bomb: file format elf64-x86-64

Disassembly of section .init:

0000000000400ad0 <\_init>:

400ad0: 48 83 ec 08 sub $0x8,%rsp

400ad4: 48 8b 05 1d 35 20 00 mov 0x20351d(%rip),%rax # 603ff8 <\_DYNAMIC+0x1d0>

400adb: 48 85 c0 test %rax,%rax

400ade: 74 05 je 400ae5 <\_init+0x15>

400ae0: e8 0b 01 00 00 callq 400bf0 <\_\_gmon\_start\_\_@plt>

400ae5: 48 83 c4 08 add $0x8,%rsp

400ae9: c3 retq

Disassembly of section .plt:

0000000000400af0 <getenv@plt-0x10>:

400af0: ff 35 12 35 20 00 pushq 0x203512(%rip) # 604008 <\_GLOBAL\_OFFSET\_TABLE\_+0x8>

400af6: ff 25 14 35 20 00 jmpq \*0x203514(%rip) # 604010 <\_GLOBAL\_OFFSET\_TABLE\_+0x10>

400afc: 0f 1f 40 00 nopl 0x0(%rax)

0000000000400b00 <getenv@plt>:

400b00: ff 25 12 35 20 00 jmpq \*0x203512(%rip) # 604018 <\_GLOBAL\_OFFSET\_TABLE\_+0x18>

400b06: 68 00 00 00 00 pushq $0x0

400b0b: e9 e0 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400b10 <strcasecmp@plt>:

400b10: ff 25 0a 35 20 00 jmpq \*0x20350a(%rip) # 604020 <\_GLOBAL\_OFFSET\_TABLE\_+0x20>

400b16: 68 01 00 00 00 pushq $0x1

400b1b: e9 d0 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400b20 <\_\_errno\_location@plt>:

400b20: ff 25 02 35 20 00 jmpq \*0x203502(%rip) # 604028 <\_GLOBAL\_OFFSET\_TABLE\_+0x28>

400b26: 68 02 00 00 00 pushq $0x2

400b2b: e9 c0 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400b30 <strcpy@plt>:

400b30: ff 25 fa 34 20 00 jmpq \*0x2034fa(%rip) # 604030 <\_GLOBAL\_OFFSET\_TABLE\_+0x30>

400b36: 68 03 00 00 00 pushq $0x3

400b3b: e9 b0 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400b40 <puts@plt>:

400b40: ff 25 f2 34 20 00 jmpq \*0x2034f2(%rip) # 604038 <\_GLOBAL\_OFFSET\_TABLE\_+0x38>

400b46: 68 04 00 00 00 pushq $0x4

400b4b: e9 a0 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400b50 <write@plt>:

400b50: ff 25 ea 34 20 00 jmpq \*0x2034ea(%rip) # 604040 <\_GLOBAL\_OFFSET\_TABLE\_+0x40>

400b56: 68 05 00 00 00 pushq $0x5

400b5b: e9 90 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400b60 <printf@plt>:

400b60: ff 25 e2 34 20 00 jmpq \*0x2034e2(%rip) # 604048 <\_GLOBAL\_OFFSET\_TABLE\_+0x48>

400b66: 68 06 00 00 00 pushq $0x6

400b6b: e9 80 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400b70 <alarm@plt>:

400b70: ff 25 da 34 20 00 jmpq \*0x2034da(%rip) # 604050 <\_GLOBAL\_OFFSET\_TABLE\_+0x50>

400b76: 68 07 00 00 00 pushq $0x7

400b7b: e9 70 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400b80 <close@plt>:

400b80: ff 25 d2 34 20 00 jmpq \*0x2034d2(%rip) # 604058 <\_GLOBAL\_OFFSET\_TABLE\_+0x58>

400b86: 68 08 00 00 00 pushq $0x8

400b8b: e9 60 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400b90 <read@plt>:

400b90: ff 25 ca 34 20 00 jmpq \*0x2034ca(%rip) # 604060 <\_GLOBAL\_OFFSET\_TABLE\_+0x60>

400b96: 68 09 00 00 00 pushq $0x9

400b9b: e9 50 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400ba0 <\_\_libc\_start\_main@plt>:

400ba0: ff 25 c2 34 20 00 jmpq \*0x2034c2(%rip) # 604068 <\_GLOBAL\_OFFSET\_TABLE\_+0x68>

400ba6: 68 0a 00 00 00 pushq $0xa

400bab: e9 40 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400bb0 <fgets@plt>:

400bb0: ff 25 ba 34 20 00 jmpq \*0x2034ba(%rip) # 604070 <\_GLOBAL\_OFFSET\_TABLE\_+0x70>

400bb6: 68 0b 00 00 00 pushq $0xb

400bbb: e9 30 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400bc0 <signal@plt>:

400bc0: ff 25 b2 34 20 00 jmpq \*0x2034b2(%rip) # 604078 <\_GLOBAL\_OFFSET\_TABLE\_+0x78>

400bc6: 68 0c 00 00 00 pushq $0xc

400bcb: e9 20 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400bd0 <gethostbyname@plt>:

400bd0: ff 25 aa 34 20 00 jmpq \*0x2034aa(%rip) # 604080 <\_GLOBAL\_OFFSET\_TABLE\_+0x80>

400bd6: 68 0d 00 00 00 pushq $0xd

400bdb: e9 10 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400be0 <fprintf@plt>:

400be0: ff 25 a2 34 20 00 jmpq \*0x2034a2(%rip) # 604088 <\_GLOBAL\_OFFSET\_TABLE\_+0x88>

400be6: 68 0e 00 00 00 pushq $0xe

400beb: e9 00 ff ff ff jmpq 400af0 <\_init+0x20>

0000000000400bf0 <\_\_gmon\_start\_\_@plt>:

400bf0: ff 25 9a 34 20 00 jmpq \*0x20349a(%rip) # 604090 <\_GLOBAL\_OFFSET\_TABLE\_+0x90>

400bf6: 68 0f 00 00 00 pushq $0xf

400bfb: e9 f0 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400c00 <strtol@plt>:

400c00: ff 25 92 34 20 00 jmpq \*0x203492(%rip) # 604098 <\_GLOBAL\_OFFSET\_TABLE\_+0x98>

400c06: 68 10 00 00 00 pushq $0x10

400c0b: e9 e0 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400c10 <memcpy@plt>:

400c10: ff 25 8a 34 20 00 jmpq \*0x20348a(%rip) # 6040a0 <\_GLOBAL\_OFFSET\_TABLE\_+0xa0>

400c16: 68 11 00 00 00 pushq $0x11

400c1b: e9 d0 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400c20 <fflush@plt>:

400c20: ff 25 82 34 20 00 jmpq \*0x203482(%rip) # 6040a8 <\_GLOBAL\_OFFSET\_TABLE\_+0xa8>

400c26: 68 12 00 00 00 pushq $0x12

400c2b: e9 c0 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400c30 <\_\_isoc99\_sscanf@plt>:

400c30: ff 25 7a 34 20 00 jmpq \*0x20347a(%rip) # 6040b0 <\_GLOBAL\_OFFSET\_TABLE\_+0xb0>

400c36: 68 13 00 00 00 pushq $0x13

400c3b: e9 b0 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400c40 <bcopy@plt>:

400c40: ff 25 72 34 20 00 jmpq \*0x203472(%rip) # 6040b8 <\_GLOBAL\_OFFSET\_TABLE\_+0xb8>

400c46: 68 14 00 00 00 pushq $0x14

400c4b: e9 a0 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400c50 <fopen@plt>:

400c50: ff 25 6a 34 20 00 jmpq \*0x20346a(%rip) # 6040c0 <\_GLOBAL\_OFFSET\_TABLE\_+0xc0>

400c56: 68 15 00 00 00 pushq $0x15

400c5b: e9 90 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400c60 <gethostname@plt>:

400c60: ff 25 62 34 20 00 jmpq \*0x203462(%rip) # 6040c8 <\_GLOBAL\_OFFSET\_TABLE\_+0xc8>

400c66: 68 16 00 00 00 pushq $0x16

400c6b: e9 80 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400c70 <sprintf@plt>:

400c70: ff 25 5a 34 20 00 jmpq \*0x20345a(%rip) # 6040d0 <\_GLOBAL\_OFFSET\_TABLE\_+0xd0>

400c76: 68 17 00 00 00 pushq $0x17

400c7b: e9 70 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400c80 <exit@plt>:

400c80: ff 25 52 34 20 00 jmpq \*0x203452(%rip) # 6040d8 <\_GLOBAL\_OFFSET\_TABLE\_+0xd8>

400c86: 68 18 00 00 00 pushq $0x18

400c8b: e9 60 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400c90 <connect@plt>:

400c90: ff 25 4a 34 20 00 jmpq \*0x20344a(%rip) # 6040e0 <\_GLOBAL\_OFFSET\_TABLE\_+0xe0>

400c96: 68 19 00 00 00 pushq $0x19

400c9b: e9 50 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400ca0 <sleep@plt>:

400ca0: ff 25 42 34 20 00 jmpq \*0x203442(%rip) # 6040e8 <\_GLOBAL\_OFFSET\_TABLE\_+0xe8>

400ca6: 68 1a 00 00 00 pushq $0x1a

400cab: e9 40 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400cb0 <\_\_ctype\_b\_loc@plt>:

400cb0: ff 25 3a 34 20 00 jmpq \*0x20343a(%rip) # 6040f0 <\_GLOBAL\_OFFSET\_TABLE\_+0xf0>

400cb6: 68 1b 00 00 00 pushq $0x1b

400cbb: e9 30 fe ff ff jmpq 400af0 <\_init+0x20>

0000000000400cc0 <socket@plt>:

400cc0: ff 25 32 34 20 00 jmpq \*0x203432(%rip) # 6040f8 <\_GLOBAL\_OFFSET\_TABLE\_+0xf8>

400cc6: 68 1c 00 00 00 pushq $0x1c

400ccb: e9 20 fe ff ff jmpq 400af0 <\_init+0x20>

Disassembly of section .text:

0000000000400cd0 <\_start>:

400cd0: 31 ed xor %ebp,%ebp

400cd2: 49 89 d1 mov %rdx,%r9

400cd5: 5e pop %rsi

400cd6: 48 89 e2 mov %rsp,%rdx

400cd9: 48 83 e4 f0 and $0xfffffffffffffff0,%rsp

400cdd: 50 push %rax

400cde: 54 push %rsp

400cdf: 49 c7 c0 80 23 40 00 mov $0x402380,%r8

400ce6: 48 c7 c1 10 23 40 00 mov $0x402310,%rcx

400ced: 48 c7 c7 bd 0d 40 00 mov $0x400dbd,%rdi

400cf4: e8 a7 fe ff ff callq 400ba0 <\_\_libc\_start\_main@plt>

400cf9: f4 hlt

400cfa: 66 0f 1f 44 00 00 nopw 0x0(%rax,%rax,1)

0000000000400d00 <deregister\_tm\_clones>:

400d00: b8 87 47 60 00 mov $0x604787,%eax

400d05: 55 push %rbp

400d06: 48 2d 80 47 60 00 sub $0x604780,%rax

400d0c: 48 83 f8 0e cmp $0xe,%rax

400d10: 48 89 e5 mov %rsp,%rbp

400d13: 77 02 ja 400d17 <deregister\_tm\_clones+0x17>

400d15: 5d pop %rbp

400d16: c3 retq

400d17: b8 00 00 00 00 mov $0x0,%eax

400d1c: 48 85 c0 test %rax,%rax

400d1f: 74 f4 je 400d15 <deregister\_tm\_clones+0x15>

400d21: 5d pop %rbp

400d22: bf 80 47 60 00 mov $0x604780,%edi

400d27: ff e0 jmpq \*%rax

400d29: 0f 1f 80 00 00 00 00 nopl 0x0(%rax)

0000000000400d30 <register\_tm\_clones>:

400d30: b8 80 47 60 00 mov $0x604780,%eax

400d35: 55 push %rbp

400d36: 48 2d 80 47 60 00 sub $0x604780,%rax

400d3c: 48 c1 f8 03 sar $0x3,%rax

400d40: 48 89 e5 mov %rsp,%rbp

400d43: 48 89 c2 mov %rax,%rdx

400d46: 48 c1 ea 3f shr $0x3f,%rdx

400d4a: 48 01 d0 add %rdx,%rax

400d4d: 48 d1 f8 sar %rax

400d50: 75 02 jne 400d54 <register\_tm\_clones+0x24>

400d52: 5d pop %rbp

400d53: c3 retq

400d54: ba 00 00 00 00 mov $0x0,%edx

400d59: 48 85 d2 test %rdx,%rdx

400d5c: 74 f4 je 400d52 <register\_tm\_clones+0x22>

400d5e: 5d pop %rbp

400d5f: 48 89 c6 mov %rax,%rsi

400d62: bf 80 47 60 00 mov $0x604780,%edi

400d67: ff e2 jmpq \*%rdx

400d69: 0f 1f 80 00 00 00 00 nopl 0x0(%rax)

0000000000400d70 <\_\_do\_global\_dtors\_aux>:

400d70: 80 3d 21 3a 20 00 00 cmpb $0x0,0x203a21(%rip) # 604798 <completed.6355>

400d77: 75 11 jne 400d8a <\_\_do\_global\_dtors\_aux+0x1a>

400d79: 55 push %rbp

400d7a: 48 89 e5 mov %rsp,%rbp

400d7d: e8 7e ff ff ff callq 400d00 <deregister\_tm\_clones>

400d82: 5d pop %rbp

400d83: c6 05 0e 3a 20 00 01 movb $0x1,0x203a0e(%rip) # 604798 <completed.6355>

400d8a: f3 c3 repz retq

400d8c: 0f 1f 40 00 nopl 0x0(%rax)

0000000000400d90 <frame\_dummy>:

400d90: 48 83 3d 88 30 20 00 cmpq $0x0,0x203088(%rip) # 603e20 <\_\_JCR\_END\_\_>

400d97: 00

400d98: 74 1e je 400db8 <frame\_dummy+0x28>

400d9a: b8 00 00 00 00 mov $0x0,%eax

400d9f: 48 85 c0 test %rax,%rax

400da2: 74 14 je 400db8 <frame\_dummy+0x28>

400da4: 55 push %rbp

400da5: bf 20 3e 60 00 mov $0x603e20,%edi

400daa: 48 89 e5 mov %rsp,%rbp

400dad: ff d0 callq \*%rax

400daf: 5d pop %rbp

400db0: e9 7b ff ff ff jmpq 400d30 <register\_tm\_clones>

400db5: 0f 1f 00 nopl (%rax)

400db8: e9 73 ff ff ff jmpq 400d30 <register\_tm\_clones>

0000000000400dbd <main>:

400dbd: 53 push %rbx

400dbe: 83 ff 01 cmp $0x1,%edi

400dc1: 75 10 jne 400dd3 <main+0x16>

400dc3: 48 8b 05 be 39 20 00 mov 0x2039be(%rip),%rax # 604788 <stdin@@GLIBC\_2.2.5>

400dca: 48 89 05 cf 39 20 00 mov %rax,0x2039cf(%rip) # 6047a0 <infile>

400dd1: eb 59 jmp 400e2c <main+0x6f>

400dd3: 48 89 f3 mov %rsi,%rbx

400dd6: 83 ff 02 cmp $0x2,%edi

400dd9: 75 35 jne 400e10 <main+0x53>

400ddb: 48 8b 7e 08 mov 0x8(%rsi),%rdi

400ddf: be b0 23 40 00 mov $0x4023b0,%esi

400de4: e8 67 fe ff ff callq 400c50 <fopen@plt>

400de9: 48 89 05 b0 39 20 00 mov %rax,0x2039b0(%rip) # 6047a0 <infile>

400df0: 48 85 c0 test %rax,%rax

400df3: 75 37 jne 400e2c <main+0x6f>

400df5: 48 8b 53 08 mov 0x8(%rbx),%rdx

400df9: 48 8b 33 mov (%rbx),%rsi

400dfc: bf b2 23 40 00 mov $0x4023b2,%edi

400e01: e8 5a fd ff ff callq 400b60 <printf@plt>

400e06: bf 08 00 00 00 mov $0x8,%edi

400e0b: e8 70 fe ff ff callq 400c80 <exit@plt>

400e10: 48 8b 36 mov (%rsi),%rsi

400e13: bf cf 23 40 00 mov $0x4023cf,%edi

400e18: b8 00 00 00 00 mov $0x0,%eax

400e1d: e8 3e fd ff ff callq 400b60 <printf@plt>

400e22: bf 08 00 00 00 mov $0x8,%edi

400e27: e8 54 fe ff ff callq 400c80 <exit@plt>

400e2c: e8 26 05 00 00 callq 401357 <initialize\_bomb>

400e31: bf 38 24 40 00 mov $0x402438,%edi

400e36: e8 05 fd ff ff callq 400b40 <puts@plt>

400e3b: bf 78 24 40 00 mov $0x402478,%edi

400e40: e8 fb fc ff ff callq 400b40 <puts@plt>

400e45: e8 c7 07 00 00 callq 401611 <read\_line>

400e4a: 48 89 c7 mov %rax,%rdi

400e4d: e8 9e 00 00 00 callq 400ef0 <phase\_1>

400e52: e8 e0 08 00 00 callq 401737 <phase\_defused>

400e57: bf a8 24 40 00 mov $0x4024a8,%edi

400e5c: e8 df fc ff ff callq 400b40 <puts@plt>

400e61: e8 ab 07 00 00 callq 401611 <read\_line>

400e66: 48 89 c7 mov %rax,%rdi

400e69: e8 9e 00 00 00 callq 400f0c <phase\_2>

400e6e: e8 c4 08 00 00 callq 401737 <phase\_defused>

400e73: bf e9 23 40 00 mov $0x4023e9,%edi

400e78: e8 c3 fc ff ff callq 400b40 <puts@plt>

400e7d: e8 8f 07 00 00 callq 401611 <read\_line>

400e82: 48 89 c7 mov %rax,%rdi

400e85: e8 cd 00 00 00 callq 400f57 <phase\_3>

400e8a: e8 a8 08 00 00 callq 401737 <phase\_defused>

400e8f: bf 07 24 40 00 mov $0x402407,%edi

400e94: e8 a7 fc ff ff callq 400b40 <puts@plt>

400e99: e8 73 07 00 00 callq 401611 <read\_line>

400e9e: 48 89 c7 mov %rax,%rdi

400ea1: e8 7a 01 00 00 callq 401020 <phase\_4>

400ea6: e8 8c 08 00 00 callq 401737 <phase\_defused>

400eab: bf d8 24 40 00 mov $0x4024d8,%edi

400eb0: e8 8b fc ff ff callq 400b40 <puts@plt>

400eb5: e8 57 07 00 00 callq 401611 <read\_line>

400eba: 48 89 c7 mov %rax,%rdi

400ebd: e8 b5 01 00 00 callq 401077 <phase\_5>

400ec2: e8 70 08 00 00 callq 401737 <phase\_defused>

400ec7: bf 16 24 40 00 mov $0x402416,%edi

400ecc: e8 6f fc ff ff callq 400b40 <puts@plt>

400ed1: e8 3b 07 00 00 callq 401611 <read\_line>

400ed6: 48 89 c7 mov %rax,%rdi

400ed9: e8 da 01 00 00 callq 4010b8 <phase\_6>

400ede: e8 54 08 00 00 callq 401737 <phase\_defused>

400ee3: b8 00 00 00 00 mov $0x0,%eax

400ee8: 5b pop %rbx

400ee9: c3 retq

400eea: 66 0f 1f 44 00 00 nopw 0x0(%rax,%rax,1)

0000000000400ef0 <phase\_1>:

400ef0: 48 83 ec 08 sub $0x8,%rsp

400ef4: be 00 25 40 00 mov $0x402500,%esi

400ef9: e8 f0 03 00 00 callq 4012ee <strings\_not\_equal>

400efe: 85 c0 test %eax,%eax//Test: 与运算，不改变目的寄存器

400f00: 74 05 je 400f07 <phase\_1+0x17>//JE:jump if ZF=1

400f02: e8 92 06 00 00 callq 401599 <explode\_bomb>

400f07: 48 83 c4 08 add $0x8,%rsp

400f0b: c3 retq

0000000000400f0c <phase\_2>:

400f0c: 55 push %rbp

400f0d: 53 push %rbx

400f0e: 48 83 ec 28 sub $0x28,%rsp //%rsp = %rsp-40

400f12: 48 89 e6 mov %rsp,%rsi //%rsi = %rsp

400f15: e8 b5 06 00 00 callq 4015cf <read\_six\_numbers>

400f1a: 83 3c 24 00 cmpl $0x0,(%rsp)

400f1e: 79 24 jns 400f44 <phase\_2+0x38>

400f20: e8 74 06 00 00 callq 401599 <explode\_bomb>

400f25: eb 1d jmp 400f44 <phase\_2+0x38>

//循环体\_1

400f27: 89 d8 mov %ebx,%eax //%eax = %ebx

400f29: 03 45 fc add -0x4(%rbp),%eax //%eax = %eax + \*(%rbp-4)

400f2c: 39 45 00 cmp %eax,0x0(%rbp) //eax + a[i] == a[i+1]

400f2f: 74 05 je 400f36 <phase\_2+0x2a>

400f31: e8 63 06 00 00 callq 401599 <explode\_bomb>

//循环体\_2

400f36: 83 c3 01 add $0x1,%ebx //ebx += 1

400f39: 48 83 c5 04 add $0x4,%rbp //rbp += 4

//循环条件

400f3d: 83 fb 06 cmp $0x6,%ebx

400f40: 75 e5 jne 400f27 <phase\_2+0x1b>

400f42: eb 0c jmp 400f50 <phase\_2+0x44>

//初始化循环变量

400f44: 48 8d 6c 24 04 lea 0x4(%rsp),%rbp //%rbp = %rsp+4

400f49: bb 01 00 00 00 mov $0x1,%ebx //&ebx = 1

400f4e: eb d7 jmp 400f27 <phase\_2+0x1b>

400f50: 48 83 c4 28 add $0x28,%rsp

400f54: 5b pop %rbx

400f55: 5d pop %rbp

400f56: c3 retq

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| eax: | 1 | 2 | 3 | 4 | 5 | 6 |
| a[6] | 1 | 2 | 4 | 7 | 11 | 16 |

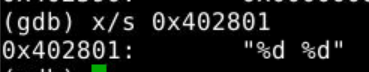
0000000000400f57 <phase\_3>:

400f57: 48 83 ec 18 sub $0x18,%rsp

400f5b: 48 8d 4c 24 08 lea 0x8(%rsp),%rcx

400f60: 48 8d 54 24 0c lea 0xc(%rsp),%rdx

400f65: be 01 28 40 00 mov $0x402801,%esi



400f6a: b8 00 00 00 00 mov $0x0,%eax

400f6f: e8 bc fc ff ff callq 400c30 <\_\_isoc99\_sscanf@plt>

400f74: 83 f8 01 cmp $0x1,%eax

400f77: 7f 05 jg 400f7e <phase\_3+0x27>

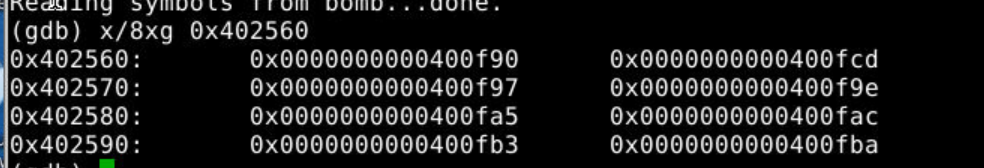
400f79: e8 1b 06 00 00 callq 401599 <explode\_bomb>

400f7e: 83 7c 24 0c 07 cmpl $0x7,0xc(%rsp) //第三个参数

400f83: 77 3c ja 400fc1 <phase\_3+0x6a>

400f85: 8b 44 24 0c mov 0xc(%rsp),%eax

400f89: ff 24 c5 60 25 40 00 jmpq \*0x402560(,%rax,8) //\*[基地址+8\*rax]



400f90: b8 18 03 00 00 mov $0x318,%eax

400f95: eb 3b jmp 400fd2 <phase\_3+0x7b>

400f97: b8 60 01 00 00 mov $0x160,%eax

400f9c: eb 34 jmp 400fd2 <phase\_3+0x7b>

400f9e: b8 ce 01 00 00 mov $0x1ce,%eax

400fa3: eb 2d jmp 400fd2 <phase\_3+0x7b>

400fa5: b8 f7 01 00 00 mov $0x1f7,%eax

400faa: eb 26 jmp 400fd2 <phase\_3+0x7b>

400fac: b8 39 02 00 00 mov $0x239,%eax

400fb1: eb 1f jmp 400fd2 <phase\_3+0x7b>

400fb3: b8 50 02 00 00 mov $0x250,%eax

400fb8: eb 18 jmp 400fd2 <phase\_3+0x7b>

400fba: b8 ce 01 00 00 mov $0x1ce,%eax

400fbf: eb 11 jmp 400fd2 <phase\_3+0x7b>

400fc1: e8 d3 05 00 00 callq 401599 <explode\_bomb>

400fc6: b8 00 00 00 00 mov $0x0,%eax

400fcb: eb 05 jmp 400fd2 <phase\_3+0x7b>

400fcd: b8 a1 01 00 00 mov $0x1a1,%eax

400fd2: 3b 44 24 08 cmp 0x8(%rsp),%eax //第四个参数与返回值相比较

400fd6: 74 05 je 400fdd <phase\_3+0x86>

400fd8: e8 bc 05 00 00 callq 401599 <explode\_bomb>

400fdd: 48 83 c4 18 add $0x18,%rsp

400fe1: c3 retq

0000000000400fe2 <func4>:

//（a,0,14） //(x,y,z)

//SAR是算数右移指令（shift arithmetic right），而SHR是逻辑右移指令

400fe2: 48 83 ec 08 sub $0x8,%rsp

400fe6: 89 d0 mov %edx,%eax //result = z

400fe8: 29 f0 sub %esi,%eax //result -= y

400fea: 89 c1 mov %eax,%ecx

400fec: c1 e9 1f shr $0x1f,%ecx //逻辑右移31位取符号位

400fef: 01 c8 add %ecx,%eax //result + {0,1}

400ff1: d1 f8 sar %eax //result /=2

400ff3: 8d 0c 30 lea (%rax,%rsi,1),%ecx //ecx = (z-y)/2+y = (z+y)/2

//func4(x,y,z-1)

400ff6: 39 f9 cmp %edi,%ecx // if (x< (z+y)/2)

400ff8: 7e 0c jle 401006 <func4+0x24>

400ffa: 8d 51 ff lea -0x1(%rcx),%edx //?

400ffd: e8 e0 ff ff ff callq 400fe2 <func4>

401002: 01 c0 add %eax,%eax //return 2\*func4

401004: eb 15 jmp 40101b <func4+0x39>

//func4(x,ecx+1,z)

401006: b8 00 00 00 00 mov $0x0,%eax

40100b: 39 f9 cmp %edi,%ecx

40100d: 7d 0c jge 40101b <func4+0x39>

40100f: 8d 71 01 lea 0x1(%rcx),%esi

401012: e8 cb ff ff ff callq 400fe2 <func4>

401017: 8d 44 00 01 lea 0x1(%rax,%rax,1),%eax //return 2\*func4+1

40101b: 48 83 c4 08 add $0x8,%rsp

40101f: c3 retq

0000000000401020 <phase\_4>:

//解析输入

401020: 48 83 ec 18 sub $0x18,%rsp

401024: 48 8d 4c 24 08 lea 0x8(%rsp),%rcx

401029: 48 8d 54 24 0c lea 0xc(%rsp),%rdx

40102e: be 01 28 40 00 mov $0x402801,%esi

401033: b8 00 00 00 00 mov $0x0,%eax

401038: e8 f3 fb ff ff callq 400c30 <\_\_isoc99\_sscanf@plt>

40103d: 83 f8 02 cmp $0x2,%eax

401040: 75 07 jne 401049 <phase\_4+0x29>

401042: 83 7c 24 0c 0e cmpl $0xe,0xc(%rsp) //第三个参数与14相比较

401047: 76 05 jbe 40104e <phase\_4+0x2e>

401049: e8 4b 05 00 00 callq 401599 <explode\_bomb>

//初始化参数，调用func4()

40104e: ba 0e 00 00 00 mov $0xe,%edx

401053: be 00 00 00 00 mov $0x0,%esi

401058: 8b 7c 24 0c mov 0xc(%rsp),%edi

40105c: e8 81 ff ff ff callq 400fe2 <func4> //func4(a，0，14) ；a=(rsp+4)

401061: 83 f8 06 cmp $0x6,%eax //func4() == 6

401064: 75 07 jne 40106d <phase\_4+0x4d>

401066: 83 7c 24 08 06 cmpl $0x6,0x8(%rsp) //第四个参数等于6

40106b: 74 05 je 401072 <phase\_4+0x52>

40106d: e8 27 05 00 00 callq 401599 <explode\_bomb>

401072: 48 83 c4 18 add $0x18,%rsp

401076: c3 retq

0000000000401077 <phase\_5>:

401077: 53 push %rbx

401078: 48 89 fb mov %rdi,%rbx

40107b: e8 51 02 00 00 callq 4012d1 <string\_length>

401080: 83 f8 06 cmp $0x6,%eax

401083: 74 05 je 40108a <phase\_5+0x13>

401085: e8 0f 05 00 00 callq 401599 <explode\_bomb>

//初始化变量

40108a: b8 00 00 00 00 mov $0x0,%eax

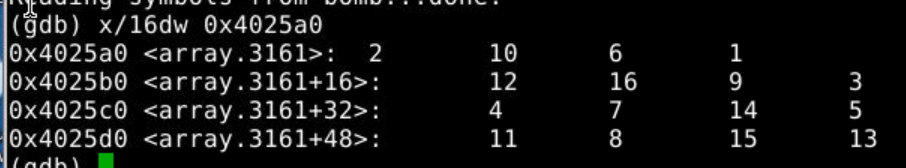
40108f: ba 00 00 00 00 mov $0x0,%edx

//循环体

401094: 0f b6 0c 03 movzbl (%rbx,%rax,1),%ecx //零扩展

401098: 83 e1 0f and $0xf,%ecx

40109b: 03 14 8d a0 25 40 00 add 0x4025a0(,%rcx,4),%edx



//循环变量

4010a2: 48 83 c0 01 add $0x1,%rax

//循环终止条件

4010a6: 48 83 f8 06 cmp $0x6,%rax

4010aa: 75 e8 jne 401094 <phase\_5+0x1d>

4010ac: 83 fa 2f cmp $0x2f,%edx //edx == 47

4010af: 74 05 je 4010b6 <phase\_5+0x3f>

4010b1: e8 e3 04 00 00 callq 401599 <explode\_bomb>

4010b6: 5b pop %rbx

4010b7: c3 retq

00000000004010b8 <phase\_6>:

4010b8: 41 56 push %r14

4010ba: 41 55 push %r13

4010bc: 41 54 push %r12

4010be: 55 push %rbp

4010bf: 53 push %rbx

4010c0: 48 83 ec 50 sub $0x50,%rsp

//read\_six\_numbers(rdi,rsi)

4010c4: 4c 8d 6c 24 30 lea 0x30(%rsp),%r13

4010c9: 4c 89 ee mov %r13,%rsi

4010cc: e8 fe 04 00 00 callq 4015cf <read\_six\_numbers>

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| rsp+48 | rsp+52 | rsp+56 | rsp+60 | rsp+64 | rsp+68 | rsp+72 |
| a[0] | a[1] | a[2] | a[3] | a[4] | a[5] |  |

4010d1: 4d 89 ee mov %r13,%r14

4010d4: 41 bc 00 00 00 00 mov $0x0,%r12d

//嵌套循环\_1

4010da: 4c 89 ed mov %r13,%rbp

4010dd: 41 8b 45 00 mov 0x0(%r13),%eax //eax = a[0]

4010e1: 83 e8 01 sub $0x1,%eax //eax - = 1

4010e4: 83 f8 05 cmp $0x5,%eax // eax<5 (a[0]<=6)

4010e7: 76 05 jbe 4010ee <phase\_6+0x36>

4010e9: e8 ab 04 00 00 callq 401599 <explode\_bomb>

//a[i]两两之间各不相同

//循环初始化

4010ee: 41 83 c4 01 add $0x1,%r12d //r12 += 1

4010f2: 41 83 fc 06 cmp $0x6,%r12d //r12 == 6

4010f6: 74 22 je 40111a <phase\_6+0x62>

4010f8: 44 89 e3 mov %r12d,%ebx

//循环体

4010fb: 48 63 c3 movslq %ebx,%rax //rax = r12

4010fe: 8b 44 84 30 mov 0x30(%rsp,%rax,4),%eax

401102: 39 45 00 cmp %eax,0x0(%rbp) //a[i]!=a[0] (i>=1)

401105: 75 05 jne 40110c <phase\_6+0x54>

401107: e8 8d 04 00 00 callq 401599 <explode\_bomb>

//循环变量与终止条件

40110c: 83 c3 01 add $0x1,%ebx //ebx+=1

40110f: 83 fb 05 cmp $0x5,%ebx

401112: 7e e7 jle 4010fb <phase\_6+0x43> //ebx <=5

401114: 49 83 c5 04 add $0x4,%r13 //r13 = a[i]

401118: eb c0 jmp 4010da <phase\_6+0x22>

//用7-a[i]替换所输入的数字

//循环初始化

40111a: 48 8d 74 24 48 lea 0x48(%rsp),%rsi

40111f: 4c 89 f0 mov %r14,%rax //rax = a[0]

401122: b9 07 00 00 00 mov $0x7,%ecx //ecx = 7

//循环体

401127: 89 ca mov %ecx,%edx

401129: 2b 10 sub (%rax),%edx //edx = 7-a[0]

40112b: 89 10 mov %edx,(%rax) //a[0] = edx

40112d: 48 83 c0 04 add $0x4,%rax //rax = a[1]

401131: 48 39 f0 cmp %rsi,%rax //rsi = rsp + 72

401134: 75 f1 jne 401127 <phase\_6+0x6f>

//使得数组按所输入数字从低往高排列

401136: be 00 00 00 00 mov $0x0,%esi

40113b: eb 20 jmp 40115d <phase\_6+0xa5>

40113d: 48 8b 52 08 mov 0x8(%rdx),%rdx

401141: 83 c0 01 add $0x1,%eax

401144: 39 c8 cmp %ecx,%eax

401146: 75 f5 jne 40113d <phase\_6+0x85>

401148: eb 05 jmp 40114f <phase\_6+0x97>

40114a: ba f0 42 60 00 mov $0x6042f0,%edx

40114f: 48 89 14 74 mov %rdx,(%rsp,%rsi,2) //\*(rsp + 2\*rsi) = rdx

//循环条件

401153: 48 83 c6 04 add $0x4,%rsi

401157: 48 83 fe 18 cmp $0x18,%rsi

//跳出循环

40115b: 74 15 je 401172 <phase\_6+0xba>

40115d: 8b 4c 34 30 mov 0x30(%rsp,%rsi,1),%ecx //ecx = a[0]

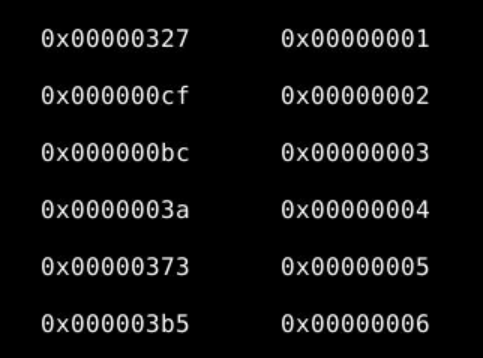
401161: 83 f9 01 cmp $0x1,%ecx

401164: 7e e4 jle 40114a <phase\_6+0x92> //a[i] <=1

401166: b8 01 00 00 00 mov $0x1,%eax

40116b: ba f0 42 60 00 mov $0x6042f0,%edx

401170: eb cb jmp 40113d <phase\_6+0x85>



//循环初始化

401172: 48 8b 1c 24 mov (%rsp),%rbx //b[0]

401176: 48 8d 44 24 08 lea 0x8(%rsp),%rax //&b[1]

40117b: 48 8d 74 24 30 lea 0x30(%rsp),%rsi //&a[0]

401180: 48 89 d9 mov %rbx,%rcx //b[0]

//循环体

401183: 48 8b 10 mov (%rax),%rdx //b[i+1]

401186: 48 89 51 08 mov %rdx,0x8(%rcx)

40118a: 48 83 c0 08 add $0x8,%rax

40118e: 48 39 f0 cmp %rsi,%rax

401191: 74 05 je 401198 <phase\_6+0xe0>

401193: 48 89 d1 mov %rdx,%rcx //b[i]

401196: eb eb jmp 401183 <phase\_6+0xcb>

//判断是否降序排列

401198: 48 c7 42 08 00 00 00 movq $0x0,0x8(%rdx)

40119f: 00

4011a0: bd 05 00 00 00 mov $0x5,%ebp

4011a5: 48 8b 43 08 mov 0x8(%rbx),%rax

4011a9: 8b 00 mov (%rax),%eax

4011ab: 39 03 cmp %eax,(%rbx) // b[i+1]< = b[i]

4011ad: 7d 05 jge 4011b4 <phase\_6+0xfc>

4011af: e8 e5 03 00 00 callq 401599 <explode\_bomb>

4011b4: 48 8b 5b 08 mov 0x8(%rbx),%rbx

4011b8: 83 ed 01 sub $0x1,%ebp

4011bb: 75 e8 jne 4011a5 <phase\_6+0xed>

4011bd: 48 83 c4 50 add $0x50,%rsp

4011c1: 5b pop %rbx

4011c2: 5d pop %rbp

4011c3: 41 5c pop %r12

4011c5: 41 5d pop %r13

4011c7: 41 5e pop %r14

4011c9: c3 retq

00000000004011ca <fun7>:

(0x604110,x)

4011ca: 48 83 ec 08 sub $0x8,%rsp

4011ce: 48 85 ff test %rdi,%rdi

4011d1: 74 2b je 4011fe <fun7+0x34>

4011d3: 8b 17 mov (%rdi),%edx

4011d5: 39 f2 cmp %esi,%edx

4011d7: 7e 0d jle 4011e6 <fun7+0x1c>

//edx>esi

4011d9: 48 8b 7f 08 mov 0x8(%rdi),%rdi

4011dd: e8 e8 ff ff ff callq 4011ca <fun7>

4011e2: 01 c0 add %eax,%eax

//return 2\*func(0x8(%rdi),x) 往左

4011e4: eb 1d jmp 401203 <fun7+0x39>

//edx<=esi

4011e6: b8 00 00 00 00 mov $0x0,%eax

//递归结束

4011eb: 39 f2 cmp %esi,%edx //if(edx==esi)

4011ed: 74 14 je 401203 <fun7+0x39>

4011ef: 48 8b 7f 10 mov 0x10(%rdi),%rdi

4011f3: e8 d2 ff ff ff callq 4011ca <fun7>

//return 2\*func(0x10(%rdi),x)+1 往右

4011f8: 8d 44 00 01 lea 0x1(%rax,%rax,1),%eax

4011fc: eb 05 jmp 401203 <fun7+0x39>

4011fe: b8 ff ff ff ff mov $0xffffffff,%eax

401203: 48 83 c4 08 add $0x8,%rsp

401207: c3 retq

0000000000401208 <secret\_phase>:

401208: 53 push %rbx

401209: e8 03 04 00 00 callq 401611 <read\_line>

40120e: ba 0a 00 00 00 mov $0xa,%edx //edx = 10

401213: be 00 00 00 00 mov $0x0,%esi //esi = 0

401218: 48 89 c7 mov %rax,%rdi //rdi = 输入

//strtol(x,0,10)

40121b: e8 e0 f9 ff ff callq 400c00 <strtol@plt>

401220: 48 89 c3 mov %rax,%rbx

401223: 8d 40 ff lea -0x1(%rax),%eax //eax = rax - 1

401226: 3d e8 03 00 00 cmp $0x3e8,%eax // eax<=0x3e8=1000

40122b: 76 05 jbe 401232 <secret\_phase+0x2a>

40122d: e8 67 03 00 00 callq 401599 <explode\_bomb>

401232: 89 de mov %ebx,%esi

401234: bf 10 41 60 00 mov $0x604110,%edi

//func7(0x604110,x)

401239: e8 8c ff ff ff callq 4011ca <fun7>

40123e: 83 f8 01 cmp $0x1,%eax //func7 == 1

401241: 74 05 je 401248 <secret\_phase+0x40>

401243: e8 51 03 00 00 callq 401599 <explode\_bomb>

401248: bf 38 25 40 00 mov $0x402538,%edi

40124d: e8 ee f8 ff ff callq 400b40 <puts@plt>

401252: e8 e0 04 00 00 callq 401737 <phase\_defused>

401257: 5b pop %rbx

401258: c3 retq

401259: 0f 1f 80 00 00 00 00 nopl 0x0(%rax)

0000000000401260 <sig\_handler>:

401260: 48 83 ec 08 sub $0x8,%rsp

401264: bf e0 25 40 00 mov $0x4025e0,%edi

401269: e8 d2 f8 ff ff callq 400b40 <puts@plt>

40126e: bf 03 00 00 00 mov $0x3,%edi

401273: e8 28 fa ff ff callq 400ca0 <sleep@plt>

401278: bf 71 27 40 00 mov $0x402771,%edi

40127d: b8 00 00 00 00 mov $0x0,%eax

401282: e8 d9 f8 ff ff callq 400b60 <printf@plt>

401287: 48 8b 3d f2 34 20 00 mov 0x2034f2(%rip),%rdi # 604780 <\_\_TMC\_END\_\_>

40128e: e8 8d f9 ff ff callq 400c20 <fflush@plt>

401293: bf 01 00 00 00 mov $0x1,%edi

401298: e8 03 fa ff ff callq 400ca0 <sleep@plt>

40129d: bf 79 27 40 00 mov $0x402779,%edi

4012a2: e8 99 f8 ff ff callq 400b40 <puts@plt>

4012a7: bf 10 00 00 00 mov $0x10,%edi

4012ac: e8 cf f9 ff ff callq 400c80 <exit@plt>

00000000004012b1 <invalid\_phase>:

4012b1: 48 83 ec 08 sub $0x8,%rsp

4012b5: 48 89 fe mov %rdi,%rsi

4012b8: bf 81 27 40 00 mov $0x402781,%edi

4012bd: b8 00 00 00 00 mov $0x0,%eax

4012c2: e8 99 f8 ff ff callq 400b60 <printf@plt>

4012c7: bf 08 00 00 00 mov $0x8,%edi

4012cc: e8 af f9 ff ff callq 400c80 <exit@plt>

00000000004012d1 <string\_length>:

4012d1: 80 3f 00 cmpb $0x0,(%rdi)

4012d4: 74 12 je 4012e8 <string\_length+0x17>

4012d6: 48 89 fa mov %rdi,%rdx

4012d9: 48 83 c2 01 add $0x1,%rdx

4012dd: 89 d0 mov %edx,%eax

4012df: 29 f8 sub %edi,%eax

4012e1: 80 3a 00 cmpb $0x0,(%rdx)

4012e4: 75 f3 jne 4012d9 <string\_length+0x8>

4012e6: f3 c3 repz retq

4012e8: b8 00 00 00 00 mov $0x0,%eax

4012ed: c3 retq

00000000004012ee <strings\_not\_equal>:

4012ee: 41 54 push %r12

4012f0: 55 push %rbp

4012f1: 53 push %rbx

4012f2: 48 89 fb mov %rdi,%rbx

4012f5: 48 89 f5 mov %rsi,%rbp

4012f8: e8 d4 ff ff ff callq 4012d1 <string\_length>

4012fd: 41 89 c4 mov %eax,%r12d

401300: 48 89 ef mov %rbp,%rdi

401303: e8 c9 ff ff ff callq 4012d1 <string\_length>

401308: ba 01 00 00 00 mov $0x1,%edx

40130d: 41 39 c4 cmp %eax,%r12d

401310: 75 3e jne 401350 <strings\_not\_equal+0x62>

401312: 0f b6 03 movzbl (%rbx),%eax

401315: 84 c0 test %al,%al

401317: 74 24 je 40133d <strings\_not\_equal+0x4f>

401319: 3a 45 00 cmp 0x0(%rbp),%al

40131c: 74 09 je 401327 <strings\_not\_equal+0x39>

40131e: 66 90 xchg %ax,%ax

401320: eb 22 jmp 401344 <strings\_not\_equal+0x56>

401322: 3a 45 00 cmp 0x0(%rbp),%al

401325: 75 24 jne 40134b <strings\_not\_equal+0x5d>

401327: 48 83 c3 01 add $0x1,%rbx

40132b: 48 83 c5 01 add $0x1,%rbp

40132f: 0f b6 03 movzbl (%rbx),%eax

401332: 84 c0 test %al,%al

401334: 75 ec jne 401322 <strings\_not\_equal+0x34>

401336: ba 00 00 00 00 mov $0x0,%edx

40133b: eb 13 jmp 401350 <strings\_not\_equal+0x62>

40133d: ba 00 00 00 00 mov $0x0,%edx

401342: eb 0c jmp 401350 <strings\_not\_equal+0x62>

401344: ba 01 00 00 00 mov $0x1,%edx

401349: eb 05 jmp 401350 <strings\_not\_equal+0x62>

40134b: ba 01 00 00 00 mov $0x1,%edx

401350: 89 d0 mov %edx,%eax

401352: 5b pop %rbx

401353: 5d pop %rbp

401354: 41 5c pop %r12

401356: c3 retq

0000000000401357 <initialize\_bomb>:

401357: 53 push %rbx

401358: 48 81 ec 40 20 00 00 sub $0x2040,%rsp

40135f: be 60 12 40 00 mov $0x401260,%esi

401364: bf 02 00 00 00 mov $0x2,%edi

401369: e8 52 f8 ff ff callq 400bc0 <signal@plt>

40136e: be 40 00 00 00 mov $0x40,%esi

401373: 48 8d bc 24 00 20 00 lea 0x2000(%rsp),%rdi

40137a: 00

40137b: e8 e0 f8 ff ff callq 400c60 <gethostname@plt>

401380: 85 c0 test %eax,%eax

401382: 75 13 jne 401397 <initialize\_bomb+0x40>

401384: 48 8b 3d f5 2f 20 00 mov 0x202ff5(%rip),%rdi # 604380 <host\_table>

40138b: bb 88 43 60 00 mov $0x604388,%ebx

401390: 48 85 ff test %rdi,%rdi

401393: 75 16 jne 4013ab <initialize\_bomb+0x54>

401395: eb 32 jmp 4013c9 <initialize\_bomb+0x72>

401397: bf 18 26 40 00 mov $0x402618,%edi

40139c: e8 9f f7 ff ff callq 400b40 <puts@plt>

4013a1: bf 08 00 00 00 mov $0x8,%edi

4013a6: e8 d5 f8 ff ff callq 400c80 <exit@plt>

4013ab: 48 8d b4 24 00 20 00 lea 0x2000(%rsp),%rsi

4013b2: 00

4013b3: e8 58 f7 ff ff callq 400b10 <strcasecmp@plt>

4013b8: 85 c0 test %eax,%eax

4013ba: 74 0d je 4013c9 <initialize\_bomb+0x72>

4013bc: 48 83 c3 08 add $0x8,%rbx

4013c0: 48 8b 7b f8 mov -0x8(%rbx),%rdi

4013c4: 48 85 ff test %rdi,%rdi

4013c7: 75 e2 jne 4013ab <initialize\_bomb+0x54>

4013c9: 48 89 e7 mov %rsp,%rdi

4013cc: e8 1d 0d 00 00 callq 4020ee <init\_driver>

4013d1: 85 c0 test %eax,%eax

4013d3: 79 1c jns 4013f1 <initialize\_bomb+0x9a>

4013d5: 48 89 e6 mov %rsp,%rsi

4013d8: bf 92 27 40 00 mov $0x402792,%edi

4013dd: b8 00 00 00 00 mov $0x0,%eax

4013e2: e8 79 f7 ff ff callq 400b60 <printf@plt>

4013e7: bf 08 00 00 00 mov $0x8,%edi

4013ec: e8 8f f8 ff ff callq 400c80 <exit@plt>

4013f1: 48 81 c4 40 20 00 00 add $0x2040,%rsp

4013f8: 5b pop %rbx

4013f9: c3 retq

00000000004013fa <initialize\_bomb\_solve>:

4013fa: f3 c3 repz retq

00000000004013fc <blank\_line>:

4013fc: 55 push %rbp

4013fd: 53 push %rbx

4013fe: 48 83 ec 08 sub $0x8,%rsp

401402: 48 89 fb mov %rdi,%rbx

401405: eb 17 jmp 40141e <blank\_line+0x22>

401407: e8 a4 f8 ff ff callq 400cb0 <\_\_ctype\_b\_loc@plt>

40140c: 48 83 c3 01 add $0x1,%rbx

401410: 48 0f be ed movsbq %bpl,%rbp

401414: 48 8b 00 mov (%rax),%rax

401417: f6 44 68 01 20 testb $0x20,0x1(%rax,%rbp,2)

40141c: 74 0f je 40142d <blank\_line+0x31>

40141e: 0f b6 2b movzbl (%rbx),%ebp

401421: 40 84 ed test %bpl,%bpl

401424: 75 e1 jne 401407 <blank\_line+0xb>

401426: b8 01 00 00 00 mov $0x1,%eax

40142b: eb 05 jmp 401432 <blank\_line+0x36>

40142d: b8 00 00 00 00 mov $0x0,%eax

401432: 48 83 c4 08 add $0x8,%rsp

401436: 5b pop %rbx

401437: 5d pop %rbp

401438: c3 retq

0000000000401439 <skip>:

401439: 53 push %rbx

40143a: 48 63 05 5b 33 20 00 movslq 0x20335b(%rip),%rax # 60479c <num\_input\_strings>

401441: 48 8d 3c 80 lea (%rax,%rax,4),%rdi

401445: 48 c1 e7 04 shl $0x4,%rdi

401449: 48 81 c7 c0 47 60 00 add $0x6047c0,%rdi

401450: 48 8b 15 49 33 20 00 mov 0x203349(%rip),%rdx # 6047a0 <infile>

401457: be 50 00 00 00 mov $0x50,%esi

40145c: e8 4f f7 ff ff callq 400bb0 <fgets@plt>

401461: 48 89 c3 mov %rax,%rbx

401464: 48 85 c0 test %rax,%rax

401467: 74 0c je 401475 <skip+0x3c>

401469: 48 89 c7 mov %rax,%rdi

40146c: e8 8b ff ff ff callq 4013fc <blank\_line>

401471: 85 c0 test %eax,%eax

401473: 75 c5 jne 40143a <skip+0x1>

401475: 48 89 d8 mov %rbx,%rax

401478: 5b pop %rbx

401479: c3 retq

000000000040147a <send\_msg>:

40147a: 53 push %rbx

40147b: 48 81 ec 20 40 00 00 sub $0x4020,%rsp

401482: 89 fb mov %edi,%ebx

401484: bf bd 27 40 00 mov $0x4027bd,%edi

401489: e8 72 f6 ff ff callq 400b00 <getenv@plt>

40148e: 48 89 c2 mov %rax,%rdx

401491: 48 b8 6e 6f 63 67 75 movabs $0x7265737567636f6e,%rax

401498: 73 65 72

40149b: 48 89 44 24 10 mov %rax,0x10(%rsp)

4014a0: 66 c7 44 24 18 69 64 movw $0x6469,0x18(%rsp)

4014a7: c6 44 24 1a 00 movb $0x0,0x1a(%rsp)

4014ac: 48 8d 44 24 10 lea 0x10(%rsp),%rax

4014b1: 48 85 d2 test %rdx,%rdx

4014b4: 48 0f 44 d0 cmove %rax,%rdx

4014b8: 44 8b 0d dd 32 20 00 mov 0x2032dd(%rip),%r9d # 60479c <num\_input\_strings>

4014bf: 41 8d 41 ff lea -0x1(%r9),%eax

4014c3: 48 98 cltq

4014c5: 4c 8d 14 80 lea (%rax,%rax,4),%r10

4014c9: 49 c1 e2 04 shl $0x4,%r10

4014cd: 49 81 c2 c0 47 60 00 add $0x6047c0,%r10

4014d4: 48 c7 c6 ff ff ff ff mov $0xffffffffffffffff,%rsi

4014db: 4c 89 d7 mov %r10,%rdi

4014de: b8 00 00 00 00 mov $0x0,%eax

4014e3: 48 89 f1 mov %rsi,%rcx

4014e6: f2 ae repnz scas %es:(%rdi),%al

4014e8: 48 f7 d1 not %rcx

4014eb: 49 89 cb mov %rcx,%r11

4014ee: 48 89 d7 mov %rdx,%rdi

4014f1: 48 89 f1 mov %rsi,%rcx

4014f4: f2 ae repnz scas %es:(%rdi),%al

4014f6: 48 89 ce mov %rcx,%rsi

4014f9: 48 f7 d6 not %rsi

4014fc: 49 8d 44 33 62 lea 0x62(%r11,%rsi,1),%rax

401501: 48 3d 00 20 00 00 cmp $0x2000,%rax

401507: 76 19 jbe 401522 <send\_msg+0xa8>

401509: bf 50 26 40 00 mov $0x402650,%edi

40150e: b8 00 00 00 00 mov $0x0,%eax

401513: e8 48 f6 ff ff callq 400b60 <printf@plt>

401518: bf 08 00 00 00 mov $0x8,%edi

40151d: e8 5e f7 ff ff callq 400c80 <exit@plt>

401522: 85 db test %ebx,%ebx

401524: b8 ac 27 40 00 mov $0x4027ac,%eax

401529: 41 b8 b4 27 40 00 mov $0x4027b4,%r8d

40152f: 4c 0f 45 c0 cmovne %rax,%r8

401533: 4c 89 14 24 mov %r10,(%rsp)

401537: 48 89 d1 mov %rdx,%rcx

40153a: 8b 15 34 2e 20 00 mov 0x202e34(%rip),%edx # 604374 <bomb\_id>

401540: be c6 27 40 00 mov $0x4027c6,%esi

401545: 48 8d bc 24 20 20 00 lea 0x2020(%rsp),%rdi

40154c: 00

40154d: b8 00 00 00 00 mov $0x0,%eax

401552: e8 19 f7 ff ff callq 400c70 <sprintf@plt>

401557: 4c 8d 44 24 20 lea 0x20(%rsp),%r8

40155c: b9 00 00 00 00 mov $0x0,%ecx

401561: 48 8d 94 24 20 20 00 lea 0x2020(%rsp),%rdx

401568: 00

401569: be 50 43 60 00 mov $0x604350,%esi

40156e: bf 65 43 60 00 mov $0x604365,%edi

401573: e8 14 0d 00 00 callq 40228c <driver\_post>

401578: 85 c0 test %eax,%eax

40157a: 79 14 jns 401590 <send\_msg+0x116>

40157c: 48 8d 7c 24 20 lea 0x20(%rsp),%rdi

401581: e8 ba f5 ff ff callq 400b40 <puts@plt>

401586: bf 00 00 00 00 mov $0x0,%edi

40158b: e8 f0 f6 ff ff callq 400c80 <exit@plt>

401590: 48 81 c4 20 40 00 00 add $0x4020,%rsp

401597: 5b pop %rbx

401598: c3 retq

0000000000401599 <explode\_bomb>:

401599: 48 83 ec 08 sub $0x8,%rsp

40159d: bf d5 27 40 00 mov $0x4027d5,%edi

4015a2: e8 99 f5 ff ff callq 400b40 <puts@plt>

4015a7: bf de 27 40 00 mov $0x4027de,%edi

4015ac: e8 8f f5 ff ff callq 400b40 <puts@plt>

4015b1: bf 00 00 00 00 mov $0x0,%edi

4015b6: e8 bf fe ff ff callq 40147a <send\_msg>

4015bb: bf 78 26 40 00 mov $0x402678,%edi

4015c0: e8 7b f5 ff ff callq 400b40 <puts@plt>

4015c5: bf 08 00 00 00 mov $0x8,%edi

4015ca: e8 b1 f6 ff ff callq 400c80 <exit@plt>

00000000004015cf <read\_six\_numbers>:

4015cf: 48 83 ec 18 sub $0x18,%rsp

4015d3: 48 89 f2 mov %rsi,%rdx

4015d6: 48 8d 4e 04 lea 0x4(%rsi),%rcx

4015da: 48 8d 46 14 lea 0x14(%rsi),%rax

4015de: 48 89 44 24 08 mov %rax,0x8(%rsp)

4015e3: 48 8d 46 10 lea 0x10(%rsi),%rax

4015e7: 48 89 04 24 mov %rax,(%rsp)

4015eb: 4c 8d 4e 0c lea 0xc(%rsi),%r9

4015ef: 4c 8d 46 08 lea 0x8(%rsi),%r8

4015f3: be f5 27 40 00 mov $0x4027f5,%esi

4015f8: b8 00 00 00 00 mov $0x0,%eax

4015fd: e8 2e f6 ff ff callq 400c30 <\_\_isoc99\_sscanf@plt>

401602: 83 f8 05 cmp $0x5,%eax

401605: 7f 05 jg 40160c <read\_six\_numbers+0x3d>

401607: e8 8d ff ff ff callq 401599 <explode\_bomb>

40160c: 48 83 c4 18 add $0x18,%rsp

401610: c3 retq

0000000000401611 <read\_line>:

401611: 48 83 ec 08 sub $0x8,%rsp

401615: b8 00 00 00 00 mov $0x0,%eax

40161a: e8 1a fe ff ff callq 401439 <skip>

40161f: 48 85 c0 test %rax,%rax

401622: 75 6e jne 401692 <read\_line+0x81>

401624: 48 8b 05 5d 31 20 00 mov 0x20315d(%rip),%rax # 604788 <stdin@@GLIBC\_2.2.5>

40162b: 48 39 05 6e 31 20 00 cmp %rax,0x20316e(%rip) # 6047a0 <infile>

401632: 75 14 jne 401648 <read\_line+0x37>

401634: bf 07 28 40 00 mov $0x402807,%edi

401639: e8 02 f5 ff ff callq 400b40 <puts@plt>

40163e: bf 08 00 00 00 mov $0x8,%edi

401643: e8 38 f6 ff ff callq 400c80 <exit@plt>

401648: bf 25 28 40 00 mov $0x402825,%edi

40164d: e8 ae f4 ff ff callq 400b00 <getenv@plt>

401652: 48 85 c0 test %rax,%rax

401655: 74 0a je 401661 <read\_line+0x50>

401657: bf 00 00 00 00 mov $0x0,%edi

40165c: e8 1f f6 ff ff callq 400c80 <exit@plt>

401661: 48 8b 05 20 31 20 00 mov 0x203120(%rip),%rax # 604788 <stdin@@GLIBC\_2.2.5>

401668: 48 89 05 31 31 20 00 mov %rax,0x203131(%rip) # 6047a0 <infile>

40166f: b8 00 00 00 00 mov $0x0,%eax

401674: e8 c0 fd ff ff callq 401439 <skip>

401679: 48 85 c0 test %rax,%rax

40167c: 75 14 jne 401692 <read\_line+0x81>

40167e: bf 07 28 40 00 mov $0x402807,%edi

401683: e8 b8 f4 ff ff callq 400b40 <puts@plt>

401688: bf 00 00 00 00 mov $0x0,%edi

40168d: e8 ee f5 ff ff callq 400c80 <exit@plt>

401692: 8b 15 04 31 20 00 mov 0x203104(%rip),%edx # 60479c <num\_input\_strings>

401698: 48 63 c2 movslq %edx,%rax

40169b: 48 8d 34 80 lea (%rax,%rax,4),%rsi

40169f: 48 c1 e6 04 shl $0x4,%rsi

4016a3: 48 81 c6 c0 47 60 00 add $0x6047c0,%rsi

4016aa: 48 89 f7 mov %rsi,%rdi

4016ad: b8 00 00 00 00 mov $0x0,%eax

4016b2: 48 c7 c1 ff ff ff ff mov $0xffffffffffffffff,%rcx

4016b9: f2 ae repnz scas %es:(%rdi),%al

4016bb: 48 f7 d1 not %rcx

4016be: 48 83 e9 01 sub $0x1,%rcx

4016c2: 83 f9 4e cmp $0x4e,%ecx

4016c5: 7e 46 jle 40170d <read\_line+0xfc>

4016c7: bf 30 28 40 00 mov $0x402830,%edi

4016cc: e8 6f f4 ff ff callq 400b40 <puts@plt>

4016d1: 8b 05 c5 30 20 00 mov 0x2030c5(%rip),%eax # 60479c <num\_input\_strings>

4016d7: 8d 50 01 lea 0x1(%rax),%edx

4016da: 89 15 bc 30 20 00 mov %edx,0x2030bc(%rip) # 60479c <num\_input\_strings>

4016e0: 48 98 cltq

4016e2: 48 6b c0 50 imul $0x50,%rax,%rax

4016e6: 48 bf 2a 2a 2a 74 72 movabs $0x636e7572742a2a2a,%rdi

4016ed: 75 6e 63

4016f0: 48 89 b8 c0 47 60 00 mov %rdi,0x6047c0(%rax)

4016f7: 48 bf 61 74 65 64 2a movabs $0x2a2a2a64657461,%rdi

4016fe: 2a 2a 00

401701: 48 89 b8 c8 47 60 00 mov %rdi,0x6047c8(%rax)

401708: e8 8c fe ff ff callq 401599 <explode\_bomb>

40170d: 83 e9 01 sub $0x1,%ecx

401710: 48 63 c9 movslq %ecx,%rcx

401713: 48 63 c2 movslq %edx,%rax

401716: 48 8d 04 80 lea (%rax,%rax,4),%rax

40171a: 48 c1 e0 04 shl $0x4,%rax

40171e: c6 84 01 c0 47 60 00 movb $0x0,0x6047c0(%rcx,%rax,1)

401725: 00

401726: 83 c2 01 add $0x1,%edx

401729: 89 15 6d 30 20 00 mov %edx,0x20306d(%rip) # 60479c <num\_input\_strings>

40172f: 48 89 f0 mov %rsi,%rax

401732: 48 83 c4 08 add $0x8,%rsp

401736: c3 retq

0000000000401737 <phase\_defused>:

401737: 48 83 ec 68 sub $0x68,%rsp

40173b: bf 01 00 00 00 mov $0x1,%edi

401740: e8 35 fd ff ff callq 40147a <send\_msg>

401745: 83 3d 50 30 20 00 06 cmpl $0x6,0x203050(%rip) # 60479c <num\_input\_strings>

40174c: 75 6d jne 4017bb <phase\_defused+0x84>

40174e: 4c 8d 44 24 10 lea 0x10(%rsp),%r8

401753: 48 8d 4c 24 08 lea 0x8(%rsp),%rcx

401758: 48 8d 54 24 0c lea 0xc(%rsp),%rdx

40175d: be 4b 28 40 00 mov $0x40284b,%esi

401762: bf b0 48 60 00 mov $0x6048b0,%edi

401767: b8 00 00 00 00 mov $0x0,%eax

40176c: e8 bf f4 ff ff callq 400c30 <\_\_isoc99\_sscanf@plt>

401771: 83 f8 03 cmp $0x3,%eax

401774: 75 31 jne 4017a7 <phase\_defused+0x70>

401776: be 54 28 40 00 mov $0x402854,%esi

40177b: 48 8d 7c 24 10 lea 0x10(%rsp),%rdi

401780: e8 69 fb ff ff callq 4012ee <strings\_not\_equal>

401785: 85 c0 test %eax,%eax

401787: 75 1e jne 4017a7 <phase\_defused+0x70>

401789: bf a0 26 40 00 mov $0x4026a0,%edi

40178e: e8 ad f3 ff ff callq 400b40 <puts@plt>

401793: bf c8 26 40 00 mov $0x4026c8,%edi

401798: e8 a3 f3 ff ff callq 400b40 <puts@plt>

40179d: b8 00 00 00 00 mov $0x0,%eax

4017a2: e8 61 fa ff ff callq 401208 <secret\_phase>

4017a7: bf 00 27 40 00 mov $0x402700,%edi

4017ac: e8 8f f3 ff ff callq 400b40 <puts@plt>

4017b1: bf 30 27 40 00 mov $0x402730,%edi

4017b6: e8 85 f3 ff ff callq 400b40 <puts@plt>

4017bb: 48 83 c4 68 add $0x68,%rsp

4017bf: c3 retq

00000000004017c0 <sigalrm\_handler>:

4017c0: 48 83 ec 08 sub $0x8,%rsp

4017c4: ba 00 00 00 00 mov $0x0,%edx

4017c9: be c8 28 40 00 mov $0x4028c8,%esi

4017ce: 48 8b 3d bb 2f 20 00 mov 0x202fbb(%rip),%rdi # 604790 <stderr@@GLIBC\_2.2.5>

4017d5: b8 00 00 00 00 mov $0x0,%eax

4017da: e8 01 f4 ff ff callq 400be0 <fprintf@plt>

4017df: bf 01 00 00 00 mov $0x1,%edi

4017e4: e8 97 f4 ff ff callq 400c80 <exit@plt>

00000000004017e9 <rio\_readlineb>:

4017e9: 41 57 push %r15

4017eb: 41 56 push %r14

4017ed: 41 55 push %r13

4017ef: 41 54 push %r12

4017f1: 55 push %rbp

4017f2: 53 push %rbx

4017f3: 48 83 ec 38 sub $0x38,%rsp

4017f7: 49 89 f6 mov %rsi,%r14

4017fa: 48 89 54 24 18 mov %rdx,0x18(%rsp)

4017ff: 48 83 fa 01 cmp $0x1,%rdx

401803: 0f 86 c2 00 00 00 jbe 4018cb <rio\_readlineb+0xe2>

401809: 48 89 fb mov %rdi,%rbx

40180c: 41 bd 01 00 00 00 mov $0x1,%r13d

401812: 4c 8d 67 10 lea 0x10(%rdi),%r12

401816: eb 2e jmp 401846 <rio\_readlineb+0x5d>

401818: ba 00 20 00 00 mov $0x2000,%edx

40181d: 4c 89 e6 mov %r12,%rsi

401820: 8b 3b mov (%rbx),%edi

401822: e8 69 f3 ff ff callq 400b90 <read@plt>

401827: 89 43 04 mov %eax,0x4(%rbx)

40182a: 85 c0 test %eax,%eax

40182c: 79 0f jns 40183d <rio\_readlineb+0x54>

40182e: e8 ed f2 ff ff callq 400b20 <\_\_errno\_location@plt>

401833: 83 38 04 cmpl $0x4,(%rax)

401836: 74 0e je 401846 <rio\_readlineb+0x5d>

401838: e9 9d 00 00 00 jmpq 4018da <rio\_readlineb+0xf1>

40183d: 85 c0 test %eax,%eax

40183f: 90 nop

401840: 74 6c je 4018ae <rio\_readlineb+0xc5>

401842: 4c 89 63 08 mov %r12,0x8(%rbx)

401846: 8b 6b 04 mov 0x4(%rbx),%ebp

401849: 85 ed test %ebp,%ebp

40184b: 7e cb jle 401818 <rio\_readlineb+0x2f>

40184d: 85 ed test %ebp,%ebp

40184f: 41 0f 95 c7 setne %r15b

401853: 41 0f b6 c7 movzbl %r15b,%eax

401857: 89 44 24 0c mov %eax,0xc(%rsp)

40185b: 45 0f b6 ff movzbl %r15b,%r15d

40185f: 48 8b 4b 08 mov 0x8(%rbx),%rcx

401863: 4c 89 fa mov %r15,%rdx

401866: 48 89 4c 24 10 mov %rcx,0x10(%rsp)

40186b: 48 89 ce mov %rcx,%rsi

40186e: 48 8d 7c 24 2f lea 0x2f(%rsp),%rdi

401873: e8 98 f3 ff ff callq 400c10 <memcpy@plt>

401878: 4c 03 7c 24 10 add 0x10(%rsp),%r15

40187d: 4c 89 7b 08 mov %r15,0x8(%rbx)

401881: 8b 44 24 0c mov 0xc(%rsp),%eax

401885: 29 c5 sub %eax,%ebp

401887: 89 6b 04 mov %ebp,0x4(%rbx)

40188a: 83 f8 01 cmp $0x1,%eax

40188d: 75 13 jne 4018a2 <rio\_readlineb+0xb9>

40188f: 49 83 c6 01 add $0x1,%r14

401893: 0f b6 44 24 2f movzbl 0x2f(%rsp),%eax

401898: 41 88 46 ff mov %al,-0x1(%r14)

40189c: 3c 0a cmp $0xa,%al

40189e: 75 18 jne 4018b8 <rio\_readlineb+0xcf>

4018a0: eb 2f jmp 4018d1 <rio\_readlineb+0xe8>

4018a2: 83 7c 24 0c 00 cmpl $0x0,0xc(%rsp)

4018a7: 75 3a jne 4018e3 <rio\_readlineb+0xfa>

4018a9: 44 89 e8 mov %r13d,%eax

4018ac: eb 03 jmp 4018b1 <rio\_readlineb+0xc8>

4018ae: 44 89 e8 mov %r13d,%eax

4018b1: 83 f8 01 cmp $0x1,%eax

4018b4: 75 1b jne 4018d1 <rio\_readlineb+0xe8>

4018b6: eb 34 jmp 4018ec <rio\_readlineb+0x103>

4018b8: 41 83 c5 01 add $0x1,%r13d

4018bc: 49 63 c5 movslq %r13d,%rax

4018bf: 48 3b 44 24 18 cmp 0x18(%rsp),%rax

4018c4: 73 0b jae 4018d1 <rio\_readlineb+0xe8>

4018c6: e9 7b ff ff ff jmpq 401846 <rio\_readlineb+0x5d>

4018cb: 41 bd 01 00 00 00 mov $0x1,%r13d

4018d1: 41 c6 06 00 movb $0x0,(%r14)

4018d5: 49 63 c5 movslq %r13d,%rax

4018d8: eb 17 jmp 4018f1 <rio\_readlineb+0x108>

4018da: 48 c7 c0 ff ff ff ff mov $0xffffffffffffffff,%rax

4018e1: eb 0e jmp 4018f1 <rio\_readlineb+0x108>

4018e3: 48 c7 c0 ff ff ff ff mov $0xffffffffffffffff,%rax

4018ea: eb 05 jmp 4018f1 <rio\_readlineb+0x108>

4018ec: b8 00 00 00 00 mov $0x0,%eax

4018f1: 48 83 c4 38 add $0x38,%rsp

4018f5: 5b pop %rbx

4018f6: 5d pop %rbp

4018f7: 41 5c pop %r12

4018f9: 41 5d pop %r13

4018fb: 41 5e pop %r14

4018fd: 41 5f pop %r15

4018ff: c3 retq

0000000000401900 <submitr>:

401900: 41 57 push %r15

401902: 41 56 push %r14

401904: 41 55 push %r13

401906: 41 54 push %r12

401908: 55 push %rbp

401909: 53 push %rbx

40190a: 48 81 ec 68 a0 00 00 sub $0xa068,%rsp

401911: 48 89 fd mov %rdi,%rbp

401914: 41 89 f5 mov %esi,%r13d

401917: 48 89 54 24 08 mov %rdx,0x8(%rsp)

40191c: 48 89 4c 24 10 mov %rcx,0x10(%rsp)

401921: 4c 89 44 24 18 mov %r8,0x18(%rsp)

401926: 4d 89 cf mov %r9,%r15

401929: 48 8b 9c 24 a0 a0 00 mov 0xa0a0(%rsp),%rbx

401930: 00

401931: 4c 8b b4 24 a8 a0 00 mov 0xa0a8(%rsp),%r14

401938: 00

401939: c7 84 24 3c 20 00 00 movl $0x0,0x203c(%rsp)

401940: 00 00 00 00

401944: ba 00 00 00 00 mov $0x0,%edx

401949: be 01 00 00 00 mov $0x1,%esi

40194e: bf 02 00 00 00 mov $0x2,%edi

401953: e8 68 f3 ff ff callq 400cc0 <socket@plt>

401958: 41 89 c4 mov %eax,%r12d

40195b: 85 c0 test %eax,%eax

40195d: 79 50 jns 4019af <submitr+0xaf>

40195f: 48 b8 45 72 72 6f 72 movabs $0x43203a726f727245,%rax

401966: 3a 20 43

401969: 49 89 06 mov %rax,(%r14)

40196c: 48 b8 6c 69 65 6e 74 movabs $0x6e7520746e65696c,%rax

401973: 20 75 6e

401976: 49 89 46 08 mov %rax,0x8(%r14)

40197a: 48 b8 61 62 6c 65 20 movabs $0x206f7420656c6261,%rax

401981: 74 6f 20

401984: 49 89 46 10 mov %rax,0x10(%r14)

401988: 48 b8 63 72 65 61 74 movabs $0x7320657461657263,%rax

40198f: 65 20 73

401992: 49 89 46 18 mov %rax,0x18(%r14)

401996: 41 c7 46 20 6f 63 6b movl $0x656b636f,0x20(%r14)

40199d: 65

40199e: 66 41 c7 46 24 74 00 movw $0x74,0x24(%r14)

4019a5: b8 ff ff ff ff mov $0xffffffff,%eax

4019aa: e9 06 07 00 00 jmpq 4020b5 <submitr+0x7b5>

4019af: 48 89 ef mov %rbp,%rdi

4019b2: e8 19 f2 ff ff callq 400bd0 <gethostbyname@plt>

4019b7: 48 85 c0 test %rax,%rax

4019ba: 75 6b jne 401a27 <submitr+0x127>

4019bc: 48 b8 45 72 72 6f 72 movabs $0x44203a726f727245,%rax

4019c3: 3a 20 44

4019c6: 49 89 06 mov %rax,(%r14)

4019c9: 48 b8 4e 53 20 69 73 movabs $0x6e7520736920534e,%rax

4019d0: 20 75 6e

4019d3: 49 89 46 08 mov %rax,0x8(%r14)

4019d7: 48 b8 61 62 6c 65 20 movabs $0x206f7420656c6261,%rax

4019de: 74 6f 20

4019e1: 49 89 46 10 mov %rax,0x10(%r14)

4019e5: 48 b8 72 65 73 6f 6c movabs $0x2065766c6f736572,%rax

4019ec: 76 65 20

4019ef: 49 89 46 18 mov %rax,0x18(%r14)

4019f3: 48 b8 73 65 72 76 65 movabs $0x6120726576726573,%rax

4019fa: 72 20 61

4019fd: 49 89 46 20 mov %rax,0x20(%r14)

401a01: 41 c7 46 28 64 64 72 movl $0x65726464,0x28(%r14)

401a08: 65

401a09: 66 41 c7 46 2c 73 73 movw $0x7373,0x2c(%r14)

401a10: 41 c6 46 2e 00 movb $0x0,0x2e(%r14)

401a15: 44 89 e7 mov %r12d,%edi

401a18: e8 63 f1 ff ff callq 400b80 <close@plt>

401a1d: b8 ff ff ff ff mov $0xffffffff,%eax

401a22: e9 8e 06 00 00 jmpq 4020b5 <submitr+0x7b5>

401a27: 48 c7 84 24 50 a0 00 movq $0x0,0xa050(%rsp)

401a2e: 00 00 00 00 00

401a33: 48 c7 84 24 58 a0 00 movq $0x0,0xa058(%rsp)

401a3a: 00 00 00 00 00

401a3f: 66 c7 84 24 50 a0 00 movw $0x2,0xa050(%rsp)

401a46: 00 02 00

401a49: 48 63 50 14 movslq 0x14(%rax),%rdx

401a4d: 48 8d b4 24 54 a0 00 lea 0xa054(%rsp),%rsi

401a54: 00

401a55: 48 8b 40 18 mov 0x18(%rax),%rax

401a59: 48 8b 38 mov (%rax),%rdi

401a5c: e8 df f1 ff ff callq 400c40 <bcopy@plt>

401a61: 66 41 c1 cd 08 ror $0x8,%r13w

401a66: 66 44 89 ac 24 52 a0 mov %r13w,0xa052(%rsp)

401a6d: 00 00

401a6f: ba 10 00 00 00 mov $0x10,%edx

401a74: 48 8d b4 24 50 a0 00 lea 0xa050(%rsp),%rsi

401a7b: 00

401a7c: 44 89 e7 mov %r12d,%edi

401a7f: e8 0c f2 ff ff callq 400c90 <connect@plt>

401a84: 85 c0 test %eax,%eax

401a86: 79 5d jns 401ae5 <submitr+0x1e5>

401a88: 48 b8 45 72 72 6f 72 movabs $0x55203a726f727245,%rax

401a8f: 3a 20 55

401a92: 49 89 06 mov %rax,(%r14)

401a95: 48 b8 6e 61 62 6c 65 movabs $0x6f7420656c62616e,%rax

401a9c: 20 74 6f

401a9f: 49 89 46 08 mov %rax,0x8(%r14)

401aa3: 48 b8 20 63 6f 6e 6e movabs $0x7463656e6e6f6320,%rax

401aaa: 65 63 74

401aad: 49 89 46 10 mov %rax,0x10(%r14)

401ab1: 48 b8 20 74 6f 20 74 movabs $0x20656874206f7420,%rax

401ab8: 68 65 20

401abb: 49 89 46 18 mov %rax,0x18(%r14)

401abf: 41 c7 46 20 73 65 72 movl $0x76726573,0x20(%r14)

401ac6: 76

401ac7: 66 41 c7 46 24 65 72 movw $0x7265,0x24(%r14)

401ace: 41 c6 46 26 00 movb $0x0,0x26(%r14)

401ad3: 44 89 e7 mov %r12d,%edi

401ad6: e8 a5 f0 ff ff callq 400b80 <close@plt>

401adb: b8 ff ff ff ff mov $0xffffffff,%eax

401ae0: e9 d0 05 00 00 jmpq 4020b5 <submitr+0x7b5>

401ae5: 48 c7 c2 ff ff ff ff mov $0xffffffffffffffff,%rdx

401aec: 48 89 df mov %rbx,%rdi

401aef: b8 00 00 00 00 mov $0x0,%eax

401af4: 48 89 d1 mov %rdx,%rcx

401af7: f2 ae repnz scas %es:(%rdi),%al

401af9: 48 f7 d1 not %rcx

401afc: 48 89 ce mov %rcx,%rsi

401aff: 48 8b 7c 24 08 mov 0x8(%rsp),%rdi

401b04: 48 89 d1 mov %rdx,%rcx

401b07: f2 ae repnz scas %es:(%rdi),%al

401b09: 49 89 c8 mov %rcx,%r8

401b0c: 48 8b 7c 24 10 mov 0x10(%rsp),%rdi

401b11: 48 89 d1 mov %rdx,%rcx

401b14: f2 ae repnz scas %es:(%rdi),%al

401b16: 48 f7 d1 not %rcx

401b19: 49 89 c9 mov %rcx,%r9

401b1c: 4c 89 ff mov %r15,%rdi

401b1f: 48 89 d1 mov %rdx,%rcx

401b22: f2 ae repnz scas %es:(%rdi),%al

401b24: 4d 29 c1 sub %r8,%r9

401b27: 49 29 c9 sub %rcx,%r9

401b2a: 48 8d 44 76 fd lea -0x3(%rsi,%rsi,2),%rax

401b2f: 49 8d 44 01 7b lea 0x7b(%r9,%rax,1),%rax

401b34: 48 3d 00 20 00 00 cmp $0x2000,%rax

401b3a: 76 73 jbe 401baf <submitr+0x2af>

401b3c: 48 b8 45 72 72 6f 72 movabs $0x52203a726f727245,%rax

401b43: 3a 20 52

401b46: 49 89 06 mov %rax,(%r14)

401b49: 48 b8 65 73 75 6c 74 movabs $0x747320746c757365,%rax

401b50: 20 73 74

401b53: 49 89 46 08 mov %rax,0x8(%r14)

401b57: 48 b8 72 69 6e 67 20 movabs $0x6f6f7420676e6972,%rax

401b5e: 74 6f 6f

401b61: 49 89 46 10 mov %rax,0x10(%r14)

401b65: 48 b8 20 6c 61 72 67 movabs $0x202e656772616c20,%rax

401b6c: 65 2e 20

401b6f: 49 89 46 18 mov %rax,0x18(%r14)

401b73: 48 b8 49 6e 63 72 65 movabs $0x6573616572636e49,%rax

401b7a: 61 73 65

401b7d: 49 89 46 20 mov %rax,0x20(%r14)

401b81: 48 b8 20 53 55 42 4d movabs $0x5254494d42555320,%rax

401b88: 49 54 52

401b8b: 49 89 46 28 mov %rax,0x28(%r14)

401b8f: 48 b8 5f 4d 41 58 42 movabs $0x46554258414d5f,%rax

401b96: 55 46 00

401b99: 49 89 46 30 mov %rax,0x30(%r14)

401b9d: 44 89 e7 mov %r12d,%edi

401ba0: e8 db ef ff ff callq 400b80 <close@plt>

401ba5: b8 ff ff ff ff mov $0xffffffff,%eax

401baa: e9 06 05 00 00 jmpq 4020b5 <submitr+0x7b5>

401baf: 48 8d 94 24 40 40 00 lea 0x4040(%rsp),%rdx

401bb6: 00

401bb7: b9 00 04 00 00 mov $0x400,%ecx

401bbc: b8 00 00 00 00 mov $0x0,%eax

401bc1: 48 89 d7 mov %rdx,%rdi

401bc4: f3 48 ab rep stos %rax,%es:(%rdi)

401bc7: 48 89 df mov %rbx,%rdi

401bca: 48 c7 c1 ff ff ff ff mov $0xffffffffffffffff,%rcx

401bd1: f2 ae repnz scas %es:(%rdi),%al

401bd3: 48 f7 d1 not %rcx

401bd6: 48 83 e9 01 sub $0x1,%rcx

401bda: 85 c9 test %ecx,%ecx

401bdc: 0f 84 d3 03 00 00 je 401fb5 <submitr+0x6b5>

401be2: 8d 41 ff lea -0x1(%rcx),%eax

401be5: 4c 8d 6c 03 01 lea 0x1(%rbx,%rax,1),%r13

401bea: 48 89 d5 mov %rdx,%rbp

401bed: 0f b6 13 movzbl (%rbx),%edx

401bf0: 80 fa 2a cmp $0x2a,%dl

401bf3: 74 1f je 401c14 <submitr+0x314>

401bf5: 8d 42 d3 lea -0x2d(%rdx),%eax

401bf8: 3c 01 cmp $0x1,%al

401bfa: 76 18 jbe 401c14 <submitr+0x314>

401bfc: 80 fa 5f cmp $0x5f,%dl

401bff: 74 13 je 401c14 <submitr+0x314>

401c01: 8d 42 d0 lea -0x30(%rdx),%eax

401c04: 3c 09 cmp $0x9,%al

401c06: 76 0c jbe 401c14 <submitr+0x314>

401c08: 89 d0 mov %edx,%eax

401c0a: 83 e0 df and $0xffffffdf,%eax

401c0d: 83 e8 41 sub $0x41,%eax

401c10: 3c 19 cmp $0x19,%al

401c12: 77 09 ja 401c1d <submitr+0x31d>

401c14: 48 8d 45 01 lea 0x1(%rbp),%rax

401c18: 88 55 00 mov %dl,0x0(%rbp)

401c1b: eb 52 jmp 401c6f <submitr+0x36f>

401c1d: 80 fa 20 cmp $0x20,%dl

401c20: 75 0a jne 401c2c <submitr+0x32c>

401c22: 48 8d 45 01 lea 0x1(%rbp),%rax

401c26: c6 45 00 2b movb $0x2b,0x0(%rbp)

401c2a: eb 43 jmp 401c6f <submitr+0x36f>

401c2c: 8d 42 e0 lea -0x20(%rdx),%eax

401c2f: 3c 5f cmp $0x5f,%al

401c31: 76 09 jbe 401c3c <submitr+0x33c>

401c33: 80 fa 09 cmp $0x9,%dl

401c36: 0f 85 f1 03 00 00 jne 40202d <submitr+0x72d>

401c3c: 0f b6 d2 movzbl %dl,%edx

401c3f: be 98 29 40 00 mov $0x402998,%esi

401c44: 48 8d 7c 24 20 lea 0x20(%rsp),%rdi

401c49: b8 00 00 00 00 mov $0x0,%eax

401c4e: e8 1d f0 ff ff callq 400c70 <sprintf@plt>

401c53: 0f b6 44 24 20 movzbl 0x20(%rsp),%eax

401c58: 88 45 00 mov %al,0x0(%rbp)

401c5b: 0f b6 44 24 21 movzbl 0x21(%rsp),%eax

401c60: 88 45 01 mov %al,0x1(%rbp)

401c63: 48 8d 45 03 lea 0x3(%rbp),%rax

401c67: 0f b6 54 24 22 movzbl 0x22(%rsp),%edx

401c6c: 88 55 02 mov %dl,0x2(%rbp)

401c6f: 48 83 c3 01 add $0x1,%rbx

401c73: 4c 39 eb cmp %r13,%rbx

401c76: 0f 84 39 03 00 00 je 401fb5 <submitr+0x6b5>

401c7c: 48 89 c5 mov %rax,%rbp

401c7f: e9 69 ff ff ff jmpq 401bed <submitr+0x2ed>

401c84: 48 89 da mov %rbx,%rdx

401c87: 48 89 ee mov %rbp,%rsi

401c8a: 44 89 e7 mov %r12d,%edi

401c8d: e8 be ee ff ff callq 400b50 <write@plt>

401c92: 48 85 c0 test %rax,%rax

401c95: 7f 10 jg 401ca7 <submitr+0x3a7>

401c97: e8 84 ee ff ff callq 400b20 <\_\_errno\_location@plt>

401c9c: 83 38 04 cmpl $0x4,(%rax)

401c9f: 90 nop

401ca0: 75 12 jne 401cb4 <submitr+0x3b4>

401ca2: b8 00 00 00 00 mov $0x0,%eax

401ca7: 48 01 c5 add %rax,%rbp

401caa: 48 29 c3 sub %rax,%rbx

401cad: 75 d5 jne 401c84 <submitr+0x384>

401caf: 4d 85 ed test %r13,%r13

401cb2: 79 5f jns 401d13 <submitr+0x413>

401cb4: 48 b8 45 72 72 6f 72 movabs $0x43203a726f727245,%rax

401cbb: 3a 20 43

401cbe: 49 89 06 mov %rax,(%r14)

401cc1: 48 b8 6c 69 65 6e 74 movabs $0x6e7520746e65696c,%rax

401cc8: 20 75 6e

401ccb: 49 89 46 08 mov %rax,0x8(%r14)

401ccf: 48 b8 61 62 6c 65 20 movabs $0x206f7420656c6261,%rax

401cd6: 74 6f 20

401cd9: 49 89 46 10 mov %rax,0x10(%r14)

401cdd: 48 b8 77 72 69 74 65 movabs $0x6f74206574697277,%rax

401ce4: 20 74 6f

401ce7: 49 89 46 18 mov %rax,0x18(%r14)

401ceb: 48 b8 20 74 68 65 20 movabs $0x7265732065687420,%rax

401cf2: 73 65 72

401cf5: 49 89 46 20 mov %rax,0x20(%r14)

401cf9: 41 c7 46 28 76 65 72 movl $0x726576,0x28(%r14)

401d00: 00

401d01: 44 89 e7 mov %r12d,%edi

401d04: e8 77 ee ff ff callq 400b80 <close@plt>

401d09: b8 ff ff ff ff mov $0xffffffff,%eax

401d0e: e9 a2 03 00 00 jmpq 4020b5 <submitr+0x7b5>

401d13: 44 89 a4 24 40 80 00 mov %r12d,0x8040(%rsp)

401d1a: 00

401d1b: c7 84 24 44 80 00 00 movl $0x0,0x8044(%rsp)

401d22: 00 00 00 00

401d26: 48 8d 84 24 50 80 00 lea 0x8050(%rsp),%rax

401d2d: 00

401d2e: 48 89 84 24 48 80 00 mov %rax,0x8048(%rsp)

401d35: 00

401d36: ba 00 20 00 00 mov $0x2000,%edx

401d3b: 48 8d b4 24 40 60 00 lea 0x6040(%rsp),%rsi

401d42: 00

401d43: 48 8d bc 24 40 80 00 lea 0x8040(%rsp),%rdi

401d4a: 00

401d4b: e8 99 fa ff ff callq 4017e9 <rio\_readlineb>

401d50: 48 85 c0 test %rax,%rax

401d53: 7f 74 jg 401dc9 <submitr+0x4c9>

401d55: 48 b8 45 72 72 6f 72 movabs $0x43203a726f727245,%rax

401d5c: 3a 20 43

401d5f: 49 89 06 mov %rax,(%r14)

401d62: 48 b8 6c 69 65 6e 74 movabs $0x6e7520746e65696c,%rax

401d69: 20 75 6e

401d6c: 49 89 46 08 mov %rax,0x8(%r14)

401d70: 48 b8 61 62 6c 65 20 movabs $0x206f7420656c6261,%rax

401d77: 74 6f 20

401d7a: 49 89 46 10 mov %rax,0x10(%r14)

401d7e: 48 b8 72 65 61 64 20 movabs $0x7269662064616572,%rax

401d85: 66 69 72

401d88: 49 89 46 18 mov %rax,0x18(%r14)

401d8c: 48 b8 73 74 20 68 65 movabs $0x6564616568207473,%rax

401d93: 61 64 65

401d96: 49 89 46 20 mov %rax,0x20(%r14)

401d9a: 48 b8 72 20 66 72 6f movabs $0x73206d6f72662072,%rax

401da1: 6d 20 73

401da4: 49 89 46 28 mov %rax,0x28(%r14)

401da8: 41 c7 46 30 65 72 76 movl $0x65767265,0x30(%r14)

401daf: 65

401db0: 66 41 c7 46 34 72 00 movw $0x72,0x34(%r14)

401db7: 44 89 e7 mov %r12d,%edi

401dba: e8 c1 ed ff ff callq 400b80 <close@plt>

401dbf: b8 ff ff ff ff mov $0xffffffff,%eax

401dc4: e9 ec 02 00 00 jmpq 4020b5 <submitr+0x7b5>

401dc9: 4c 8d 44 24 30 lea 0x30(%rsp),%r8

401dce: 48 8d 8c 24 3c 20 00 lea 0x203c(%rsp),%rcx

401dd5: 00

401dd6: 48 8d 94 24 40 20 00 lea 0x2040(%rsp),%rdx

401ddd: 00

401dde: be 9f 29 40 00 mov $0x40299f,%esi

401de3: 48 8d bc 24 40 60 00 lea 0x6040(%rsp),%rdi

401dea: 00

401deb: b8 00 00 00 00 mov $0x0,%eax

401df0: e8 3b ee ff ff callq 400c30 <\_\_isoc99\_sscanf@plt>

401df5: 8b 94 24 3c 20 00 00 mov 0x203c(%rsp),%edx

401dfc: 81 fa c8 00 00 00 cmp $0xc8,%edx

401e02: 0f 84 b2 00 00 00 je 401eba <submitr+0x5ba>

401e08: 48 8d 4c 24 30 lea 0x30(%rsp),%rcx

401e0d: be f0 28 40 00 mov $0x4028f0,%esi

401e12: 4c 89 f7 mov %r14,%rdi

401e15: b8 00 00 00 00 mov $0x0,%eax

401e1a: e8 51 ee ff ff callq 400c70 <sprintf@plt>

401e1f: 44 89 e7 mov %r12d,%edi

401e22: e8 59 ed ff ff callq 400b80 <close@plt>

401e27: b8 ff ff ff ff mov $0xffffffff,%eax

401e2c: e9 84 02 00 00 jmpq 4020b5 <submitr+0x7b5>

401e31: ba 00 20 00 00 mov $0x2000,%edx

401e36: 48 8d b4 24 40 60 00 lea 0x6040(%rsp),%rsi

401e3d: 00

401e3e: 48 8d bc 24 40 80 00 lea 0x8040(%rsp),%rdi

401e45: 00

401e46: e8 9e f9 ff ff callq 4017e9 <rio\_readlineb>

401e4b: 48 85 c0 test %rax,%rax

401e4e: 7f 6a jg 401eba <submitr+0x5ba>

401e50: 48 b8 45 72 72 6f 72 movabs $0x43203a726f727245,%rax

401e57: 3a 20 43

401e5a: 49 89 06 mov %rax,(%r14)

401e5d: 48 b8 6c 69 65 6e 74 movabs $0x6e7520746e65696c,%rax

401e64: 20 75 6e

401e67: 49 89 46 08 mov %rax,0x8(%r14)

401e6b: 48 b8 61 62 6c 65 20 movabs $0x206f7420656c6261,%rax

401e72: 74 6f 20

401e75: 49 89 46 10 mov %rax,0x10(%r14)

401e79: 48 b8 72 65 61 64 20 movabs $0x6165682064616572,%rax

401e80: 68 65 61

401e83: 49 89 46 18 mov %rax,0x18(%r14)

401e87: 48 b8 64 65 72 73 20 movabs $0x6f72662073726564,%rax

401e8e: 66 72 6f

401e91: 49 89 46 20 mov %rax,0x20(%r14)

401e95: 48 b8 6d 20 73 65 72 movabs $0x726576726573206d,%rax

401e9c: 76 65 72

401e9f: 49 89 46 28 mov %rax,0x28(%r14)

401ea3: 41 c6 46 30 00 movb $0x0,0x30(%r14)

401ea8: 44 89 e7 mov %r12d,%edi

401eab: e8 d0 ec ff ff callq 400b80 <close@plt>

401eb0: b8 ff ff ff ff mov $0xffffffff,%eax

401eb5: e9 fb 01 00 00 jmpq 4020b5 <submitr+0x7b5>

401eba: 80 bc 24 40 60 00 00 cmpb $0xd,0x6040(%rsp)

401ec1: 0d

401ec2: 0f 85 69 ff ff ff jne 401e31 <submitr+0x531>

401ec8: 80 bc 24 41 60 00 00 cmpb $0xa,0x6041(%rsp)

401ecf: 0a

401ed0: 0f 85 5b ff ff ff jne 401e31 <submitr+0x531>

401ed6: 80 bc 24 42 60 00 00 cmpb $0x0,0x6042(%rsp)

401edd: 00

401ede: 0f 85 4d ff ff ff jne 401e31 <submitr+0x531>

401ee4: ba 00 20 00 00 mov $0x2000,%edx

401ee9: 48 8d b4 24 40 60 00 lea 0x6040(%rsp),%rsi

401ef0: 00

401ef1: 48 8d bc 24 40 80 00 lea 0x8040(%rsp),%rdi

401ef8: 00

401ef9: e8 eb f8 ff ff callq 4017e9 <rio\_readlineb>

401efe: 48 85 c0 test %rax,%rax

401f01: 7f 73 jg 401f76 <submitr+0x676>

401f03: 48 b8 45 72 72 6f 72 movabs $0x43203a726f727245,%rax

401f0a: 3a 20 43

401f0d: 49 89 06 mov %rax,(%r14)

401f10: 48 b8 6c 69 65 6e 74 movabs $0x6e7520746e65696c,%rax

401f17: 20 75 6e

401f1a: 49 89 46 08 mov %rax,0x8(%r14)

401f1e: 48 b8 61 62 6c 65 20 movabs $0x206f7420656c6261,%rax

401f25: 74 6f 20

401f28: 49 89 46 10 mov %rax,0x10(%r14)

401f2c: 48 b8 72 65 61 64 20 movabs $0x6174732064616572,%rax

401f33: 73 74 61

401f36: 49 89 46 18 mov %rax,0x18(%r14)

401f3a: 48 b8 74 75 73 20 6d movabs $0x7373656d20737574,%rax

401f41: 65 73 73

401f44: 49 89 46 20 mov %rax,0x20(%r14)

401f48: 48 b8 61 67 65 20 66 movabs $0x6d6f726620656761,%rax

401f4f: 72 6f 6d

401f52: 49 89 46 28 mov %rax,0x28(%r14)

401f56: 48 b8 20 73 65 72 76 movabs $0x72657672657320,%rax

401f5d: 65 72 00

401f60: 49 89 46 30 mov %rax,0x30(%r14)

401f64: 44 89 e7 mov %r12d,%edi

401f67: e8 14 ec ff ff callq 400b80 <close@plt>

401f6c: b8 ff ff ff ff mov $0xffffffff,%eax

401f71: e9 3f 01 00 00 jmpq 4020b5 <submitr+0x7b5>

401f76: 48 8d b4 24 40 60 00 lea 0x6040(%rsp),%rsi

401f7d: 00

401f7e: 4c 89 f7 mov %r14,%rdi

401f81: e8 aa eb ff ff callq 400b30 <strcpy@plt>

401f86: 44 89 e7 mov %r12d,%edi

401f89: e8 f2 eb ff ff callq 400b80 <close@plt>

401f8e: 41 0f b6 06 movzbl (%r14),%eax

401f92: 83 e8 4f sub $0x4f,%eax

401f95: 75 0f jne 401fa6 <submitr+0x6a6>

401f97: 41 0f b6 46 01 movzbl 0x1(%r14),%eax

401f9c: 83 e8 4b sub $0x4b,%eax

401f9f: 75 05 jne 401fa6 <submitr+0x6a6>

401fa1: 41 0f b6 46 02 movzbl 0x2(%r14),%eax

401fa6: 85 c0 test %eax,%eax

401fa8: 0f 95 c0 setne %al

401fab: 0f b6 c0 movzbl %al,%eax

401fae: f7 d8 neg %eax

401fb0: e9 00 01 00 00 jmpq 4020b5 <submitr+0x7b5>

401fb5: 48 8d 84 24 40 40 00 lea 0x4040(%rsp),%rax

401fbc: 00

401fbd: 48 89 04 24 mov %rax,(%rsp)

401fc1: 4d 89 f9 mov %r15,%r9

401fc4: 4c 8b 44 24 18 mov 0x18(%rsp),%r8

401fc9: 48 8b 4c 24 10 mov 0x10(%rsp),%rcx

401fce: 48 8b 54 24 08 mov 0x8(%rsp),%rdx

401fd3: be 20 29 40 00 mov $0x402920,%esi

401fd8: 48 8d bc 24 40 60 00 lea 0x6040(%rsp),%rdi

401fdf: 00

401fe0: b8 00 00 00 00 mov $0x0,%eax

401fe5: e8 86 ec ff ff callq 400c70 <sprintf@plt>

401fea: 48 8d bc 24 40 60 00 lea 0x6040(%rsp),%rdi

401ff1: 00

401ff2: e8 49 eb ff ff callq 400b40 <puts@plt>

401ff7: 48 8d bc 24 40 60 00 lea 0x6040(%rsp),%rdi

401ffe: 00

401fff: b8 00 00 00 00 mov $0x0,%eax

402004: 48 c7 c1 ff ff ff ff mov $0xffffffffffffffff,%rcx

40200b: f2 ae repnz scas %es:(%rdi),%al

40200d: 48 f7 d1 not %rcx

402010: 48 83 e9 01 sub $0x1,%rcx

402014: 49 89 cd mov %rcx,%r13

402017: 0f 84 f6 fc ff ff je 401d13 <submitr+0x413>

40201d: 48 89 cb mov %rcx,%rbx

402020: 48 8d ac 24 40 60 00 lea 0x6040(%rsp),%rbp

402027: 00

402028: e9 57 fc ff ff jmpq 401c84 <submitr+0x384>

40202d: 48 b8 45 72 72 6f 72 movabs $0x52203a726f727245,%rax

402034: 3a 20 52

402037: 49 89 06 mov %rax,(%r14)

40203a: 48 b8 65 73 75 6c 74 movabs $0x747320746c757365,%rax

402041: 20 73 74

402044: 49 89 46 08 mov %rax,0x8(%r14)

402048: 48 b8 72 69 6e 67 20 movabs $0x6e6f6320676e6972,%rax

40204f: 63 6f 6e

402052: 49 89 46 10 mov %rax,0x10(%r14)

402056: 48 b8 74 61 69 6e 73 movabs $0x6e6120736e696174,%rax

40205d: 20 61 6e

402060: 49 89 46 18 mov %rax,0x18(%r14)

402064: 48 b8 20 69 6c 6c 65 movabs $0x6c6167656c6c6920,%rax

40206b: 67 61 6c

40206e: 49 89 46 20 mov %rax,0x20(%r14)

402072: 48 b8 20 6f 72 20 75 movabs $0x72706e7520726f20,%rax

402079: 6e 70 72

40207c: 49 89 46 28 mov %rax,0x28(%r14)

402080: 48 b8 69 6e 74 61 62 movabs $0x20656c6261746e69,%rax

402087: 6c 65 20

40208a: 49 89 46 30 mov %rax,0x30(%r14)

40208e: 48 b8 63 68 61 72 61 movabs $0x6574636172616863,%rax

402095: 63 74 65

402098: 49 89 46 38 mov %rax,0x38(%r14)

40209c: 66 41 c7 46 40 72 2e movw $0x2e72,0x40(%r14)

4020a3: 41 c6 46 42 00 movb $0x0,0x42(%r14)

4020a8: 44 89 e7 mov %r12d,%edi

4020ab: e8 d0 ea ff ff callq 400b80 <close@plt>

4020b0: b8 ff ff ff ff mov $0xffffffff,%eax

4020b5: 48 81 c4 68 a0 00 00 add $0xa068,%rsp

4020bc: 5b pop %rbx

4020bd: 5d pop %rbp

4020be: 41 5c pop %r12

4020c0: 41 5d pop %r13

4020c2: 41 5e pop %r14

4020c4: 41 5f pop %r15

4020c6: c3 retq

00000000004020c7 <init\_timeout>:

4020c7: 53 push %rbx

4020c8: 89 fb mov %edi,%ebx

4020ca: 85 ff test %edi,%edi

4020cc: 74 1e je 4020ec <init\_timeout+0x25>

4020ce: be c0 17 40 00 mov $0x4017c0,%esi

4020d3: bf 0e 00 00 00 mov $0xe,%edi

4020d8: e8 e3 ea ff ff callq 400bc0 <signal@plt>

4020dd: 85 db test %ebx,%ebx

4020df: bf 00 00 00 00 mov $0x0,%edi

4020e4: 0f 49 fb cmovns %ebx,%edi

4020e7: e8 84 ea ff ff callq 400b70 <alarm@plt>

4020ec: 5b pop %rbx

4020ed: c3 retq

00000000004020ee <init\_driver>:

4020ee: 55 push %rbp

4020ef: 53 push %rbx

4020f0: 48 83 ec 18 sub $0x18,%rsp

4020f4: 48 89 fd mov %rdi,%rbp

4020f7: be 01 00 00 00 mov $0x1,%esi

4020fc: bf 0d 00 00 00 mov $0xd,%edi

402101: e8 ba ea ff ff callq 400bc0 <signal@plt>

402106: be 01 00 00 00 mov $0x1,%esi

40210b: bf 1d 00 00 00 mov $0x1d,%edi

402110: e8 ab ea ff ff callq 400bc0 <signal@plt>

402115: be 01 00 00 00 mov $0x1,%esi

40211a: bf 1d 00 00 00 mov $0x1d,%edi

40211f: e8 9c ea ff ff callq 400bc0 <signal@plt>

402124: ba 00 00 00 00 mov $0x0,%edx

402129: be 01 00 00 00 mov $0x1,%esi

40212e: bf 02 00 00 00 mov $0x2,%edi

402133: e8 88 eb ff ff callq 400cc0 <socket@plt>

402138: 89 c3 mov %eax,%ebx

40213a: 85 c0 test %eax,%eax

40213c: 79 4f jns 40218d <init\_driver+0x9f>

40213e: 48 b8 45 72 72 6f 72 movabs $0x43203a726f727245,%rax

402145: 3a 20 43

402148: 48 89 45 00 mov %rax,0x0(%rbp)

40214c: 48 b8 6c 69 65 6e 74 movabs $0x6e7520746e65696c,%rax

402153: 20 75 6e

402156: 48 89 45 08 mov %rax,0x8(%rbp)

40215a: 48 b8 61 62 6c 65 20 movabs $0x206f7420656c6261,%rax

402161: 74 6f 20

402164: 48 89 45 10 mov %rax,0x10(%rbp)

402168: 48 b8 63 72 65 61 74 movabs $0x7320657461657263,%rax

40216f: 65 20 73

402172: 48 89 45 18 mov %rax,0x18(%rbp)

402176: c7 45 20 6f 63 6b 65 movl $0x656b636f,0x20(%rbp)

40217d: 66 c7 45 24 74 00 movw $0x74,0x24(%rbp)

402183: b8 ff ff ff ff mov $0xffffffff,%eax

402188: e9 f8 00 00 00 jmpq 402285 <init\_driver+0x197>

40218d: bf b0 29 40 00 mov $0x4029b0,%edi

402192: e8 39 ea ff ff callq 400bd0 <gethostbyname@plt>

402197: 48 85 c0 test %rax,%rax

40219a: 75 68 jne 402204 <init\_driver+0x116>

40219c: 48 b8 45 72 72 6f 72 movabs $0x44203a726f727245,%rax

4021a3: 3a 20 44

4021a6: 48 89 45 00 mov %rax,0x0(%rbp)

4021aa: 48 b8 4e 53 20 69 73 movabs $0x6e7520736920534e,%rax

4021b1: 20 75 6e

4021b4: 48 89 45 08 mov %rax,0x8(%rbp)

4021b8: 48 b8 61 62 6c 65 20 movabs $0x206f7420656c6261,%rax

4021bf: 74 6f 20

4021c2: 48 89 45 10 mov %rax,0x10(%rbp)

4021c6: 48 b8 72 65 73 6f 6c movabs $0x2065766c6f736572,%rax

4021cd: 76 65 20

4021d0: 48 89 45 18 mov %rax,0x18(%rbp)

4021d4: 48 b8 73 65 72 76 65 movabs $0x6120726576726573,%rax

4021db: 72 20 61

4021de: 48 89 45 20 mov %rax,0x20(%rbp)

4021e2: c7 45 28 64 64 72 65 movl $0x65726464,0x28(%rbp)

4021e9: 66 c7 45 2c 73 73 movw $0x7373,0x2c(%rbp)

4021ef: c6 45 2e 00 movb $0x0,0x2e(%rbp)

4021f3: 89 df mov %ebx,%edi

4021f5: e8 86 e9 ff ff callq 400b80 <close@plt>

4021fa: b8 ff ff ff ff mov $0xffffffff,%eax

4021ff: e9 81 00 00 00 jmpq 402285 <init\_driver+0x197>

402204: 48 c7 04 24 00 00 00 movq $0x0,(%rsp)

40220b: 00

40220c: 48 c7 44 24 08 00 00 movq $0x0,0x8(%rsp)

402213: 00 00

402215: 66 c7 04 24 02 00 movw $0x2,(%rsp)

40221b: 48 63 50 14 movslq 0x14(%rax),%rdx

40221f: 48 8d 74 24 04 lea 0x4(%rsp),%rsi

402224: 48 8b 40 18 mov 0x18(%rax),%rax

402228: 48 8b 38 mov (%rax),%rdi

40222b: e8 10 ea ff ff callq 400c40 <bcopy@plt>

402230: 66 c7 44 24 02 3b 6e movw $0x6e3b,0x2(%rsp)

402237: ba 10 00 00 00 mov $0x10,%edx

40223c: 48 89 e6 mov %rsp,%rsi

40223f: 89 df mov %ebx,%edi

402241: e8 4a ea ff ff callq 400c90 <connect@plt>

402246: 85 c0 test %eax,%eax

402248: 79 25 jns 40226f <init\_driver+0x181>

40224a: ba b0 29 40 00 mov $0x4029b0,%edx

40224f: be 70 29 40 00 mov $0x402970,%esi

402254: 48 89 ef mov %rbp,%rdi

402257: b8 00 00 00 00 mov $0x0,%eax

40225c: e8 0f ea ff ff callq 400c70 <sprintf@plt>

402261: 89 df mov %ebx,%edi

402263: e8 18 e9 ff ff callq 400b80 <close@plt>

402268: b8 ff ff ff ff mov $0xffffffff,%eax

40226d: eb 16 jmp 402285 <init\_driver+0x197>

40226f: 89 df mov %ebx,%edi

402271: e8 0a e9 ff ff callq 400b80 <close@plt>

402276: 66 c7 45 00 4f 4b movw $0x4b4f,0x0(%rbp)

40227c: c6 45 02 00 movb $0x0,0x2(%rbp)

402280: b8 00 00 00 00 mov $0x0,%eax

402285: 48 83 c4 18 add $0x18,%rsp

402289: 5b pop %rbx

40228a: 5d pop %rbp

40228b: c3 retq

000000000040228c <driver\_post>:

40228c: 53 push %rbx

40228d: 48 83 ec 10 sub $0x10,%rsp

402291: 4c 89 c3 mov %r8,%rbx

402294: 85 c9 test %ecx,%ecx

402296: 74 22 je 4022ba <driver\_post+0x2e>

402298: 48 89 d6 mov %rdx,%rsi

40229b: bf bd 29 40 00 mov $0x4029bd,%edi

4022a0: b8 00 00 00 00 mov $0x0,%eax

4022a5: e8 b6 e8 ff ff callq 400b60 <printf@plt>

4022aa: 66 c7 03 4f 4b movw $0x4b4f,(%rbx)

4022af: c6 43 02 00 movb $0x0,0x2(%rbx)

4022b3: b8 00 00 00 00 mov $0x0,%eax

4022b8: eb 43 jmp 4022fd <driver\_post+0x71>

4022ba: 48 85 ff test %rdi,%rdi

4022bd: 74 30 je 4022ef <driver\_post+0x63>

4022bf: 80 3f 00 cmpb $0x0,(%rdi)

4022c2: 74 2b je 4022ef <driver\_post+0x63>

4022c4: 4c 89 44 24 08 mov %r8,0x8(%rsp)

4022c9: 48 89 14 24 mov %rdx,(%rsp)

4022cd: 41 b9 d4 29 40 00 mov $0x4029d4,%r9d

4022d3: 49 89 f0 mov %rsi,%r8

4022d6: 48 89 f9 mov %rdi,%rcx

4022d9: ba da 29 40 00 mov $0x4029da,%edx

4022de: be 6e 3b 00 00 mov $0x3b6e,%esi

4022e3: bf b0 29 40 00 mov $0x4029b0,%edi

4022e8: e8 13 f6 ff ff callq 401900 <submitr>

4022ed: eb 0e jmp 4022fd <driver\_post+0x71>

4022ef: 66 c7 03 4f 4b movw $0x4b4f,(%rbx)

4022f4: c6 43 02 00 movb $0x0,0x2(%rbx)

4022f8: b8 00 00 00 00 mov $0x0,%eax

4022fd: 48 83 c4 10 add $0x10,%rsp

402301: 5b pop %rbx

402302: c3 retq

402303: 66 2e 0f 1f 84 00 00 nopw %cs:0x0(%rax,%rax,1)

40230a: 00 00 00

40230d: 0f 1f 00 nopl (%rax)

0000000000402310 <\_\_libc\_csu\_init>:

402310: 41 57 push %r15

402312: 41 89 ff mov %edi,%r15d

402315: 41 56 push %r14

402317: 49 89 f6 mov %rsi,%r14

40231a: 41 55 push %r13

40231c: 49 89 d5 mov %rdx,%r13

40231f: 41 54 push %r12

402321: 4c 8d 25 e8 1a 20 00 lea 0x201ae8(%rip),%r12 # 603e10 <\_\_frame\_dummy\_init\_array\_entry>

402328: 55 push %rbp

402329: 48 8d 2d e8 1a 20 00 lea 0x201ae8(%rip),%rbp # 603e18 <\_\_init\_array\_end>

402330: 53 push %rbx

402331: 4c 29 e5 sub %r12,%rbp

402334: 31 db xor %ebx,%ebx

402336: 48 c1 fd 03 sar $0x3,%rbp

40233a: 48 83 ec 08 sub $0x8,%rsp

40233e: e8 8d e7 ff ff callq 400ad0 <\_init>

402343: 48 85 ed test %rbp,%rbp

402346: 74 1e je 402366 <\_\_libc\_csu\_init+0x56>

402348: 0f 1f 84 00 00 00 00 nopl 0x0(%rax,%rax,1)

40234f: 00

402350: 4c 89 ea mov %r13,%rdx

402353: 4c 89 f6 mov %r14,%rsi

402356: 44 89 ff mov %r15d,%edi

402359: 41 ff 14 dc callq \*(%r12,%rbx,8)

40235d: 48 83 c3 01 add $0x1,%rbx

402361: 48 39 eb cmp %rbp,%rbx

402364: 75 ea jne 402350 <\_\_libc\_csu\_init+0x40>

402366: 48 83 c4 08 add $0x8,%rsp

40236a: 5b pop %rbx

40236b: 5d pop %rbp

40236c: 41 5c pop %r12

40236e: 41 5d pop %r13

402370: 41 5e pop %r14

402372: 41 5f pop %r15

402374: c3 retq

402375: 90 nop

402376: 66 2e 0f 1f 84 00 00 nopw %cs:0x0(%rax,%rax,1)

40237d: 00 00 00

0000000000402380 <\_\_libc\_csu\_fini>:

402380: f3 c3 repz retq

Disassembly of section .fini:

0000000000402384 <\_fini>:

402384: 48 83 ec 08 sub $0x8,%rsp

402388: 48 83 c4 08 add $0x8,%rsp

40238c: c3 retq