

Bugku CTF 每日一题 where is flag

原创

彼岸花苏陌  于 2022-01-28 23:12:42 发布  735  收藏

分类专栏: [ctf](#) 文章标签: [ctf](#)

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/qq_42263820/article/details/122737676

版权



[ctf 专栏收录该内容](#)

39 篇文章 1 订阅

订阅专栏

where is flag 番外篇

解压得到两个压缩包 第一个压缩包key可以解压 第二个压缩包出师表要密码才能解压

打开第一个压缩包解压发现出师表中有些残缺, 比如

先帝创业未办AAAAA

而且下一段也接不上 而且有些有aaa啥的有些又没有，于是想到是不是凑字数？于是看了一下长度在这里发现了异常（用360解压不行，用的winrar）

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
p1.txt	353	278	文本文档	2021/5/26 15:...	E765FAA6
p2.txt	284	183	文本文档	2021/5/26 15:...	DF16CD...
p3.txt	315	194	文本文档	2021/5/26 15:...	54423241
p4.txt	238	180	文本文档	2021/5/26 15:...	08B0BAEA
p5.txt	331	241	文本文档	2021/5/26 15:...	D868AA...
p6.txt	351	247	文本文档	2021/5/26 15:...	E28185E6
p7.txt	316	199	文本文档	2021/5/26 16:...	56993A...
p8.txt	247	176	文本文档	2021/5/26 15:...	7E3B7621
p9.txt	246	170	文本文档	2021/5/26 15:...	9E9684FD
p10.txt	283	219	文本文档	2021/5/26 16:...	EDCF4B17
p11.txt	283	219	文本文档	2021/5/26 16:...	79DD398E
p12.txt	123	77	文本文档	2021/5/26 16:...	51196FC3
p13.txt	125	77	文本文档	2021/5/26 16:...	BD2AB7...

CSDN @彼岸花苏陌

前面的减去后面的

$$353-278=75$$

$$284-183=101$$

$$315-194=121$$

$$238-180=58$$

$$331-241=90$$

$$351-247=104$$

$$316-199=117$$

$$247-176=71$$

$$246-170=76$$

$$283-219=64$$

$$283-219=64$$

$$123-77=46$$

$$125-77=48$$

这些不就在ascii范围之间吗？

于是放进解码得到

Key:ZhuGL@@.0

得到密码

然后解压后放进winhex

搜索flag得到一段

272	57 A8 6F 62 2B 96 AB A4 32 0B 98 72 D8 0E A9 E5	W`ob+-«2 ~r0`@å
288	E8 8F E4 C8 72 8F B5 61 D6 5C 6E E2 86 0E 4A 59	è àÈr paÖ\nâ† JY
304	E5 84 D0 51 81 CD 14 6E D1 B3 AB 2A 7C 14 59 AA	å,,DQ í nÑ«* Yª
320	EA B0 51 D4 2F 46 54 8F 50 D3 77 AF AE 4B B8 49	è°QÔ/FT PÓw`@K,I
336	5E 39 F9 B6 BE F8 64 B7 9A BF 35 7F DB 70 6E 69	^9ùq³ød·š¿5 Ūpni
352	F8 6B 23 9A 66 A7 2F 6D 5B 06 9D DD FF 97 F3 11	øk#šfš/m[Ýÿ-ó
368	B6 5B BA E0 0A 01 08 40 00 02 10 78 73 02 AB 82	ŕ[°à @ xs «,
384	F9 D3 40 F5 8E F6 6B BA 20 20 66 6C 61 67 20 69	ùó@öžök° flag i
400	6E 20 68 65 72 65 20 7B 4C 6A 46 57 42 75 78 46	n here {LjFWBuxF
416	4E 54 7A 45 57 76 36 74 32 4E 66 78 6A 4E 46 53	NTzEWv6t2NfxjNFS
432	48 31 73 51 45 77 42 74 35 77 54 54 4C 44 31 66	HlsQEwBt5wTTLd1f
448	4A 7D 0A 11 8B 1D 1D 91 93 CB B7 AD 99 9A 40 CE	J} < ``È·-³š@î
464	D5 4B 3D 4B 5B 17 36 1C 2B 59 BA D4 C2 6A D4 BC	ÖK=K[6 +Y°ÔÅjÔ¼
480	1A C3 6A 6F 86 FD 5C 02 C4 96 9E CB 93 BB 41 00	Åjotý\ Ä-žÈ»A
496	02 10 80 C0 67 10 48 61 D4 8E 55 39 8A F1 4C A1	èÀg HaÔŽU9šñL;
512	67 B4 80 69 1C 5D 68 09 E5 30 52 5B 11 FB 74 04	g'èi]h å0R[út
528	50 4B A7 7B 64 38 0C 01 08 40 00 02 BB 13 F0 5A	PKš{d8 @ » öZ
544	20 FD 3C AD B7 A9 84 A4 96 86 C1 5E 4A 2A 29 D4	ý<-·@,,³-†Á^J*)Ô
560	E4 68 53 06 9F 2C B2 8A BD FB 20 70 E0 61 02 A8	ähš Ý,²š³:ú pàa ..
576	A5 87 51 51 11 02 10 80 00 04 20 10 04 B4 3A DB	¥±QQ e ' :Ū
592	BB BA 42 F9 38 43 62 48 29 04 54 2C 5A FA D2 5E	»°Bù8CbH) T, Zúò^
608	36 AD BF 76 40 C9 3A 29 D4 52 DF AF B2 49 EB 93	6-¿v@É:)ÔRš³-²Iè"

CSDN @彼岸花苏陌

感觉有点像base64，丢进去发现解不了密，于是又试试其他的base32 16 58 92等

最终在base58解密得到了正确答案

```
bugku{th1s_1s_chu_Sh1_B1A0!!@}
```

where is flag

同样的压缩包 打开发现前面有点大 但是后面只有几十，不构成组成flag的条件

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
1.txt	98,117	40	文本文档	2021/5/18 14:26	94C55FBC
2.txt	10,310	22	文本文档	2021/5/18 14:26	832CF907
3.txt	71,171	39	文本文档	2021/5/18 14:27	51F03001
4.txt	23,110	23	文本文档	2021/5/18 14:32	6E215A61
5.txt	9,748	22	文本文档	2021/5/18 14:28	73481FB2
6.txt	100,481	40	文本文档	2021/5/18 14:28	069A8249
7.txt	10,103	22	文本文档	2021/5/18 14:28	B4DEC49A
8.txt	10,097	22	文本文档	2021/5/18 14:29	2D9B1840
9.txt	10,797	22	文本文档	2021/5/18 14:29	515CA97D
10.txt	49,125	37	文本文档	2021/5/18 14:29	9B1F76B9

CSDN @彼岸花苏陌

但是看到第一个是98117 拆开不就是98 117吗？于是把前面组合一下 然后按ascii的范围一个个拆开

(范围尽量在32-127之间)

```
98-b  
117-u  
103-g  
107-k  
117-u  
123-  
110-n  
97-a  
48-  
100-d  
48-  
110-n  
103-g  
100-d  
97-a  
107-k  
97-a  
49-1  
125}
```

于是得到了flag

```
bugku{na0d0ngdaka1}
```