BUUCTF [NPUCTF2020]芜湖

原创

皮皮蟹！ 于 2022-01-09 14:17:22 发布 2315 收藏
分类专栏： BUUCTF 文章标签： 安全

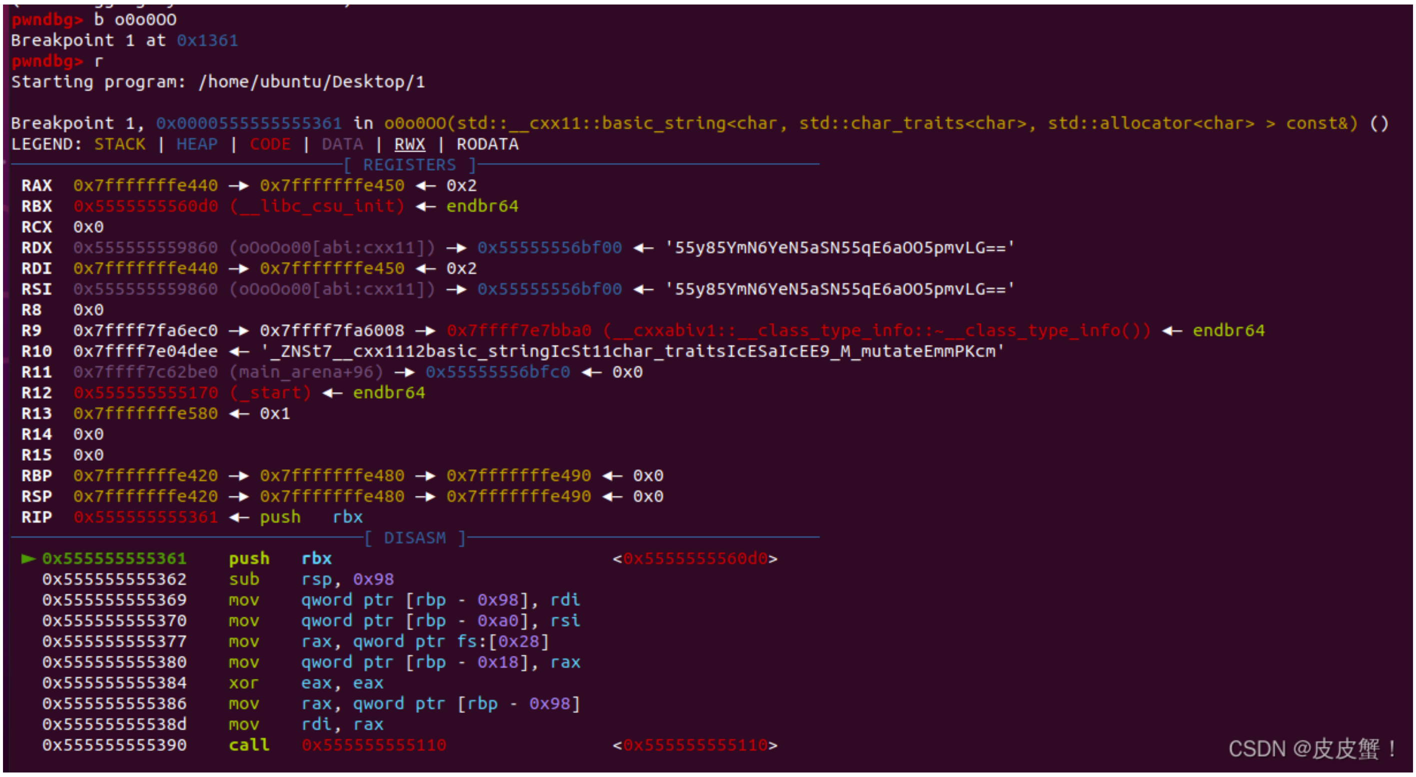
本文链接：https://blog.csdn.net/weixin_53349587/article/details/122392222
版权

BUUCTF 专栏收录该内容
20 篇文章 0 订阅
订阅专栏

这道题是一个base64隐写，我们要先提取出所有的base加密值，然后用base隐写提取的函数，把flag提取出来，就得到了flag。

1.提取base值

本来想着用ida动调一下，应该可以提出来，结果值在堆上面，ida动调只能看到一半的base值，一点用也没有，没办法，就用pwn的pwndbg查看堆：



```
pwndbg> b o0o0OO
Breakpoint 1 at 0x1361
pwndbg> r
Starting program: /home/ubuntu/Desktop/1

Breakpoint 1, 0x0000555555555361 in o0o0OO(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&) ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
─────────────────────────────────[ REGISTERS ]─────────────────────────────────
 RAX  0x7fffffffe440 → 0x7fffffffe450 ← 0x2
 RBX  0x5555555560d0 (__libc_csu_init) ← endbr64
 RCX  0x0
 RDX  0x555555559860 (o0o0o00[abi:cxx11]) → 0x55555556bf00 ← '55y85YmN6YeN5aSN55qE6a0O5pmvLG=='
 RDI  0x7fffffffe440 → 0x7fffffffe450 ← 0x2
 RSI  0x555555559860 (o0o0o00[abi:cxx11]) → 0x55555556bf00 ← '55y85YmN6YeN5aSN55qE6a0O5pmvLG=='
 R8   0x0
 R9   0x7ffff7fa6ec0 → 0x7ffff7fa6008 → 0x7ffff7e7bba0 (__cxxabiv1::__class_type_info::~__class_type_info()) ← endbr64
 R10  0x7ffff7e04dee ← '_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE9_M_mutateEmmPKcm'
 R11  0x7ffff7c62be0 (main_arena+96) → 0x55555556bfc0 ← 0x0
 R12  0x555555555170 (_start) ← endbr64
 R13  0x7fffffffe580 ← 0x1
 R14  0x0
 R15  0x0
 RBP  0x7fffffffe420 → 0x7fffffffe480 → 0x7fffffffe490 ← 0x0
 RSP  0x7fffffffe420 → 0x7fffffffe480 → 0x7fffffffe490 ← 0x0
 RIP  0x555555555361 ← push   rbx
──────────────────────────────────[ DISASM ]───────────────────────────────────
 ► 0x555555555361    push   rbx                           <0x5555555560d0>
   0x555555555362    sub    rsp, 0x98
   0x555555555369    mov    qword ptr [rbp - 0x98], rdi
   0x555555555370    mov    qword ptr [rbp - 0xa0], rsi
   0x555555555377    mov    rax, qword ptr fs:[0x28]
   0x555555555380    mov    qword ptr [rbp - 0x18], rax
   0x555555555384    xor    eax, eax
   0x555555555386    mov    rax, qword ptr [rbp - 0x98]
   0x55555555538d    mov    rdi, rax
   0x555555555390    call   0x555555555110                <0x555555555110>
```

CSDN @皮皮蟹！

接下来就一直单步s运行下去，一个一个把base值提取出来，得到最终的base值：

```
"55y85YmN6YeN5aSN55qE6aOO5pmvLG==",
"5riQ5riQ5qih57OK5LqG57qm5a6aLO==",
"5pif56m65LiL5rWB5rWq55qE5L2gLH==",
"5LuN54S256eY5a+G55qE6Led56a7LA==",
"5rip5bqm5raI5aSx55qE556s6Ze0LH==",
"5peg5rOV6Kem5pG455qE5piO5aSpLF==",
"5rKh5pyJ5byV5Yqb55qE5LiW55WMLG==",
"5rKh5pyJ6ISa5Y2w55qE5YWJ5bm0LD==",
"6L+Y5Zyo562J552A5L2g5Ye6546wLH==",
"5pel5pel5aSc5aSc6Ieq6L2s55qE6KGM5pifLE==",
"5Yiw5aSE6YGu5ruh5Yir5Lq655qE6IOM5b2xLG==",
"6K6p6aOO5ZC55pWj5re35Lmx55qE5ZG85ZC4LG==",
"5b+r5b+r5riF6YaSfn==",
"6Z2Z6Z2Z54Wn5Lqu5Y6f5p2l55qE6Ieq5bexLL==",
"5aSp56m65rSS5ruh5b+954S255qE5YWJ5piOLE==",
"55y85Lit5Y+q6KaB57ua54OC55qE5aSp6ZmFLG==",
"5YaN6aOe6KGMIW==",
"5oiR5YuH5pWi5Zyw5oqs6LW35aS0LM==",
"55yL552A6Iyr6Iyr55qE5a6H5a6ZLH==",
"5aSa5bCR5pyq55+l55qE5pif55CDLJ==",
"5pyJ5rKh5pyJ6YCa5ZCR5pyq5p2l6Lev5Y+jLD==",
"5Lqy54ix55qE5LyZ5Ly0LB==",
"6K6p5oiR5Lus5LiA6LW354K554eDLG==",
"5YuH5rCU5ZKM5L+h5b+1LO==",
"5Zyo6YGl6L+c55qE5aSp6L65LG==",
"6ZO25rKz6L6557yYLH==",
"5pyJ5LiA54mH56We5aWH55qE5b2p6Jm55rW3LC==",
"5ZKM5oiR5LiA6LW35YaS6ZmpLB==",
"6aOe5ZCR5Y+m5LiA5Liq5LiW55WMLC==",
"5Zyo6YGl6L+c55qE5aSp6L65LB==",
"6ZO25rKz6L6557yYLC==",
"5pyJ5LiA54mH56We5aWH55qE5b2p6Jm55rW3LB==",
"5ZKM5oiR5LiA6LW35YaS6ZmpLH==",
"6aOe5ZCR5Y+m5LiA5Liq5LiW55WMLN==",
"c3VwZXIgbWFnaWMgd29ybGR+fg=="
```

2.找一个base64隐写的脚本：

```
def base64_stego(lines):
    alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    flag = ''
    temp = 0
    digit = 0
    for i in lines:
        if i[-1] != '=':
            continue
        elif i[-2] != '=':
            digit += 2
            temp = (temp << 2) + (alphabet.find(i[-2]) & 0x3)
        else:
            digit += 4
            temp = (temp << 4) + (alphabet.find(i[-3]) & 0xf)
        if digit == 8:
            digit = 0
            flag += chr(temp)
            temp = 0
        elif digit > 8:
            digit = 2
            flag += chr(temp >> 2)
            temp = temp & 0x3
    return flag
```

写个python脚本：

```
def base64_stego(lines):
    alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    flag = ''
    temp = 0
    digit = 0
    for i in lines:
        if i[-1] != '=':
            continue
        elif i[-2] != '=':
            digit += 2
            temp = (temp << 2) + (alphabet.find(i[-2]) & 0x3)
        else:
            digit += 4
            temp = (temp << 4) + (alphabet.find(i[-3]) & 0xf)
        if digit == 8:
            digit = 0
            flag += chr(temp)
            temp = 0
        elif digit > 8:
            digit = 2
            flag += chr(temp >> 2)
            temp = temp & 0x3
    return flag
a = ["55y85YmN6YeN5aSN55qE6aOO5pmvLG==",
"5riQ5riQ5qih57OK5LqG57qm5a6aLO==",
"5pif56m65LiL5rWB5rWq55qE5L2gLH==",
"5LuN54S256eY5a+G55qE6Led56a7LA==",
"5rip5bqm5raI5aSx55qE556s6Ze0LH==",
"5peg5rOV6Kem5pG455qE5piO5aSpLF==",
"5rKh5pyJ5byV5Yqb55qE5LiW55WMLG==",
"5rKh5pyJ6ISa5Y2w55qE5YWJ5bm0LD==",
"6L+Y5Zyo562J552A5L2g5Ye6546wLH==",
"5pel5pel5aSc5aSc6Ieq6L2s55qE6KGM5pifLE==",
"5Yiw5aSE6YGu5ruh5Yir5Lq655qE6IOM5b2xLG==",
"6K6p6aOO5ZC55pWj5re35Lmx55qE5ZG85ZC4LG==",
"5b+r5b+r5riF6YaSfn==",
"6Z2Z6Z2Z54Wn5Lqu5Y6f5p2l55qE6Ieq5bexLL==",
"5aSp56m65rSS5ruh5b+954S255qE5YWJ5piOLE==",
"55y85Lit5Y+q6KaB57ua54OC55qE5aSp6ZmFLG==",
"5YaN6aOe6KGMIW==",
"5oiR5YuH5pWi5Zyw5oqs6LW35aS0LM==",
"55yL552A6Iyr6Iyr55qE5a6H5a6ZLH==",
"5aSa5bCR5pyq55+l55qE5pif55CDLJ==",
"5pyJ5rKh5pyJ6YCa5ZCR5pyq5p2l6Lev5Y+jLD==",
"5Lqy54ix55qE5LyZ5Ly0LB==",
"6K6p5oiR5Lus5LiA6LW354K554eDLG==",
"5YuH5rCU5ZKM5L+h5b+1LO==",
"5Zyo6YGl6L+c55qE5aSp6L65LG==",
"6ZO25rKz6L6557yYLH==",
"5pyJ5LiA54mH56We5aWH55qE5b2p6Jm55rW3LC==",
"5ZKM5oiR5LiA6LW35YaS6ZmpLB==",
"6aOe5ZCR5Y+m5LiA5Liq5LiW55WMLC==",
"5Zyo6YGl6L+c55qE5aSp6L65LB==",
"6ZO25rKz6L6557yYLC==",
"5pyJ5LiA54mH56We5aWH55qE5b2p6Jm55rW3LB==",
"5ZKM5oiR5LiA6LW35YaS6ZmpLH==",
"6aOe5ZCR5Y+m5LiA5Liq5LiW55WMLN==",
"c3VwZXIgbWFnaWMgd29ybGR+fg=="]
print(base64_stego(a))
#npuctf{Fly1ng!!!}
```

得到flag:

```
flag{Fly1ng!!!}
```