XCTF 2ex1

原创

夏了茶糜 于 2020-03-16 20:18:41 发布 297 收藏 1

分类专栏： CTF-REVERSE 文章标签： 安全

本文链接：https://blog.csdn.net/qin9800/article/details/104906558

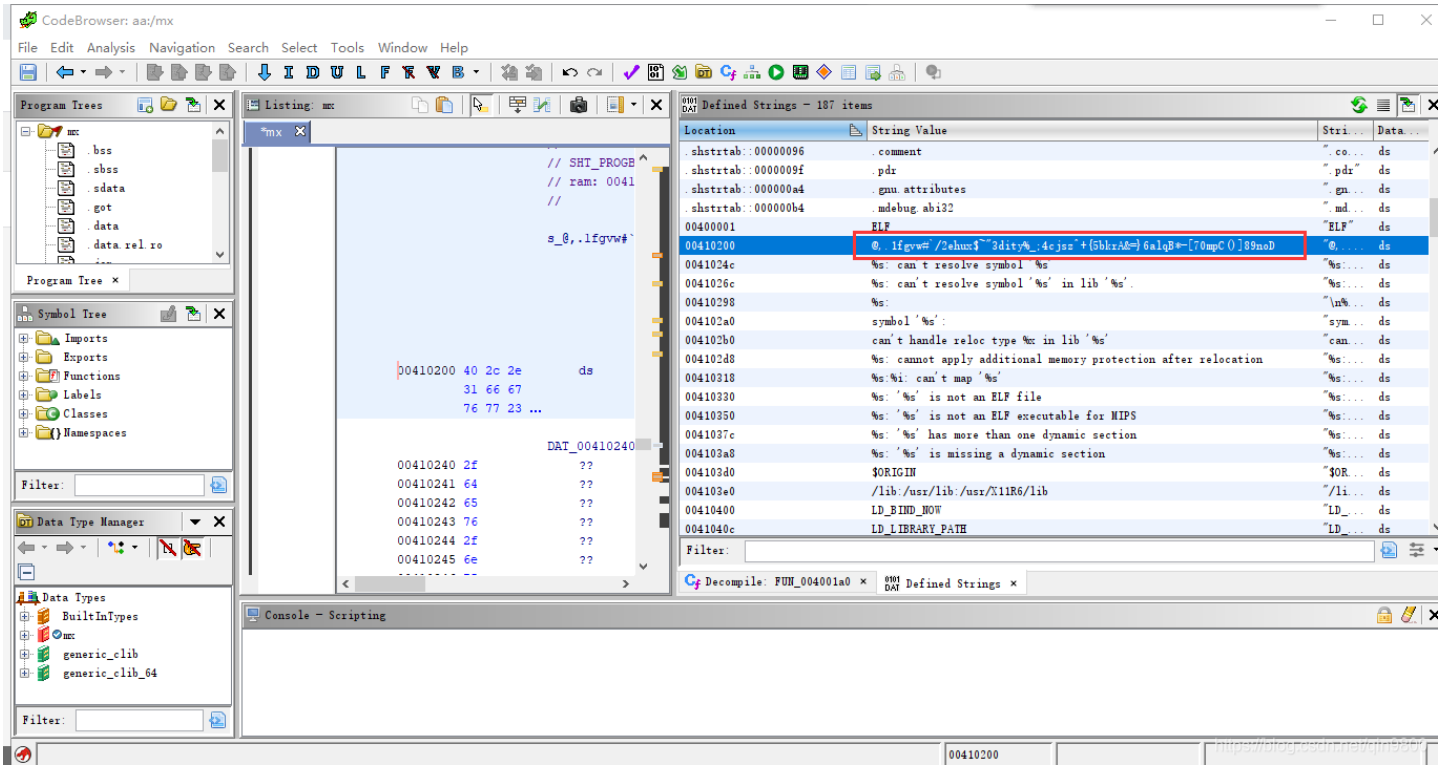
一个mips架构大端序的程序，还有一个密文

```
pwn@VirtualBox:~$ file mx
mx: ELF 32-bit MSB executable, MIPS, MIPS32 version 1 (SYSV), statically link
ed, stripped
pwn@VirtualBox:~$ cat out
|_r-+_Cl5;vgq_pdme7#7eC0=
pwn@VirtualBox:~$
```

运行下程序看看

```
pwn@VirtualBox:~$ qemu-mips mx
1111
e3f-e$@@@@@@$=]^@@@@@@@=
pwn@VirtualBox:~$ qemu-mips mx
2222
e5#[e^@@@@@@$=]^@@@@@@@=
pwn@VirtualBox:~$
```

一开始我没想出解题思路，看了大佬的wp，大佬一眼看出这是被替换了□表的base64加密
ghidra打开加解二进制文件



找到了一个足够64位的奇怪的字符串

```
@,.1fgvw#`/2ehux$~"3dity%_;4cjsz^+{5bkrA&=}6alqB*-[70mpC()]89noD
```

解密脚本

```
d = ""
ret = ""
string = "|_r-+_Cl5;vgq_pdme7#7eC0=".replace("=","")
base64_list = '@,.1fgvw#`/2ehux$~"3dity%_;4cjsz^+{5bkrA&=}6alqB*-[70mpC()]89noD'

for i in string:
 try:
  d += str(bin(base64_list.index(i))[2:]).rjust(6,"0")
 except Exception as e:
  continue
for i in range(0,len(d),8):
 if 32 <= int(d[i:i+8],2) <= 126:
  ret += chr(int(d[i:i+8],2))
print(ret)
```

flag

```
flag{change53233}
```