Phase_5

2020年4月28日 20:06

```
0000000000401062 <phase_5>:
  401062: 53                    push   %rbx
  401063: 48 83 ec 20           sub    $0x20,%rsp
  401067: 48 89 fb              mov    %rdi,%rbx
  40106a: 64 48 8b 04 25 28 00  mov    %fs:0x28,%rax
  401071: 00 00
  401073: 48 89 44 24 18        mov    %rax,0x18(%rsp)
  401078: 31 c0                 xor    %eax,%eax
  40107a: e8 9c 02 00 00        callq  40131b <string_length>
  40107f: 83 f8 06              cmp    $0x6,%eax
  401082: 74 4e                 je     4010d2 <phase_5+0x70>
  401084: e8 b1 03 00 00        callq  40143a <explode_bomb>
  401089: eb 47                 jmp    4010d2 <phase_5+0x70>
  40108b: 0f b6 0c 03           movzbl (%rbx,%rax,1),%ecx
  40108f: 88 0c 24              mov    %cl,(%rsp)
  401092: 48 8b 14 24           mov    (%rsp),%rdx
  401096: 83 e2 0f              and    $0xf,%edx
  401099: 0f b6 92 b0 24 40 00  movzbl 0x4024b0(%rdx),%edx
  4010a0: 88 54 04 10           mov    %dl,0x10(%rsp,%rax,1)
  4010a4: 48 83 c0 01           add    $0x1,%rax
  4010a8: 48 83 f8 06           cmp    $0x6,%rax
  4010ac: 75 dd                 jne    40108b <phase_5+0x29>
  4010ae: c6 44 24 16 00        movb   $0x0,0x16(%rsp)
  4010b3: be 5e 24 40 00        mov    $0x40245e,%esi
  4010b8: 48 8d 7c 24 10        lea    0x10(%rsp),%rdi
  4010bd: e8 76 02 00 00        callq  401338 <strings_not_equal>
  4010c2: 85 c0                 test   %eax,%eax
  4010c4: 74 13                 je     4010d9 <phase_5+0x77>
  4010c6: e8 6f 03 00 00        callq  40143a <explode_bomb>
  4010cb: 0f 1f 44 00 00        nopl   0x0(%rax,%rax,1)
  4010d0: eb 07                 jmp    4010d9 <phase_5+0x77>
  4010d2: b8 00 00 00 00        mov    $0x0,%eax
  4010d7: eb b2                 jmp    40108b <phase_5+0x29>
  4010d9: 48 8b 44 24 18        mov    0x18(%rsp),%rax
  4010de: 64 48 33 04 25 28 00  xor    %fs:0x28,%rax
  4010e5: 00 00
  4010e7: 74 05                 je     4010ee <phase_5+0x8c>
  4010e9: e8 42 fa ff ff        callq  400b30 <__stack_chk_fail@plt>
  4010ee: 48 83 c4 20           add    $0x20,%rsp
  4010f2: 5b                    pop    %rbx
  4010f3: c3                    retq
```

canary栈保护者

长度不为6就炸

比较wtf与0x40245e的字符串，相同就成

for循环，rax里是控制变量，初值为0，从某全局数组写入六个东西到栈上

```
Eax=0;
Loop:
    ecx=(input+rax);
    (rsp)=ecx&f;
    Rdx=(rsp);
    Rdx=rdx&0xf+0x4024b0;
    (rsp+10+rax)=rdx%32;
    Rax++;
    if(rax!=6)goto loop;
```

或曰：

```
char wtf[6]//in (rsp +10)
For(int i=0;i<6;++i)
    wtf[i]=Line[Input[i]&0xf];//input in rbx,line in 0x4024b0
```

最终翻译出的代码：

```
char line[] = "maduiersnfotvbylSo you think you can stop the bomb wit
h ctrl-c, do you?";//0x4024b0
char aaa[] = "flyers";//0x40245e
void phase_5(char input[]){
    if(strlen(input)!=5)
        explode();
    else{
        char wtf[6];//rsp+10
        for(int i=0;i<6;++i)//I in rax
            wtf[i]=line[input[i]&0xf];//input in rbx
        if(strcmp(wtf,aaa))
            explode();
    }
}
```

答案多样，字节ascii要求是 *9 *F *E *5 *6 *7,如若全部取3，则为9?>567