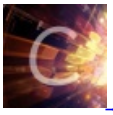
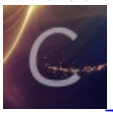
【CTF刷题之旅】XCTF嘉年华体验赛逆向题re1的writeup

原创

iqiqiya 于 2018-10-09 18:05:15 发布 1138 收藏 1
分类专栏： ------XCTF嘉年华体验赛 我的CTF之路 我的逆向之路 我的CTF进阶之路 文章标签： CTF刷题之旅 XCTF嘉年华体验赛逆向题re1的writeup re1的writeup 逆向题re1的最详细writeup
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/xiangshangbashaonian/article/details/82986322
版权


------XCTF嘉年华体验赛 同时被 3 个专栏收录
2 篇文章 0 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏


我的逆向之路
108 篇文章 10 订阅
订阅专栏

看了xctf训练平台

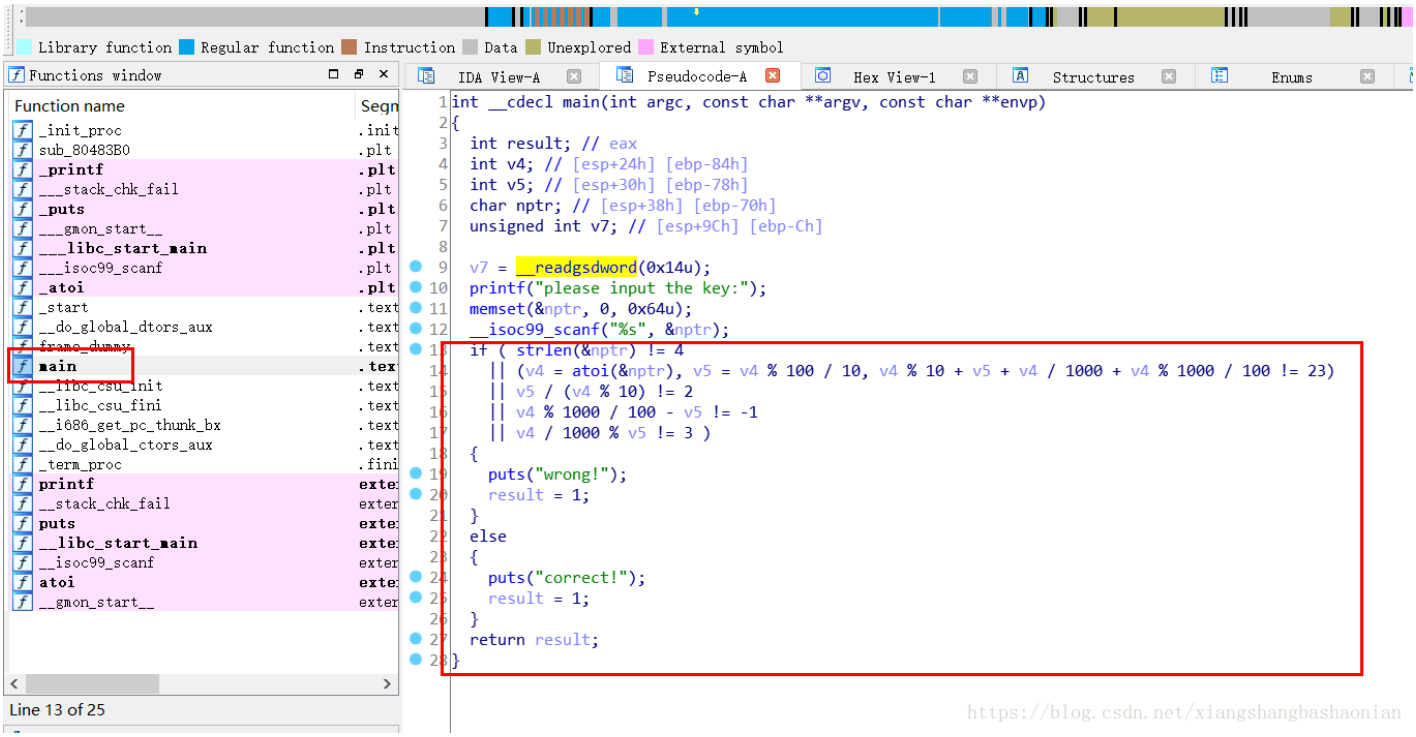
发现了这道题 可以用两种方法

最简单的就是用angr跑一下 过程不再列举(我试过了 可以成功)

具体方法可以看安装使用Angr符号执行来求解CTF逆向题

还有就是用脚本跑一下

载入IDA x32(虽然后缀是.ppp 但是一猜就知道elf 不知到位数 就先用32位IDA试一下呗)



可以看到程序就是获取我们的输入 nptr这个字符串　然后设定位数是4位

v4 = atoi(&nptr)　这个用到了atoi()这个函数　作用是把我们输入的字符串转成整型

事实上我们可以直接考虑输入的就是一个整型数据　那就不用管这个函数　而nptr也就可以直接写作v4

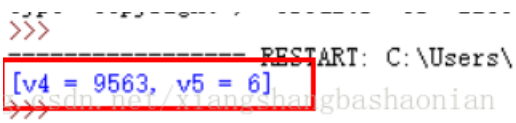
v5对100取余再对10取整 那么就相当于v4的十位上的数字

v4对10取余是个位 v4除以1000是千位 v4 % 1000 / 100就是百位

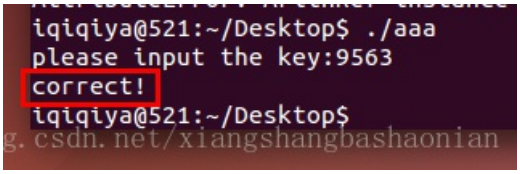
前段时间又学习了下z3(用来解方程的py库 具体可以看https://blog.csdn.net/xiangshangbashaonian/article/details/82788155)

代码如下：

```
from z3 import *
v4 = Int('v4')
v5 = Int('v5')
s = Solver()
s.add(v4 >= 1000)#这里我不知道长度怎样设置成四位　就直接这样子了
s.add(v4 <= 9999)
s.add(v5 == v4 % 100 / 10)#v5对100取余再对10取整　那么就相当于v4的十位上的数字
s.add(v4 % 10 + v5 + v4 / 1000 + v4 % 1000 / 100 == 23)#个位+十位+百位+千位等于23
s.add(v5 / (v4 % 10) == 2)#十位数字 / 个位 = 2
s.add(v4 % 1000 / 100 - v5 == -1)#剩下的自己分析吧 哈哈
s.add(v4 / 1000 % v5 == 3)#感觉用z3解有点大材小用
if s.check() != sat:
 print 'unsat'
else:
 m = s.model()
 print m
```



那么验证一下



g.csdn.net/xiangshangbashaonian

正确！