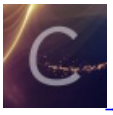
CTF挑战赛-合天网安实验室-Reverse逆向300writeup

原创

iqiqiya 于 2018-10-06 19:03:30 发布

分类专栏： 我的逆向之路 我的CTF之路 ------合天CTF 我的CTF进阶之路 文章标签： CTF挑战赛-合天网安实验室-Reverse逆向300wr 逆向300writeup CTF挑战赛-合天网安实验室-Reverse ELF

 我的逆向之路 同时被 3 个专栏收录

108 篇文章 10 订阅
订阅专栏

 我的CTF之路

92 篇文章 5 订阅
订阅专栏

 ------合天CTF

3 篇文章 0 订阅
订阅专栏

这个题目可以直接用angr来做 连分析都不用

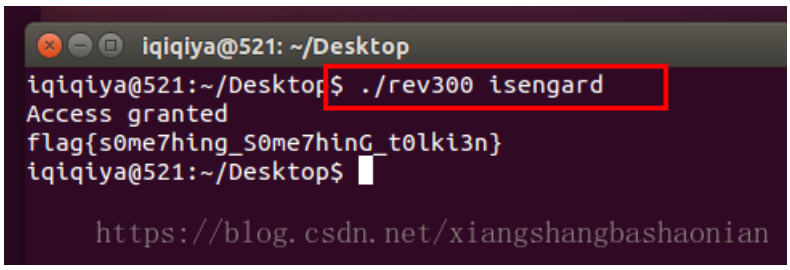
对angr不太了解的童鞋可以看这个安装使用Angr符号执行来求解CTF逆向题

找到如下图所示两个地址即可

```
.text:080485D7                call    sub_8048414
.text:080485DC                test    eax, eax
.text:080485DE                jz      short loc_80485FE
.text:080485E0                mov     dword ptr [esp], offset s ; "Access granted"
.text:080485E7                call    _puts
.text:080485EC                mov     eax, [ebp+arg_4]
.text:080485EF                add     eax, 4
.text:080485F2                mov     eax, [eax]
.text:080485F4                mov     [esp], eax
.text:080485F7                call    sub_8048538
.text:080485FC                jmp     short loc_804860A
.text:080485FE ; ---------------------------------------------------------------------------
.text:080485FE
.text:080485FE loc_80485FE:                           ; CODE XREF: main+D7j
.text:080485FE                                        ; main+29Tj
.text:080485FE                mov     dword ptr [esp], offset aAccessDenied ; "Access denied"
.text:08048605                call    _puts
.text:0804860A
.text:0804860A loc_804860A:                           ; CODE XREF: main+47Tj
.text:0804860A                mov     eax, 0
.text:0804860F                leave
.text:08048610                retn
.text:08048610 ; } // starts at 80485B5
```

```
In [1]: import angr
WARNING | 2018-10-06 05:04:30,383 | angr.analyses.disassembly_utils | Your version of capstone does not sup

In [2]: import claripy

In [3]: proj = angr.Project("./Desktop/rev300")
---------------------------------------------------------------------------
Exception                                 Traceback (most recent call last)
<ipython-input-3-e2682d5cb563> in <module>()
----> 1 proj = angr.Project("./Desktop/rev300")

/home/iqiqiya/.virtualenvs/angr/lib/python2.7/site-packages/angr/project.pyc in __init__(self, thing, defau
    120             self.loader = cle.Loader(thing, **load_options)
    121         elif not isinstance(thing, (unicode, str)) or not os.path.exists(thing) or not os.path.isfi
--> 122             raise Exception("Not a valid binary file: %s" % repr(thing))
    123         else:
    124             # use angr's loader, provided by cle

Exception: Not a valid binary file: './Desktop/rev300'

In [4]: proj = angr.Project("./rev300")#上边报错是因为路径  把文件放在/就好

In [5]: argv1 = claripy.BVS('argv1',50*8)#猜测最大输入不超过50个字节

In [6]: state = proj.factory.entry_state(args=['./rev300',argv1])

In [7]: simgr = proj.factory.simgr(state)

In [8]: simgr.explore(find=0x080485E0,avoid=0x080485FE)#输入正确以及错误的地址
Out[8]: <SimulationManager with 1 found, 8 avoid>

In [9]: print simgr.found[0].solver.eval(argv1)
106367276897217913128751644548146784277640522181918376277533300701623156663104270333417514929497791218630540

In [10]: print simgr.found[0].solver.eval(argv1,cast_to=str)#以字符串形式输出结果
Isengard  #得到的结果
```

验证得flag



常规解法可以看这个

https://blog.csdn.net/u012763794/article/details/78468581?locationNum=7&fps=1