CUIT CTF WriteUp-最简单的加解密

原创

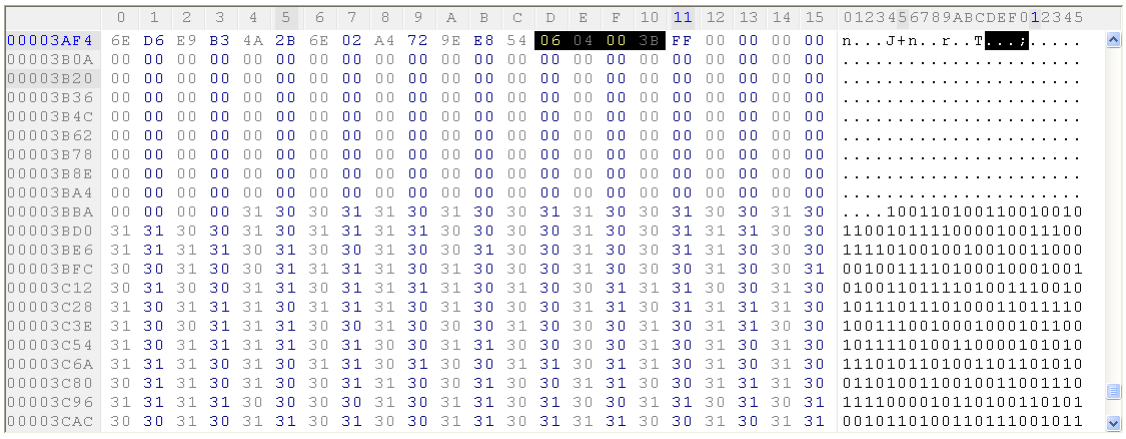
RickGray 于 2014-05-22 16:05:06 发布 4027 收藏 1
分类专栏： CTF纪实
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/u013565525/article/details/26597513
版权

CTF纪实 专栏收录该内容
10 篇文章 0 订阅
订阅专栏

首先Down下此题文件，发现是张二维码，扫描后，发现是个url地址（http://cli.im/9s7Nh）

进入该URL后，发现一张很打眼的图片

将该图片另存为保存到本地，直接用Hex Workshop打开，观察一番，发现了在gif的结尾标志后面藏了很长一串信息



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	0123456789ABCDEF012345
00003AF4	6E	D6	E9	B3	4A	2B	6E	02	A4	72	9E	E8	54	06	04	00	3B	FF	00	00	00	00	n...J+n..r..T...;.....
00003B0A	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003B20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003B36	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003B4C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003B62	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003B78	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003B8E	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003BA4	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00003BBA	00	00	00	00	31	30	30	31	31	30	31	30	30	31	31	30	30	31	30	30	31	30	....1001101001100100 10
00003BD0	31	31	30	30	31	30	31	31	31	31	30	30	30	30	31	30	30	31	31	31	30	30	1100101111000010011100
00003BE6	31	31	31	31	30	31	30	30	31	30	30	31	30	30	31	30	30	31	31	30	30	30	1111010010010010011000
00003BFC	30	30	31	30	30	31	31	31	31	30	31	30	30	30	31	30	30	30	31	30	30	31	0010011111010001000 1001
00003C12	30	31	30	30	31	31	30	31	31	31	31	30	31	30	30	31	31	31	30	30	31	30	0100110111101001110010
00003C28	31	30	31	31	31	30	31	31	31	30	31	30	30	30	31	31	30	31	31	31	31	30	1011101111010001101111 0
00003C3E	31	30	30	31	31	31	30	30	31	30	30	30	31	30	30	30	31	30	31	31	30	30	1001110010001000101100
00003C54	31	30	31	31	31	31	30	31	30	30	31	31	30	30	30	30	31	30	31	30	31	30	1011110100110000101010
00003C6A	31	31	31	30	31	30	31	31	30	31	30	30	31	31	30	31	31	30	31	30	31	30	1110101101001101101010
00003C80	30	31	31	30	31	30	30	31	31	30	30	31	30	30	31	31	30	30	31	31	31	30	0110100110010011001110
00003C96	31	31	31	31	30	30	30	30	31	30	31	31	30	31	30	30	31	31	30	31	30	31	1111000010110100110101
00003CAC	30	30	31	30	31	31	30	31	30	30	31	31	30	31	31	31	30	30	31	30	31	31	0010110100110111001011

数了一下，有两段10101字符串，分别为511bit和63bit，这个这个~~~~，这个结构直接想到了DES，但是都少了1bit，于是各种遍历补0逆序解DES，结果发现全是乱码~~~~（好坑！！）。

镇定下来后，想到了先对密文和密钥进行解码，各种尝试后，发现在前面补0时，转ascii时会显示出有用的信息

0101001101111001011000110110110000110000011101100011001101110010
-->Sycl0v3r

0100110100110010010110010111100001001110011110100100100100110000010011101000100010010100110111110100111001010111011101000110111101001110010001000101100101111010011000010101011101
-->M2YxNzl0ODJoNWtoNDYzaWZmM2gxZjZnZmY4MGc4OTM5ODAxOWtrNDlyaDVmODg0

拿去DES解密还是不对，然后又对密文进行Base64解码（长得像）

解出来是48bit的字符串，然后又根据提示有凯撒密码，又对其中的字母进行了凯撒解密（F-K）

得到最终的密文3a172482c5fc463daa3c1a6baa80b89398019ff422c5a884

拿去DES在线解密得到flag：*You_Got_It@_@*