




CTF show crypto14

原创

[yu22x](#)  于 2020-02-25 14:59:55 发布  1988  收藏 7

文章标签: [python](#) [字符串](#) [java](#)

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/miuzzx/article/details/104495832>

版权

题目地址: <https://ctf.show>

我们直接将得到的二进制转成16进制，然后再转成字符串，得到了结果如下：3EP/3VNFFmNEAnIHD5dCMmVHD5ad9uG，第一反应便是base64解码，但是解码失败。我这里就不啰嗦我的各种失败解法了。

字符	值	字符	值	字符	值	字符	值
A	0	Q	16	g	32	w	48
B	1	R	17	h	33	x	49
C	2	S	18	i	34	y	50
D	3	T	19	j	35	z	51
E	4	U	20	k	36	0	52
F	5	V	21	l	37	1	53
G	6	W	22	m	38	2	54
H	7	X	23	n	39	3	55
I	8	Y	24	o	40	4	56
J	9	Z	25	p	41	5	57
K	10	a	26	q	42	6	58
L	11	b	27	r	43	7	59
M	12	c	28	s	44	8	60
N	13	d	29	t	45	9	61
O	14	e	30	u	46	+	62
P	15	f	31	v	47	/	63

附上一张base64编码表

"flag"使用base64加密后的字符串是 ZmxhZw== 前面的ZmxhZ不管flag后面是什么都不会改变。我们对比一下前四个字符，"Zmxh"和"3EP/"在base64表中查一下，Z和3差了30，m和E差了30。这下应该明白了吧。

当然一个一个找也可以，我这里给出个脚本，运行即可得正确的base64，解码得flag：

```
#author 羽
s = '3EP/3VNFFmNEAnIHD5dCMmVHD5ad9uG'
t = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
l=""
for i in s:
    l += t[(t.index(i)-30)%64]

if len(l)%4!=0:
    l=l+"*"*(4-(len(l)%4))
print(l)
```