源 格式化 可变参数

str format

sscanf(p1 , p2, ...)

① eax > 1

⇒ 要读 2个及以上的 num!

② gdb → x/s 0x4025cf

num1 %d %d num2

放 空格 隔开.

③ num1 ≤ 7

④ 从num1 来到跳转下处的

0一下编号.

放 eax → 0x cf

至 0x2c3.

num1 不对 改的

num2 跳转后的

eax 同即可.

num1	num2
0	0x cf
1	0x 137
2	0x 2c3
3	0x 100
4	0x 185
5	0x ce
6	0x 200
7	0x 1ff

11:00 3月13日周四 VPN 32%

Vaults WSL-ACC WSL-ACC

```
0000000000400f43 <phase_3>:     input in %rdi
  400f43:  48 83 ec 18          sub    $0x18,%rsp 分配 16+8=24 bytes 的栈空间.
  400f47:  48 8d 4c 24 0c       lea    0xc(%rsp),%rcx      rcx = *(rsp+12)
  400f4c:  48 8d 54 24 08       lea    0x8(%rsp),%rdx      rdx = *(rsp+8)  num1
  400f51:  be cf 25 40 00       mov    $0x4025cf,%esi      esi = 0x4025cf
  400f56:  b8 00 00 00 00       mov    $0x0,%eax           eax = 0x 0
  400f5b:  e8 90 fc ff ff       call   400bf0 <__isoc99_sscanf@plt>  读取 input! 返回 eax 为参数
  400f60:  83 f8 01             cmp    $0x1,%eax                     sscanf.
  400f63:  7f 05                jg     400f6a <phase_3+0x27>
  400f65:  e8 d0 04 00 00       call   40143a <explode_bomb>
  400f6a:  83 7c 24 08 07       cmpl   $0x7,0x8(%rsp)
  400f6f:  77 3c                ja     400fad <phase_3+0x6a>
  400f71:  8b 44 24 08          mov    0x8(%rsp),%eax
  400f75:  ff 24 c5 70 24 40 00 jmp    *0x402470(,%rax,8)
  400f7c:  b8 cf 00 00 00       mov    $0xcf,%eax
  400f81:  eb 3b                jmp    400fbe <phase_3+0x7b>
  400f83:  b8 c3 02 00 00       mov    $0x2c3,%eax
  400f88:  eb 34                jmp    400fbe <phase_3+0x7b>
  400f8a:  b8 00 01 00 00       mov    $0x100,%eax
  400f8f:  eb 2d                jmp    400fbe <phase_3+0x7b>
  400f91:  b8 85 01 00 00       mov    $0x185,%eax
  400f96:  eb 26                jmp    400fbe <phase_3+0x7b>
  400f98:  b8 ce 00 00 00       mov    $0xce,%eax
  400f9d:  eb 1f                jmp    400fbe <phase_3+0x7b>
  400f9f:  b8 aa 02 00 00       mov    $0x2aa,%eax
  400fa4:  eb 18                jmp    400fbe <phase_3+0x7b>
  400fa6:  b8 47 01 00 00       mov    $0x147,%eax
  400fab:  eb 11                jmp    400fbe <phase_3+0x7b>
  400fad:  e8 88 04 00 00       call   40143a <explode_bomb>
  400fb2:  b8 00 00 00 00       mov    $0x0,%eax
  400fb7:  eb 05                jmp    400fbe <phase_3+0x7b>
  400fb9:  b8 37 01 00 00       mov    $0x137,%eax
  400fbe:  3b 44 24 0c          cmp    0xc(%rsp),%eax
  400fc2:  74 05                je     400fc9 <phase_3+0x86>
  400fc4:  e8 71 04 00 00       call   40143a <explode_bomb>
  400fc9:  48 83 c4 18          add    $0x18,%rsp
  400fcd:  c3                   ret
```

rdx = rsp+8 读取并存入

rcx = rsp+12

rsp → return address

if(eax > 1)

if(*(rsp+8) > 0x7)

eax = num2

0+num2*8 → 0x402470

bomb.

if(eax == num1)

{ ret }

Terminal appearance

Theme

Termius Dark

Termius Light

Kanagawa Wave

Kanagawa Dragon

Kanagawa Lotus

Hacker Blue

Hacker Green

Hacker Red