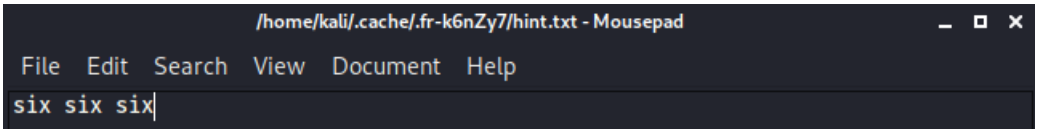
得到123.txt,https://pan.baidu.com/s/1oXOf-mKm5TOrbNWg0suWfg m6qn



使用百度网盘下载，得到123.zip,其中包含加密的123.png，hin.txt文件



打开hint.txt文件：



尝试使用666，打开123.png，错误；使用666666，打开123.png，正确。

傻了吧，

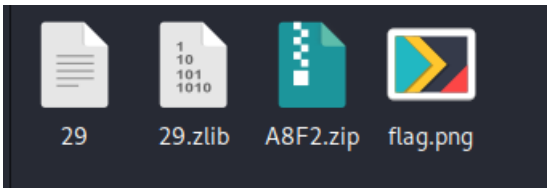
这里啥都没有

得到123.png。

02—binwalk分离

使用binwalk分离图片。

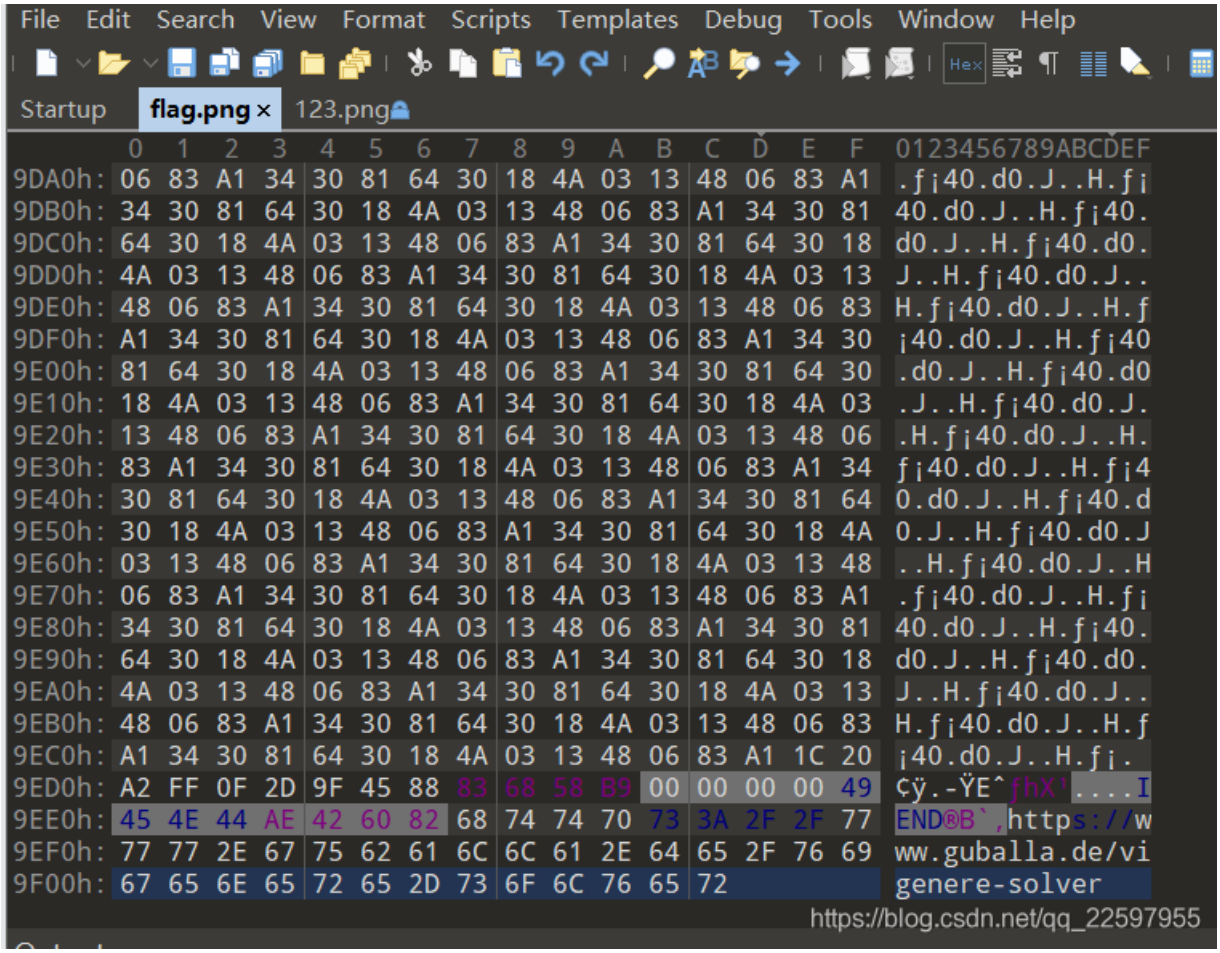
```
┌──(kali㉿kali)-[~/Desktop/lx/123]
└─$ binwalk -e 123.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 292 x 282, 8-bit/color RGBA, non-interlaced
41            0x29            Zlib compressed data, default compression
43250         0xA8F2          Zip archive data, at least v2.0 to extract, compressed size: 40009, uncompressed size: 40717, name: flag.png
83387         0x145BB         End of Zip archive, footer length: 22
```



得到flag.png。

03—010 editor 编辑图片

使用010 editor打开图片。



下拉框到最后，发现一个链接：

https://www.guballa.de/vigenere-solver

修改图片高度，与宽相同。

File Edit Search View Format Scripts Templates Debug Tools Window Help

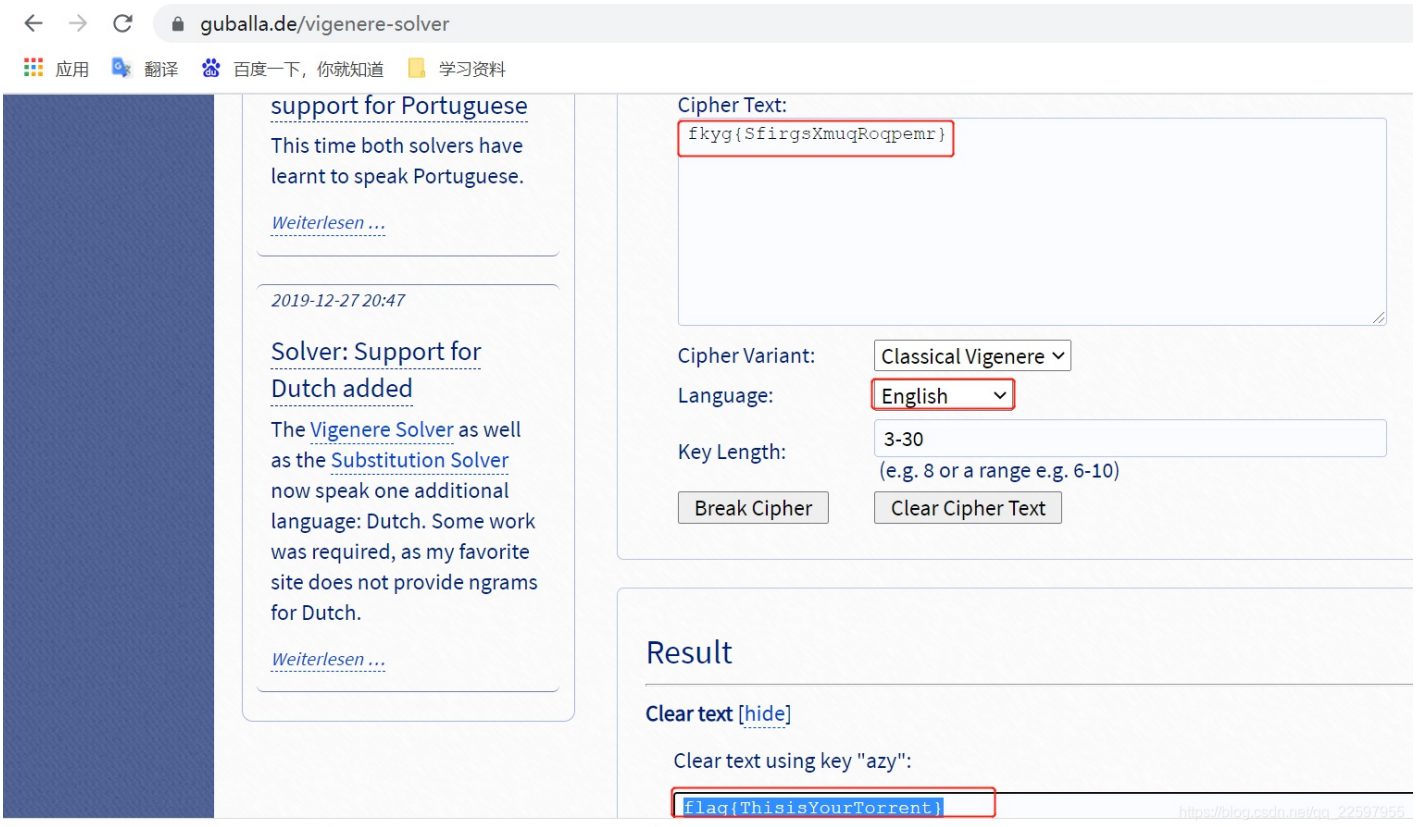
Startup flag.png × 123.png

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG....IHDR
0010h:	00	00	01	24	00	00	01	24	08	06	00	00	00	B8	89	2A	...$...$.....¸‰*
0020h:	31	00	00	20	00	49	44	41	54	78	9C	EC	BD	F9	B3	24	1.. .IDATxœì½ù³$
0030h:	C7	75	2E	F6	D5	D6	DB	ED	BE	EB	AC	98	19	60	06	43	Çu.öÕÖÛí¾ë¬˜.`.C
0040h:	62	23	00	12	20	45	89	84	29	89	22	29	D9	7E	11	B6	b#.. E‰„)‰")Ù~.¶
0050h:	C3	11	FE	C1	A1	BF	C4	61	FF	43	0E	4B	0E	85	43	72	Ã.þÁ¡¿Äaÿ C.K.…Cr
0060h:	58	F2	93	A5	17	94	48	09	24	44	00	C2	60	C7	0C	30	Xò“¥.”H.$D.Â`Ç.0
0070h:	98	FD	EE	B7	D7	DA	1D	DF	C9	3C	D5	D9	75	FB	CE	0C	˜ýî·×Ú.ßÉ<ÕÙuûÎ.
0080h:	08	CC	E0	F2	BD	4E	B0	79	A7	BB	AB	AB	B2	B2	32	BF	.Ìàò½N°y§»««²²2¿
0090h:	3C	E7	3B	9B	57	96	65	89	45	5B	B4	45	5B	B4	63	D0	<ç;›W–e‰E[´E[´cÐ
00A0h:	FC	C5	43	58	B4	45	5B	B4	E3	D2	16	80	B4	68	8B	B6	üÅCX´E[´ãÒ.€´h‹¶
00B0h:	68	C7	A6	2D	00	69	D1	16	6D	D1	8E	4D	5B	00	D2	A2	hÇ¦-.iÑ.mÑŽM[.Ò¢
00C0h:	2D	DA	A2	1D	9B	B6	00	A4	45	5B	B4	45	3B	36	6D	01	-Ú¢.›¶.¤E[´E;6m.
00D0h:	48	8B	B6	68	8B	76	6C	DA	02	90	16	6D	D1	16	ED	D8	H‹¶h‹vlÚ...mÑ.íØ
00E0h:	B4	05	20	2D	DA	A2	2D	DA	B1	69	0B	40	5A	B4	45	5B	´. -Ú¢-Ú±i.@Z´E[
00F0h:	B4	63	D3	16	80	B4	68	8B	B6	68	C7	A6	2D	00	69	D1	´cÓ.€´h‹¶hÇ¦-.iÑ
0100h:	16	6D	D1	8E	4D	5B	00	D2	A2	2D	DA	A2	1D	9B	B6	00	.mÑŽM[.Ò¢-Ú¢.›¶.
0110h:	A4	45	5B	B4	45	3B	36	6D	01	48	8B	B6	68	8B	76	6C	¤E[´E;6m.H‹¶h‹vl
0120h:	DA	02	90	16	6D	D1	16	ED	D8	B4	05	20	2D	DA	A2	2D	Ú...mÑ.íØ´. -Ú¢-
0130h:	DA	B1	69	0B	40	5A	B4	45	5B	B4	63	D3	16	80	B4	68	Ú±i.@Z´E[´cÓ.€´h
0140h:	8B	B6	68	C7	A6	2D	00	69	D1	16	6D	D1	8E	4D	5B	00	‹¶hÇ¦-.iÑ.mÑŽM[.
0150h:	D2	A2	2D	DA	A2	1D	9B	B6	00	A4	45	5B	B4	45	3B	36	Ò¢-Ú¢.›¶.¤E[´E;6
0160h:	6D	01	48	8B	B6	68	8B	76	6C	DA	02	90	16	6D	D1	16	m.H‹¶h‹vlÚ...mÑ.
0170h:	ED	D8	B4	05	20	2D	DA	A2	2D	DA	B1	69	0B	40	5A	B4	íØ´. -Ú¢-Ú±i.@Z´

Output https://blog.csdn.net/qq_22597955

fkyg{SfirgsXmuqRoqpemr}

得到 fkyg{SfirgsXmuqRoqpemr}，放入链接https://www.guballa.de/vigenere-solver中。



解码，得到flag。

写在最后：解题思路为查找隐藏信息-解密-再次查找隐藏信息-解密，本题为多重信息隐藏，需要耐心不断查找，再加以解密，得到结果。