

Bugku - 好多压缩包 - Writeup

转载

baikeng3674 于 2017-06-06 13:53:00 发布 124 收藏

原文链接: <http://www.cnblogs.com/WangAoBo/p/6951160.html>

版权

bugku - 好多压缩包 - Writeup

M4x原创, 转载请注明出处

这道题前前后后做了好几天, 这里记录一下

题目

题目 18 Solved

好多压缩包

200

123.zip

Key

SUBMIT

文件下载

分析

- 解压下载后的文件, 发现有68个压缩文件, 并且每个压缩文件里都有一个4个字节大小的名为data.txt的txt文件, 于是尝试用crc32碰撞还原出所有压缩包中的文件内容

名称	压缩后大小	原始大小	类型	修改日期	压缩方法	加密方法	循环冗余检...	属性	注释
data.txt*	18	4	TXT 文件	2016/8/2...	Deflate	ZipCrypto	75f90d3a	—	

脚本如下:

```

1 #coding:utf-8
2 import zipfile
3 import string
4 import binascii
5
6 def CrackCrc(crc):
7     for i in dic:
8         for j in dic:
9             for p in dic:
10                for q in dic:
11                    s = i + j + p + q
12                    if crc == (binascii.crc32(s) & 0xffffffff):
13                        #print s
14                        f.write(s)
15                        return
16
17 def CrackZip():
18     for I in range(68):
19         file = 'out' + str(I) + '.zip'
20         f = zipfile.ZipFile(file, 'r')
21         GetCrc = f.getinfo('data.txt')
22         crc = GetCrc.CRC
23         #以上3行为获取压缩包CRC32值的步骤
24         #print hex(crc)
25         CrackCrc(crc)
26
27 dic = string.ascii_letters + string.digits + '+/='
28
29 f = open('out.txt', 'w')
30 CrackZip()
31 f.close()

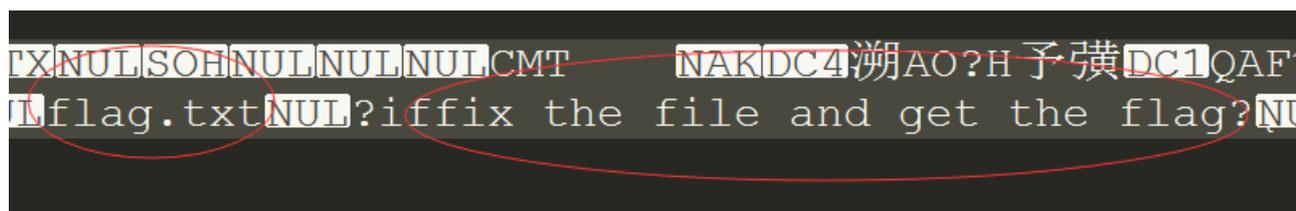
```

脚本运行时间较长

CRC32碰撞的原理请翻到[这篇文章](#)的0x06部分

步骤

根据碰撞出内容的格式（末尾两个==）推断这段数据是base64编码过的，先解码，根据解码结果中的flag.txt推断这可能是一个压缩包，同时根据*fix the file and get the flag*知需要修复文件



将解码后的文件导入16进制编辑器（如010editor），观察数据，发现存在rar的文件尾**C43D7B00400700**，但缺少文件头，于是补上rar的文件头**526172211A0700**。

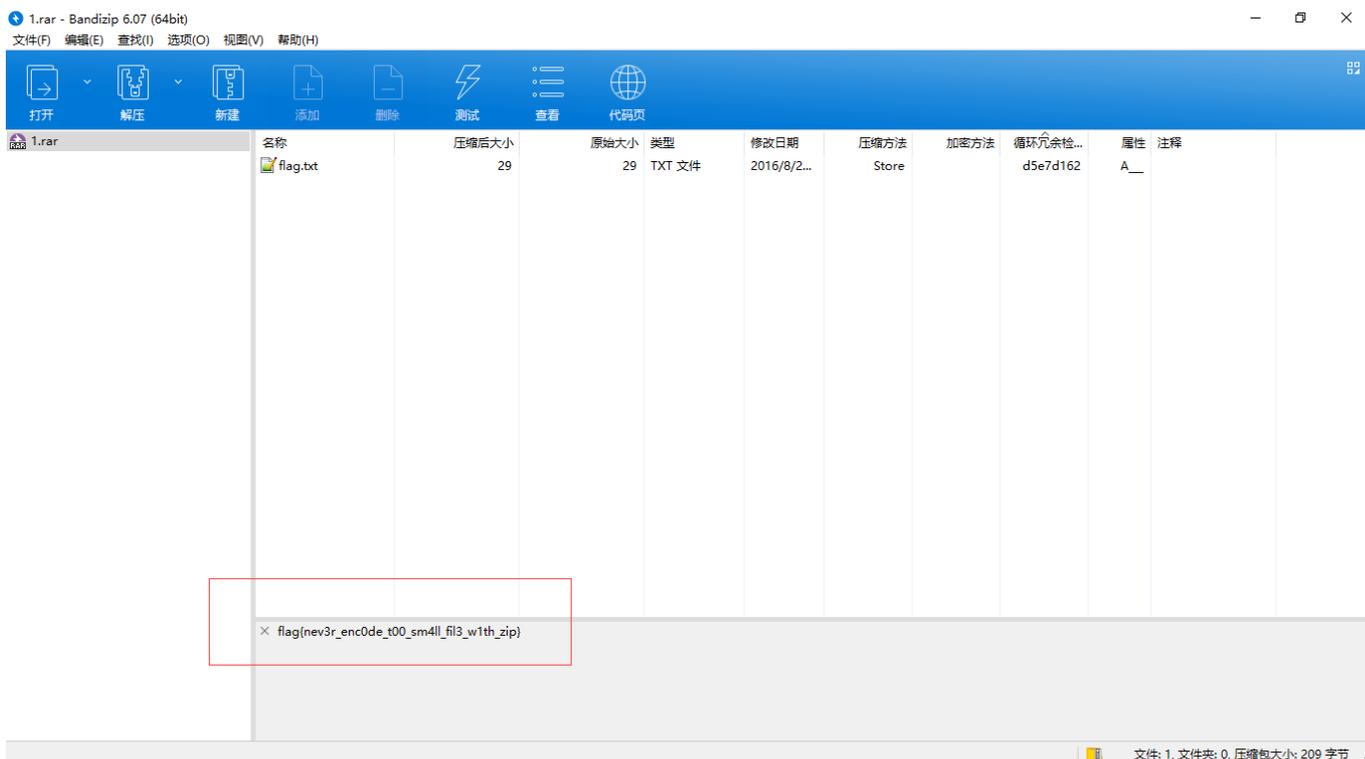
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	CF	90	73	00	00	0D	00	00	00	00	00	00	00	AA	3E	7A	I.s.....>z
0010h:	00	80	23	00	49	00	00	00	54	00	00	00	02	86	34	AB	.€#.I...T...+4«
0020h:	FE	6B	63	1D	49	1D	33	03	00	01	00	00	00	43	4D	54	bkc.I.3.....CMT
0030h:	09	15	14	CB	DD	41	4F	95	24	48	D3	E8	8F	98	45	11	...ÉYAO*\$HÓè.~E.
0040h:	51	41	46	F7	9F	1D	20	42	7C	6D	2B	B8	69	CA	9F	28	QAF=ÿ. B m+,iÊÿ(
0050h:	2C	33	28	FC	48	16	99	1F	1B	18	1D	8F	38	2C	46	76	,3(üH.™.....8,Fv
0060h:	E1	C5	ED	67	4D	72	DE	4D	4A	D5	82	74	BE	92	BD	1F	áÁigMrPMJÓ,t%’%.
0070h:	0A	94	CD	BE	AE	F7	3F	22	80	4A	F7	74	20	90	2D	00	.“í%@=?“€J=t .-
0080h:	1D	00	00	00	1D	00	00	00	02	62	D1	E7	D5	4F	63	1DbÑçÖOc.
0090h:	49	1D	30	08	00	20	00	00	00	66	6C	61	67	2E	74	78	I.0.. ...flag.tx
00A0h:	74	00	B0	34	69	66	66	69	78	20	74	68	65	20	66	69	t.°4ifix the fi
00B0h:	6C	65	20	61	6E	64	20	67	65	74	20	74	68	65	20	66	le and get the f
00C0h:	6C	61	67	C4	3D	7B	00	40	07	00							lagA={.@..

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar!...I.s.....
0010h:	00	00	00	00	AA	3E	7A	00	80	23	00	49	00	00	00	54>z.€#.I...T
0020h:	00	00	00	02	86	34	AB	FE	6B	63	1D	49	1D	33	03	00+4«pkc.I.3..
0030h:	01	00	00	00	43	4D	54	09	15	14	CB	DD	41	4F	95	24CMT...ÉYAO*\$
0040h:	48	D3	E8	8F	98	45	11	51	41	46	F7	9F	1D	20	42	7C	HÓè.~E.QAF=ÿ. B
0050h:	6D	2B	B8	69	CA	9F	28	2C	33	28	FC	48	16	99	1F	1B	m+,iÊÿ(,3(üH.™..
0060h:	18	1D	8F	38	2C	46	76	E1	C5	ED	67	4D	72	DE	4D	4A	...8,FváÁigMrPMJ
0070h:	D5	82	74	BE	92	BD	1F	0A	94	CD	BE	AE	F7	3F	22	80	Ó,t%’%.“í%@=?“€
0080h:	4A	F7	74	20	90	2D	00	1D	00	00	00	1D	00	00	00	02	J=t .-.....
0090h:	62	D1	E7	D5	4F	63	1D	49	1D	30	08	00	20	00	00	00	bÑçÖOc.I.0.. ...
00A0h:	66	6C	61	67	2E	74	78	74	00	B0	34	69	66	66	69	78	flag.txt.°4ifix
00B0h:	20	74	68	65	20	66	69	6C	65	20	61	6E	64	20	67	65	the file and ge
00C0h:	74	20	74	68	65	20	66	6C	61	67	(C4	3D)	7B	00	40	07	t the flagA={.@.
00D0h:	00																.

另存为rar格式，发现文件修复成功，解压后发现一个txt文档如下



文件已经修复但还没发现flag，仔细寻找，在注释里找到了flag



于是flag即为flag{nev3r_enc0de_t00sm4ll_fil3w1th_zip}

后来经大神提示，根据rar的文件结构可以看出还存在一个名为CMT的文件，CMT即为comment，即为注释

```
▼ Edit As: Hex ▾ Run Script ▾ Run Template: RAR.bt ▾
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 52 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00 Rar!...İ.s.....
0010h: 00 00 00 00 AA 3E 7A 00 80 23 00 49 00 00 00 54 ....>z.€#.I...T
0020h: 00 00 00 02 86 34 AB FE 6B 63 1D 49 1D 33 03 00 ....†4«pkc.I.3..
0030h: 01 00 00 00 43 4D 54 09 15 14 CB DD 41 4F 95 24 ....CMT...ÉYAO*$
0040h: 48 D3 E8 8F 98 45 11 51 41 46 F7 9F 1D 20 42 7C HÔè.~E.QAF÷ÿ. B|
0050h: 6D 2B B8 69 CA 9F 28 2C 33 28 FC 48 16 99 1F 1B m+,iÈÿ(,3(ùH.™..
0060h: 18 1D 8F 38 2C 46 76 E1 C5 (ED) 67 4D 72 DE 4D 4A ...8,FváÿigMrPMJ
0070h: D5 82 74 BE 92 BD 1F 0A 94 CD BE AE F7 3F 22 80 Ô,t%‘¼..”İ%÷?“€
0080h: 4A F7 74 20 90 2D 00 1D 00 00 00 1D 00 00 00 02 J÷t .-.....
0090h: 62 D1 E7 D5 4F 63 1D 49 1D 30 08 00 20 00 00 00 bÑçÔOc.I.O... ..
00A0h: 66 6C 61 67 2E 74 78 74 00 B0 34 69 66 66 69 78 flag.txt.°4ifix
00B0h: 20 74 68 65 20 66 69 6C 65 20 61 6E 64 20 67 65 the file and ge
00C0h: 74 20 74 68 65 20 66 6C 61 67 C4 3D 7B 00 40 07 t the flagÅ={.€
00D0h: 00 .
```

转载于:<https://www.cnblogs.com/WangAoBo/p/6951160.html>