

CUIT CTF WriteUp-Code100

原创

[RickGray](#) 于 2014-05-22 16:13:30 发布 878 收藏

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/26599009>

版权



[CTF纪实](#) 专栏收录该内容

10 篇文章 0 订阅

订阅专栏

首先吐槽一下: 题目设置有问题--

那么就挂个server接收连接呗, 还要手动输入60次!! 太坑!

还有就是, 我做这题时是直接Reverse, 如果是server端fread(flag)就不会出现这种奇葩事件, 望注意~!~!

分析过程就不说了, 程序运行弹了一串Base64编码的字符串, 解码出来是题目要求

```
Terminal - rick@RG: ~/Desktop
File Edit View Terminal Go Help
rick@RG:~/Desktop$ ./linux_calc_64bit
这是编程第一水题, 欢迎品尝
题目描述:
6L+Q6KGM56iL5bqP5LmL5ZC077yM56iL5bqP5Lya5bel5L2c5Zyo5Zyo0Tg3N+err+WPo+S4iu+8j0WQ
keiuv+mXruS7lueah0WuouS6uuWPkemAgeS4g0S6m+ihq0i+vuW8jwr0r7fkvaDorqHnrpfov5nkupvo
oajovr7lvI/nmoTlgLzjgILlubbku47moIf1h4bovpPlhaX1sIbov5nkupvlgLzovpPlhaX1iLDnqIvL
uo/kuk3vvIz1poLmnpzkvaDog73kv50K5oyBNjDova7nmoTmraPnoa7nu5PmnpzjgILpgqPkuYjmga3l
lpzkvaDjgIIK5r0o5oSP77yaCjEu5q+P5Liq6KGo6L6+5byP5pyJMjAwMOS4quw3puwPs+eahOaTjeS9
n0aVsAoyLuavj+S4quaVsOeah0Wkp+Wwj+iMg+WbtOWcqDIwNDA0MDMwNDDvVz4zMDQwNDAzMDQw5LmL
6Ze0CgrorqHnrpfmhInlv6vjgIICmJ5IFNZQy5mbHV5eSAgdHVsbmVlckBnYW1pbC5jb20K
```

(对应描述)

运行程序之后, 程序会工作在在9877端口上, 向访问他的客人发送一些表达式
请你计算这些表达式的值. 并从标准输入将这些值输入到程序中, 如果你能保持60轮的正确结果. 那么恭喜你.

注意:

1. 每个表达式有2000个左右的操作数
2. 每个数的大小范围在2040403040~3040403040之间

计算愉快.

by SYC .fluyy tulneer @gamil .com

多的不说了, 直接上脚本, 比较简单的一题- -! (Re)

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('localhost', 9877))

r = 1
while True:
    content = s.recv(65535)
    #print content
    nums = content.strip('\x00').split('+')
    #print nums
    sums = 0
    for i in nums:
        sums += int(i)
    print 'Round %d result: %d' % (r, sums)
    r += 1
```

经过60轮的蛋疼输入后，得到flag: **62b5C\6Aj7F 7Az6Aj**

4918184205273	Round 51 result: 4934033131424
4940033212658	Round 52 result: 4943149421600
4924690774359	Round 53 result: 4934949340796
4948596935211	Round 54 result: 4918184205273
4939002657577	Round 55 result: 4940033212658
4935916699960	Round 56 result: 4924690774359
4957182397152	Round 57 result: 4948596935211
KEY:62b5C\6Aj7F7Az6Aj	Round 58 result: 4939002657577
rick@RG:~/Desktop\$ a	Round 59 result: 4935916699960
	Round 60 result: 4957182397152