bomb: file format elf64-x86-64

Disassembly of section .init:

0000000000400a88 <\_init>:

400a88: 48 83 ec 08 sub $0x8,%rsp

400a8c: e8 3b 02 00 00 callq 400ccc <call\_gmon\_start>

400a91: e8 ba 02 00 00 callq 400d50 <frame\_dummy>

400a96: e8 a5 0e 00 00 callq 401940 <\_\_do\_global\_ctors\_aux>

400a9b: 48 83 c4 08 add $0x8,%rsp

400a9f: c3 retq

Disassembly of section .plt:

0000000000400aa0 <printf@plt-0x10>:

400aa0: ff 35 8a 1a 20 00 pushq 2103946(%rip) # 602530 <\_GLOBAL\_OFFSET\_TABLE\_+0x8>

400aa6: ff 25 8c 1a 20 00 jmpq \*2103948(%rip) # 602538 <\_GLOBAL\_OFFSET\_TABLE\_+0x10>

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

0000000000400ab0 <printf@plt>:

400ab0: ff 25 8a 1a 20 00 jmpq \*2103946(%rip) # 602540 <\_GLOBAL\_OFFSET\_TABLE\_+0x18>

400ab6: 68 00 00 00 00 pushq $0x0

400abb: e9 e0 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400ac0 <close@plt>:

400ac0: ff 25 82 1a 20 00 jmpq \*2103938(%rip) # 602548 <\_GLOBAL\_OFFSET\_TABLE\_+0x20>

400ac6: 68 01 00 00 00 pushq $0x1

400acb: e9 d0 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400ad0 <gethostbyname@plt>:

400ad0: ff 25 7a 1a 20 00 jmpq \*2103930(%rip) # 602550 <\_GLOBAL\_OFFSET\_TABLE\_+0x28>

400ad6: 68 02 00 00 00 pushq $0x2

400adb: e9 c0 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400ae0 <puts@plt>:

400ae0: ff 25 72 1a 20 00 jmpq \*2103922(%rip) # 602558 <\_GLOBAL\_OFFSET\_TABLE\_+0x30>

400ae6: 68 03 00 00 00 pushq $0x3

400aeb: e9 b0 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400af0 <exit@plt>:

400af0: ff 25 6a 1a 20 00 jmpq \*2103914(%rip) # 602560 <\_GLOBAL\_OFFSET\_TABLE\_+0x38>

400af6: 68 04 00 00 00 pushq $0x4

400afb: e9 a0 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400b00 <strcasecmp@plt>:

400b00: ff 25 62 1a 20 00 jmpq \*2103906(%rip) # 602568 <\_GLOBAL\_OFFSET\_TABLE\_+0x40>

400b06: 68 05 00 00 00 pushq $0x5

400b0b: e9 90 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400b10 <fopen@plt>:

400b10: ff 25 5a 1a 20 00 jmpq \*2103898(%rip) # 602570 <\_GLOBAL\_OFFSET\_TABLE\_+0x48>

400b16: 68 06 00 00 00 pushq $0x6

400b1b: e9 80 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400b20 <\_\_libc\_start\_main@plt>:

400b20: ff 25 52 1a 20 00 jmpq \*2103890(%rip) # 602578 <\_GLOBAL\_OFFSET\_TABLE\_+0x50>

400b26: 68 07 00 00 00 pushq $0x7

400b2b: e9 70 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400b30 <dup@plt>:

400b30: ff 25 4a 1a 20 00 jmpq \*2103882(%rip) # 602580 <\_GLOBAL\_OFFSET\_TABLE\_+0x58>

400b36: 68 08 00 00 00 pushq $0x8

400b3b: e9 60 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400b40 <system@plt>:

400b40: ff 25 42 1a 20 00 jmpq \*2103874(%rip) # 602588 <\_GLOBAL\_OFFSET\_TABLE\_+0x60>

400b46: 68 09 00 00 00 pushq $0x9

400b4b: e9 50 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400b50 <fgets@plt>:

400b50: ff 25 3a 1a 20 00 jmpq \*2103866(%rip) # 602590 <\_GLOBAL\_OFFSET\_TABLE\_+0x68>

400b56: 68 0a 00 00 00 pushq $0xa

400b5b: e9 40 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400b60 <fputc@plt>:

400b60: ff 25 32 1a 20 00 jmpq \*2103858(%rip) # 602598 <\_GLOBAL\_OFFSET\_TABLE\_+0x70>

400b66: 68 0b 00 00 00 pushq $0xb

400b6b: e9 30 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400b70 <bcopy@plt>:

400b70: ff 25 2a 1a 20 00 jmpq \*2103850(%rip) # 6025a0 <\_GLOBAL\_OFFSET\_TABLE\_+0x78>

400b76: 68 0c 00 00 00 pushq $0xc

400b7b: e9 20 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400b80 <\_\_ctype\_b\_loc@plt>:

400b80: ff 25 22 1a 20 00 jmpq \*2103842(%rip) # 6025a8 <\_GLOBAL\_OFFSET\_TABLE\_+0x80>

400b86: 68 0d 00 00 00 pushq $0xd

400b8b: e9 10 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400b90 <sprintf@plt>:

400b90: ff 25 1a 1a 20 00 jmpq \*2103834(%rip) # 6025b0 <\_GLOBAL\_OFFSET\_TABLE\_+0x88>

400b96: 68 0e 00 00 00 pushq $0xe

400b9b: e9 00 ff ff ff jmpq 400aa0 <\_init+0x18>

0000000000400ba0 <\_\_strtol\_internal@plt>:

400ba0: ff 25 12 1a 20 00 jmpq \*2103826(%rip) # 6025b8 <\_GLOBAL\_OFFSET\_TABLE\_+0x90>

400ba6: 68 0f 00 00 00 pushq $0xf

400bab: e9 f0 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400bb0 <sscanf@plt>:

400bb0: ff 25 0a 1a 20 00 jmpq \*2103818(%rip) # 6025c0 <\_GLOBAL\_OFFSET\_TABLE\_+0x98>

400bb6: 68 10 00 00 00 pushq $0x10

400bbb: e9 e0 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400bc0 <sleep@plt>:

400bc0: ff 25 02 1a 20 00 jmpq \*2103810(%rip) # 6025c8 <\_GLOBAL\_OFFSET\_TABLE\_+0xa0>

400bc6: 68 11 00 00 00 pushq $0x11

400bcb: e9 d0 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400bd0 <rewind@plt>:

400bd0: ff 25 fa 19 20 00 jmpq \*2103802(%rip) # 6025d0 <\_GLOBAL\_OFFSET\_TABLE\_+0xa8>

400bd6: 68 12 00 00 00 pushq $0x12

400bdb: e9 c0 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400be0 <connect@plt>:

400be0: ff 25 f2 19 20 00 jmpq \*2103794(%rip) # 6025d8 <\_GLOBAL\_OFFSET\_TABLE\_+0xb0>

400be6: 68 13 00 00 00 pushq $0x13

400beb: e9 b0 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400bf0 <gethostname@plt>:

400bf0: ff 25 ea 19 20 00 jmpq \*2103786(%rip) # 6025e0 <\_GLOBAL\_OFFSET\_TABLE\_+0xb8>

400bf6: 68 14 00 00 00 pushq $0x14

400bfb: e9 a0 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400c00 <tmpfile@plt>:

400c00: ff 25 e2 19 20 00 jmpq \*2103778(%rip) # 6025e8 <\_GLOBAL\_OFFSET\_TABLE\_+0xc0>

400c06: 68 15 00 00 00 pushq $0x15

400c0b: e9 90 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400c10 <signal@plt>:

400c10: ff 25 da 19 20 00 jmpq \*2103770(%rip) # 6025f0 <\_GLOBAL\_OFFSET\_TABLE\_+0xc8>

400c16: 68 16 00 00 00 pushq $0x16

400c1b: e9 80 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400c20 <socket@plt>:

400c20: ff 25 d2 19 20 00 jmpq \*2103762(%rip) # 6025f8 <\_GLOBAL\_OFFSET\_TABLE\_+0xd0>

400c26: 68 17 00 00 00 pushq $0x17

400c2b: e9 70 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400c30 <getenv@plt>:

400c30: ff 25 ca 19 20 00 jmpq \*2103754(%rip) # 602600 <\_GLOBAL\_OFFSET\_TABLE\_+0xd8>

400c36: 68 18 00 00 00 pushq $0x18

400c3b: e9 60 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400c40 <cuserid@plt>:

400c40: ff 25 c2 19 20 00 jmpq \*2103746(%rip) # 602608 <\_GLOBAL\_OFFSET\_TABLE\_+0xe0>

400c46: 68 19 00 00 00 pushq $0x19

400c4b: e9 50 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400c50 <strcpy@plt>:

400c50: ff 25 ba 19 20 00 jmpq \*2103738(%rip) # 602610 <\_GLOBAL\_OFFSET\_TABLE\_+0xe8>

400c56: 68 1a 00 00 00 pushq $0x1a

400c5b: e9 40 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400c60 <fclose@plt>:

400c60: ff 25 b2 19 20 00 jmpq \*2103730(%rip) # 602618 <\_GLOBAL\_OFFSET\_TABLE\_+0xf0>

400c66: 68 1b 00 00 00 pushq $0x1b

400c6b: e9 30 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400c70 <fwrite@plt>:

400c70: ff 25 aa 19 20 00 jmpq \*2103722(%rip) # 602620 <\_GLOBAL\_OFFSET\_TABLE\_+0xf8>

400c76: 68 1c 00 00 00 pushq $0x1c

400c7b: e9 20 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400c80 <fprintf@plt>:

400c80: ff 25 a2 19 20 00 jmpq \*2103714(%rip) # 602628 <\_GLOBAL\_OFFSET\_TABLE\_+0x100>

400c86: 68 1d 00 00 00 pushq $0x1d

400c8b: e9 10 fe ff ff jmpq 400aa0 <\_init+0x18>

0000000000400c90 <fflush@plt>:

400c90: ff 25 9a 19 20 00 jmpq \*2103706(%rip) # 602630 <\_GLOBAL\_OFFSET\_TABLE\_+0x108>

400c96: 68 1e 00 00 00 pushq $0x1e

400c9b: e9 00 fe ff ff jmpq 400aa0 <\_init+0x18>

Disassembly of section .text:

0000000000400ca0 <\_start>:

400ca0: 31 ed xor %ebp,%ebp

400ca2: 49 89 d1 mov %rdx,%r9

400ca5: 5e pop %rsi

400ca6: 48 89 e2 mov %rsp,%rdx

400ca9: 48 83 e4 f0 and $0xfffffffffffffff0,%rsp

400cad: 50 push %rax

400cae: 54 push %rsp

400caf: 49 c7 c0 a0 18 40 00 mov $0x4018a0,%r8

400cb6: 48 c7 c1 b0 18 40 00 mov $0x4018b0,%rcx

400cbd: 48 c7 c7 78 0d 40 00 mov $0x400d78,%rdi

400cc4: e8 57 fe ff ff callq 400b20 <\_\_libc\_start\_main@plt>

400cc9: f4 hlt

400cca: 90 nop

400ccb: 90 nop

0000000000400ccc <call\_gmon\_start>:

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

400cd0: 48 8b 05 49 18 20 00 mov 2103369(%rip),%rax # 602520 <\_DYNAMIC+0x190>

400cd7: 48 85 c0 test %rax,%rax

400cda: 74 02 je 400cde <call\_gmon\_start+0x12>

400cdc: ff d0 callq \*%rax

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

400ce2: c3 retq

400ce3: 90 nop

400ce4: 90 nop

400ce5: 90 nop

400ce6: 90 nop

400ce7: 90 nop

400ce8: 90 nop

400ce9: 90 nop

400cea: 90 nop

400ceb: 90 nop

400cec: 90 nop

400ced: 90 nop

400cee: 90 nop

400cef: 90 nop

0000000000400cf0 <\_\_do\_global\_dtors\_aux>:

400cf0: 55 push %rbp

400cf1: 48 89 e5 mov %rsp,%rbp

400cf4: 53 push %rbx

400cf5: 48 83 ec 08 sub $0x8,%rsp

400cf9: 80 3d 98 22 20 00 00 cmpb $0x0,2106008(%rip) # 602f98 <completed.6145>

400d00: 75 44 jne 400d46 <\_\_do\_global\_dtors\_aux+0x56>

400d02: b8 80 23 60 00 mov $0x602380,%eax

400d07: 48 2d 78 23 60 00 sub $0x602378,%rax

400d0d: 48 c1 f8 03 sar $0x3,%rax

400d11: 48 8d 58 ff lea 0xffffffffffffffff(%rax),%rbx

400d15: 48 8b 05 74 22 20 00 mov 2105972(%rip),%rax # 602f90 <dtor\_idx.6147>

400d1c: 48 39 c3 cmp %rax,%rbx

400d1f: 76 1e jbe 400d3f <\_\_do\_global\_dtors\_aux+0x4f>

400d21: 48 83 c0 01 add $0x1,%rax

400d25: 48 89 05 64 22 20 00 mov %rax,2105956(%rip) # 602f90 <dtor\_idx.6147>

400d2c: ff 14 c5 78 23 60 00 callq \*0x602378(,%rax,8)

400d33: 48 8b 05 56 22 20 00 mov 2105942(%rip),%rax # 602f90 <dtor\_idx.6147>

400d3a: 48 39 c3 cmp %rax,%rbx

400d3d: 77 e2 ja 400d21 <\_\_do\_global\_dtors\_aux+0x31>

400d3f: c6 05 52 22 20 00 01 movb $0x1,2105938(%rip) # 602f98 <completed.6145>

400d46: 48 83 c4 08 add $0x8,%rsp

400d4a: 5b pop %rbx

400d4b: c9 leaveq

400d4c: c3 retq

400d4d: 0f 1f 00 nopl (%rax)

0000000000400d50 <frame\_dummy>:

400d50: 55 push %rbp

400d51: 48 83 3d 2f 16 20 00 cmpq $0x0,2102831(%rip) # 602388 <\_\_JCR\_END\_\_>

400d58: 00

400d59: 48 89 e5 mov %rsp,%rbp

400d5c: 74 16 je 400d74 <frame\_dummy+0x24>

400d5e: b8 00 00 00 00 mov $0x0,%eax

400d63: 48 85 c0 test %rax,%rax

400d66: 74 0c je 400d74 <frame\_dummy+0x24>

400d68: bf 88 23 60 00 mov $0x602388,%edi

400d6d: 49 89 c3 mov %rax,%r11

400d70: c9 leaveq

400d71: 41 ff e3 jmpq \*%r11

400d74: c9 leaveq

400d75: c3 retq

400d76: 90 nop

400d77: 90 nop

0000000000400d78 <main>:

400d78: 53 push %rbx

400d79: 48 89 f3 mov %rsi,%rbx

400d7c: 83 ff 01 cmp $0x1,%edi

400d7f: 75 10 jne 400d91 <main+0x19>

400d81: 48 8b 05 f8 21 20 00 mov 2105848(%rip),%rax # 602f80 <\_\_bss\_start>

400d88: 48 89 05 11 22 20 00 mov %rax,2105873(%rip) # 602fa0 <infile>

400d8f: eb 56 jmp 400de7 <main+0x6f>

400d91: 83 ff 02 cmp $0x2,%edi

400d94: 75 35 jne 400dcb <main+0x53>

400d96: be f2 1b 40 00 mov $0x401bf2,%esi

400d9b: 48 8b 7b 08 mov 0x8(%rbx),%rdi

400d9f: e8 6c fd ff ff callq 400b10 <fopen@plt>

400da4: 48 89 05 f5 21 20 00 mov %rax,2105845(%rip) # 602fa0 <infile>

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

400dae: 75 37 jne 400de7 <main+0x6f>

400db0: 48 8b 53 08 mov 0x8(%rbx),%rdx

400db4: 48 8b 33 mov (%rbx),%rsi

400db7: bf b0 19 40 00 mov $0x4019b0,%edi

400dbc: e8 ef fc ff ff callq 400ab0 <printf@plt>

400dc1: bf 08 00 00 00 mov $0x8,%edi

400dc6: e8 25 fd ff ff callq 400af0 <exit@plt>

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

400dce: bf cd 19 40 00 mov $0x4019cd,%edi

400dd3: b8 00 00 00 00 mov $0x0,%eax

400dd8: e8 d3 fc ff ff callq 400ab0 <printf@plt>

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

400de2: e8 09 fd ff ff callq 400af0 <exit@plt>

400de7: e8 14 0a 00 00 callq 401800 <initialize\_bomb>

400dec: bf 38 1a 40 00 mov $0x401a38,%edi

400df1: e8 ea fc ff ff callq 400ae0 <puts@plt>

400df6: bf 78 1a 40 00 mov $0x401a78,%edi

400dfb: e8 e0 fc ff ff callq 400ae0 <puts@plt>

400e00: e8 cc 07 00 00 callq 4015d1 <read\_line>

400e05: 48 89 c7 mov %rax,%rdi

400e08: e8 5e 03 00 00 callq 40116b <phase\_1>

400e0d: e8 42 06 00 00 callq 401454 <phase\_defused>

400e12: bf a8 1a 40 00 mov $0x401aa8,%edi

400e17: e8 c4 fc ff ff callq 400ae0 <puts@plt>

400e1c: e8 b0 07 00 00 callq 4015d1 <read\_line>

400e21: 48 89 c7 mov %rax,%rdi

400e24: e8 d1 02 00 00 callq 4010fa <phase\_2>

400e29: e8 26 06 00 00 callq 401454 <phase\_defused>

400e2e: bf e7 19 40 00 mov $0x4019e7,%edi

400e33: e8 a8 fc ff ff callq 400ae0 <puts@plt>

400e38: e8 94 07 00 00 callq 4015d1 <read\_line>

400e3d: 48 89 c7 mov %rax,%rdi

400e40: e8 1f 02 00 00 callq 401064 <phase\_3>

400e45: e8 0a 06 00 00 callq 401454 <phase\_defused>

400e4a: bf 05 1a 40 00 mov $0x401a05,%edi

400e4f: e8 8c fc ff ff callq 400ae0 <puts@plt>

400e54: e8 78 07 00 00 callq 4015d1 <read\_line>

400e59: 48 89 c7 mov %rax,%rdi

400e5c: e8 c0 01 00 00 callq 401021 <phase\_4>

400e61: e8 ee 05 00 00 callq 401454 <phase\_defused>

400e66: bf d8 1a 40 00 mov $0x401ad8,%edi

400e6b: e8 70 fc ff ff callq 400ae0 <puts@plt>

400e70: e8 5c 07 00 00 callq 4015d1 <read\_line>

400e75: 48 89 c7 mov %rax,%rdi

400e78: e8 5d 01 00 00 callq 400fda <phase\_5>

400e7d: e8 d2 05 00 00 callq 401454 <phase\_defused>

400e82: bf 14 1a 40 00 mov $0x401a14,%edi

400e87: e8 54 fc ff ff callq 400ae0 <puts@plt>

400e8c: e8 40 07 00 00 callq 4015d1 <read\_line>

400e91: 48 89 c7 mov %rax,%rdi

400e94: e8 ee 02 00 00 callq 401187 <phase\_6>

400e99: e8 b6 05 00 00 callq 401454 <phase\_defused>

400e9e: b8 00 00 00 00 mov $0x0,%eax

400ea3: 5b pop %rbx

400ea4: c3 retq

400ea5: 90 nop

400ea6: 90 nop

400ea7: 90 nop

400ea8: 90 nop

400ea9: 90 nop

400eaa: 90 nop

400eab: 90 nop

400eac: 90 nop

400ead: 90 nop

400eae: 90 nop

400eaf: 90 nop

0000000000400eb0 <func4>:

400eb0: 48 89 5c 24 f0 mov %rbx,0xfffffffffffffff0(%rsp)

400eb5: 48 89 6c 24 f8 mov %rbp,0xfffffffffffffff8(%rsp)

400eba: 48 83 ec 10 sub $0x10,%rsp

400ebe: 89 fd mov %edi,%ebp

400ec0: b8 01 00 00 00 mov $0x1,%eax

400ec5: 83 ff 01 cmp $0x1,%edi

400ec8: 7e 14 jle 400ede <func4+0x2e>

400eca: 8d 7d ff lea 0xffffffffffffffff(%rbp),%edi

400ecd: e8 de ff ff ff callq 400eb0 <func4>

400ed2: 89 c3 mov %eax,%ebx

400ed4: 8d 7d fe lea 0xfffffffffffffffe(%rbp),%edi

400ed7: e8 d4 ff ff ff callq 400eb0 <func4>

400edc: 01 d8 add %ebx,%eax

400ede: 48 8b 1c 24 mov (%rsp),%rbx

400ee2: 48 8b 6c 24 08 mov 0x8(%rsp),%rbp

400ee7: 48 83 c4 10 add $0x10,%rsp

400eeb: c3 retq

0000000000400eec <fun6>:

400eec: 48 8b 77 08 mov 0x8(%rdi),%rsi

400ef0: 48 c7 47 08 00 00 00 movq $0x0,0x8(%rdi)

400ef7: 00

400ef8: 49 89 f8 mov %rdi,%r8

400efb: 48 89 f8 mov %rdi,%rax

400efe: 48 89 fa mov %rdi,%rdx

400f01: 48 85 f6 test %rsi,%rsi

400f04: 75 36 jne 400f3c <fun6+0x50>

400f06: eb 41 jmp 400f49 <fun6+0x5d>

400f08: 48 89 d0 mov %rdx,%rax

400f0b: 48 8b 52 08 mov 0x8(%rdx),%rdx

400f0f: 48 85 d2 test %rdx,%rdx

400f12: 74 04 je 400f18 <fun6+0x2c>

400f14: 39 0a cmp %ecx,(%rdx)

400f16: 7f f0 jg 400f08 <fun6+0x1c>

400f18: 48 39 d0 cmp %rdx,%rax

400f1b: 75 05 jne 400f22 <fun6+0x36>

400f1d: 49 89 f0 mov %rsi,%r8

400f20: eb 04 jmp 400f26 <fun6+0x3a>

400f22: 48 89 70 08 mov %rsi,0x8(%rax)

400f26: 48 8b 46 08 mov 0x8(%rsi),%rax

400f2a: 48 89 56 08 mov %rdx,0x8(%rsi)

400f2e: 48 89 c6 mov %rax,%rsi

400f31: 4c 89 c2 mov %r8,%rdx

400f34: 4c 89 c0 mov %r8,%rax

400f37: 48 85 f6 test %rsi,%rsi

400f3a: 74 0d je 400f49 <fun6+0x5d>

400f3c: 48 85 d2 test %rdx,%rdx

400f3f: 74 d7 je 400f18 <fun6+0x2c>

400f41: 8b 0e mov (%rsi),%ecx

400f43: 39 0a cmp %ecx,(%rdx)

400f45: 7f c1 jg 400f08 <fun6+0x1c>

400f47: eb cf jmp 400f18 <fun6+0x2c>

400f49: 4c 89 c0 mov %r8,%rax

400f4c: 0f 1f 40 00 nopl 0x0(%rax)

400f50: c3 retq

0000000000400f51 <fun7>:

400f51: b8 ff ff ff ff mov $0xffffffff,%eax

400f56: 48 85 ff test %rdi,%rdi

400f59: 74 28 je 400f83 <fun7+0x32>

400f5b: 8b 17 mov (%rdi),%edx

400f5d: 39 f2 cmp %esi,%edx

400f5f: 7e 0c jle 400f6d <fun7+0x1c>

400f61: 48 8b 7f 08 mov 0x8(%rdi),%rdi

400f65: e8 e7 ff ff ff callq 400f51 <fun7>

400f6a: 01 c0 add %eax,%eax

400f6c: c3 retq

400f6d: b8 00 00 00 00 mov $0x0,%eax

400f72: 39 f2 cmp %esi,%edx

400f74: 74 0d je 400f83 <fun7+0x32>

400f76: 48 8b 7f 10 mov 0x10(%rdi),%rdi

400f7a: e8 d2 ff ff ff callq 400f51 <fun7>

400f7f: 8d 44 00 01 lea 0x1(%rax,%rax,1),%eax

400f83: f3 c3 repz retq

0000000000400f85 <secret\_phase>:

400f85: 53 push %rbx

400f86: e8 46 06 00 00 callq 4015d1 <read\_line>

400f8b: 48 89 c7 mov %rax,%rdi

400f8e: b9 00 00 00 00 mov $0x0,%ecx

400f93: ba 0a 00 00 00 mov $0xa,%edx

400f98: be 00 00 00 00 mov $0x0,%esi

400f9d: e8 fe fb ff ff callq 400ba0 <\_\_strtol\_internal@plt>

400fa2: 89 c3 mov %eax,%ebx

400fa4: 8d 40 ff lea 0xffffffffffffffff(%rax),%eax

400fa7: 3d e8 03 00 00 cmp $0x3e8,%eax

400fac: 76 05 jbe 400fb3 <secret\_phase+0x2e>

400fae: e8 28 05 00 00 callq 4014db <explode\_bomb>

400fb3: 89 de mov %ebx,%esi

400fb5: bf d0 2c 60 00 mov $0x602cd0,%edi

400fba: e8 92 ff ff ff callq 400f51 <fun7>

400fbf: 83 f8 03 cmp $0x3,%eax

400fc2: 74 05 je 400fc9 <secret\_phase+0x44>

400fc4: e8 12 05 00 00 callq 4014db <explode\_bomb>

400fc9: bf 00 1b 40 00 mov $0x401b00,%edi

400fce: e8 0d fb ff ff callq 400ae0 <puts@plt>

400fd3: e8 7c 04 00 00 callq 401454 <phase\_defused>

400fd8: 5b pop %rbx

400fd9: c3 retq

0000000000400fda <phase\_5>:

400fda: 53 push %rbx

400fdb: 48 89 fb mov %rdi,%rbx

400fde: e8 dd 01 00 00 callq 4011c0 <string\_length>

400fe3: 83 f8 06 cmp $0x6,%eax

400fe6: 74 05 je 400fed <phase\_5+0x13>

400fe8: e8 ee 04 00 00 callq 4014db <explode\_bomb>

400fed: b9 00 00 00 00 mov $0x0,%ecx

400ff2: ba 00 00 00 00 mov $0x0,%edx

400ff7: 48 0f be 04 1a movsbq (%rdx,%rbx,1),%rax

400ffc: 83 e0 0f and $0xf,%eax

400fff: 03 0c 85 a0 1b 40 00 add 0x401ba0(,%rax,4),%ecx

401006: 48 83 c2 01 add $0x1,%rdx

40100a: 48 83 fa 06 cmp $0x6,%rdx

40100e: 75 e7 jne 400ff7 <phase\_5+0x1d>

401010: 83 f9 3c cmp $0x3c,%ecx

401013: 74 05 je 40101a <phase\_5+0x40>

401015: e8 c1 04 00 00 callq 4014db <explode\_bomb>

40101a: 5b pop %rbx

40101b: 0f 1f 44 00 00 nopl 0x0(%rax,%rax,1)

401020: c3 retq

0000000000401021 <phase\_4>:

401021: 48 83 ec 18 sub $0x18,%rsp

401025: 48 8d 54 24 14 lea 0x14(%rsp),%rdx

40102a: be 4f 1d 40 00 mov $0x401d4f,%esi

40102f: b8 00 00 00 00 mov $0x0,%eax

401034: e8 77 fb ff ff callq 400bb0 <sscanf@plt>

401039: 83 f8 01 cmp $0x1,%eax

40103c: 75 07 jne 401045 <phase\_4+0x24>

40103e: 83 7c 24 14 00 cmpl $0x0,0x14(%rsp)

401043: 7f 05 jg 40104a <phase\_4+0x29>

401045: e8 91 04 00 00 callq 4014db <explode\_bomb>

40104a: 8b 7c 24 14 mov 0x14(%rsp),%edi

40104e: e8 5d fe ff ff callq 400eb0 <func4>

401053: 3d 62 02 00 00 cmp $0x262,%eax

401058: 74 05 je 40105f <phase\_4+0x3e>

40105a: e8 7c 04 00 00 callq 4014db <explode\_bomb>

40105f: 48 83 c4 18 add $0x18,%rsp

401063: c3 retq

0000000000401064 <phase\_3>:

401064: 48 83 ec 18 sub $0x18,%rsp

401068: 48 8d 4c 24 10 lea 0x10(%rsp),%rcx

40106d: 48 8d 54 24 14 lea 0x14(%rsp),%rdx

401072: be 4c 1d 40 00 mov $0x401d4c,%esi

401077: b8 00 00 00 00 mov $0x0,%eax

40107c: e8 2f fb ff ff callq 400bb0 <sscanf@plt>

401081: 83 f8 01 cmp $0x1,%eax

401084: 7f 05 jg 40108b <phase\_3+0x27>

401086: e8 50 04 00 00 callq 4014db <explode\_bomb>

40108b: 83 7c 24 14 07 cmpl $0x7,0x14(%rsp)

401090: 77 47 ja 4010d9 <phase\_3+0x75>

401092: 8b 44 24 14 mov 0x14(%rsp),%eax

401096: ff 24 c5 60 1b 40 00 jmpq \*0x401b60(,%rax,8)

40109d: b8 e9 01 00 00 mov $0x1e9,%eax

4010a2: eb 46 jmp 4010ea <phase\_3+0x86>

4010a4: b8 16 03 00 00 mov $0x316,%eax

4010a9: eb 3f jmp 4010ea <phase\_3+0x86>

4010ab: b8 b8 00 00 00 mov $0xb8,%eax

4010b0: eb 38 jmp 4010ea <phase\_3+0x86>

4010b2: b8 e3 01 00 00 mov $0x1e3,%eax

4010b7: eb 31 jmp 4010ea <phase\_3+0x86>

4010b9: b8 c7 00 00 00 mov $0xc7,%eax

4010be: 66 90 xchg %ax,%ax

4010c0: eb 28 jmp 4010ea <phase\_3+0x86>

4010c2: b8 d1 00 00 00 mov $0xd1,%eax

4010c7: eb 21 jmp 4010ea <phase\_3+0x86>

4010c9: b8 08 03 00 00 mov $0x308,%eax

4010ce: 66 90 xchg %ax,%ax

4010d0: eb 18 jmp 4010ea <phase\_3+0x86>

4010d2: b8 94 01 00 00 mov $0x194,%eax

4010d7: eb 11 jmp 4010ea <phase\_3+0x86>

4010d9: 0f 1f 80 00 00 00 00 nopl 0x0(%rax)

4010e0: e8 f6 03 00 00 callq 4014db <explode\_bomb>

4010e5: b8 00 00 00 00 mov $0x0,%eax

4010ea: 3b 44 24 10 cmp 0x10(%rsp),%eax

4010ee: 74 05 je 4010f5 <phase\_3+0x91>

4010f0: e8 e6 03 00 00 callq 4014db <explode\_bomb>

4010f5: 48 83 c4 18 add $0x18,%rsp

4010f9: c3 retq

00000000004010fa <phase\_2>:

4010fa: 48 89 5c 24 e0 mov %rbx,0xffffffffffffffe0(%rsp)

4010ff: 48 89 6c 24 e8 mov %rbp,0xffffffffffffffe8(%rsp)

401104: 4c 89 64 24 f0 mov %r12,0xfffffffffffffff0(%rsp)

401109: 4c 89 6c 24 f8 mov %r13,0xfffffffffffffff8(%rsp)

40110e: 48 83 ec 48 sub $0x48,%rsp

401112: 48 89 e3 mov %rsp,%rbx

401115: 48 89 e6 mov %rsp,%rsi

401118: e8 f4 03 00 00 callq 401511 <read\_six\_numbers>

40111d: 41 bc 00 00 00 00 mov $0x0,%r12d

401123: 48 83 c3 0c add $0xc,%rbx

401127: 4c 8d 6c 24 18 lea 0x18(%rsp),%r13

40112c: 48 89 dd mov %rbx,%rbp

40112f: 8b 43 f4 mov 0xfffffffffffffff4(%rbx),%eax

401132: 3b 03 cmp (%rbx),%eax

401134: 74 05 je 40113b <phase\_2+0x41>

401136: e8 a0 03 00 00 callq 4014db <explode\_bomb>

40113b: 44 03 65 f4 add 0xfffffffffffffff4(%rbp),%r12d

40113f: 48 83 c3 04 add $0x4,%rbx

401143: 4c 39 eb cmp %r13,%rbx

401146: 75 e4 jne 40112c <phase\_2+0x32>

401148: 45 85 e4 test %r12d,%r12d

40114b: 75 05 jne 401152 <phase\_2+0x58>

40114d: e8 89 03 00 00 callq 4014db <explode\_bomb>

401152: 48 8b 5c 24 28 mov 0x28(%rsp),%rbx

401157: 48 8b 6c 24 30 mov 0x30(%rsp),%rbp

40115c: 4c 8b 64 24 38 mov 0x38(%rsp),%r12

401161: 4c 8b 6c 24 40 mov 0x40(%rsp),%r13

401166: 48 83 c4 48 add $0x48,%rsp

40116a: c3 retq

000000000040116b <phase\_1>:

40116b: 48 83 ec 08 sub $0x8,%rsp

40116f: be 28 1b 40 00 mov $0x401b28,%esi

401174: e8 66 00 00 00 callq 4011df <strings\_not\_equal>

401179: 85 c0 test %eax,%eax

40117b: 74 05 je 401182 <phase\_1+0x17>

40117d: e8 59 03 00 00 callq 4014db <explode\_bomb>

401182: 48 83 c4 08 add $0x8,%rsp

401186: c3 retq

0000000000401187 <phase\_6>:

401187: 53 push %rbx

401188: b9 00 00 00 00 mov $0x0,%ecx

40118d: ba 0a 00 00 00 mov $0xa,%edx

401192: be 00 00 00 00 mov $0x0,%esi

401197: e8 04 fa ff ff callq 400ba0 <\_\_strtol\_internal@plt>

40119c: 48 89 c3 mov %rax,%rbx

40119f: bf 00 2b 60 00 mov $0x602b00,%edi

4011a4: e8 43 fd ff ff callq 400eec <fun6>

4011a9: 48 8b 40 08 mov 0x8(%rax),%rax

4011ad: 48 8b 40 08 mov 0x8(%rax),%rax

4011b1: 48 8b 40 08 mov 0x8(%rax),%rax

4011b5: 39 18 cmp %ebx,(%rax)

4011b7: 74 05 je 4011be <phase\_6+0x37>

4011b9: e8 1d 03 00 00 callq 4014db <explode\_bomb>

4011be: 5b pop %rbx

4011bf: c3 retq

00000000004011c0 <string\_length>:

4011c0: b8 00 00 00 00 mov $0x0,%eax

4011c5: 80 3f 00 cmpb $0x0,(%rdi)

4011c8: 74 13 je 4011dd <string\_length+0x1d>

4011ca: 48 89 fa mov %rdi,%rdx

4011cd: 0f b6 42 01 movzbl 0x1(%rdx),%eax

4011d1: 48 83 c2 01 add $0x1,%rdx

4011d5: 84 c0 test %al,%al

4011d7: 75 f4 jne 4011cd <string\_length+0xd>

4011d9: 89 d0 mov %edx,%eax

4011db: 29 f8 sub %edi,%eax

4011dd: f3 c3 repz retq

00000000004011df <strings\_not\_equal>:

4011df: 41 54 push %r12

4011e1: 55 push %rbp

4011e2: 53 push %rbx

4011e3: 48 89 fd mov %rdi,%rbp

4011e6: 49 89 f4 mov %rsi,%r12

4011e9: e8 d2 ff ff ff callq 4011c0 <string\_length>

4011ee: 89 c3 mov %eax,%ebx

4011f0: 4c 89 e7 mov %r12,%rdi

4011f3: e8 c8 ff ff ff callq 4011c0 <string\_length>

4011f8: 39 c3 cmp %eax,%ebx

4011fa: 75 32 jne 40122e <strings\_not\_equal+0x4f>

4011fc: 0f b6 45 00 movzbl 0x0(%rbp),%eax

401200: 84 c0 test %al,%al

401202: 74 31 je 401235 <strings\_not\_equal+0x56>

401204: 48 89 e9 mov %rbp,%rcx

401207: 4c 89 e2 mov %r12,%rdx

40120a: 41 3a 04 24 cmp (%r12),%al

40120e: 74 13 je 401223 <strings\_not\_equal+0x44>

401210: eb 1c jmp 40122e <strings\_not\_equal+0x4f>

401212: 0f b6 42 01 movzbl 0x1(%rdx),%eax

401216: 48 83 c1 01 add $0x1,%rcx

40121a: 48 83 c2 01 add $0x1,%rdx

40121e: 40 38 c6 cmp %al,%sil

401221: 75 0b jne 40122e <strings\_not\_equal+0x4f>

401223: 0f b6 71 01 movzbl 0x1(%rcx),%esi

401227: 40 84 f6 test %sil,%sil

40122a: 75 e6 jne 401212 <strings\_not\_equal+0x33>

40122c: eb 07 jmp 401235 <strings\_not\_equal+0x56>

40122e: b8 01 00 00 00 mov $0x1,%eax

401233: eb 05 jmp 40123a <strings\_not\_equal+0x5b>

401235: b8 00 00 00 00 mov $0x0,%eax

40123a: 5b pop %rbx

40123b: 5d pop %rbp

40123c: 41 5c pop %r12

40123e: 66 90 xchg %ax,%ax

401240: c3 retq

0000000000401241 <send\_msg>:

401241: 41 56 push %r14

401243: 41 55 push %r13

401245: 41 54 push %r12

401247: 55 push %rbp

401248: 53 push %rbx

401249: 48 83 ec 60 sub $0x60,%rsp

40124d: 89 fb mov %edi,%ebx

40124f: bf 00 00 00 00 mov $0x0,%edi

401254: e8 d7 f8 ff ff callq 400b30 <dup@plt>

401259: 41 89 c6 mov %eax,%r14d

40125c: 83 f8 ff cmp $0xffffffffffffffff,%eax

40125f: 75 14 jne 401275 <send\_msg+0x34>

401261: bf e0 1b 40 00 mov $0x401be0,%edi

401266: e8 75 f8 ff ff callq 400ae0 <puts@plt>

40126b: bf 08 00 00 00 mov $0x8,%edi

401270: e8 7b f8 ff ff callq 400af0 <exit@plt>

401275: bf 00 00 00 00 mov $0x0,%edi

40127a: e8 41 f8 ff ff callq 400ac0 <close@plt>

40127f: 83 f8 ff cmp $0xffffffffffffffff,%eax

401282: 75 14 jne 401298 <send\_msg+0x57>

401284: bf f4 1b 40 00 mov $0x401bf4,%edi

401289: e8 52 f8 ff ff callq 400ae0 <puts@plt>

40128e: bf 08 00 00 00 mov $0x8,%edi

401293: e8 58 f8 ff ff callq 400af0 <exit@plt>

401298: e8 63 f9 ff ff callq 400c00 <tmpfile@plt>

40129d: 49 89 c4 mov %rax,%r12

4012a0: 48 85 c0 test %rax,%rax

4012a3: 75 14 jne 4012b9 <send\_msg+0x78>

4012a5: bf 07 1c 40 00 mov $0x401c07,%edi

4012aa: e8 31 f8 ff ff callq 400ae0 <puts@plt>

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

4012b4: e8 37 f8 ff ff callq 400af0 <exit@plt>

4012b9: 48 89 c1 mov %rax,%rcx

4012bc: ba 1b 00 00 00 mov $0x1b,%edx

4012c1: be 01 00 00 00 mov $0x1,%esi

4012c6: bf 1c 1c 40 00 mov $0x401c1c,%edi

4012cb: e8 a0 f9 ff ff callq 400c70 <fwrite@plt>

4012d0: 4c 89 e6 mov %r12,%rsi

4012d3: bf 0a 00 00 00 mov $0xa,%edi

4012d8: e8 83 f8 ff ff callq 400b60 <fputc@plt>

4012dd: bf 00 00 00 00 mov $0x0,%edi

4012e2: e8 59 f9 ff ff callq 400c40 <cuserid@plt>

4012e7: 48 85 c0 test %rax,%rax

4012ea: 75 16 jne 401302 <send\_msg+0xc1>

4012ec: c7 44 24 10 6e 6f 62 movl $0x6f626f6e,0x10(%rsp)

4012f3: 6f

4012f4: 66 c7 44 24 14 64 79 movw $0x7964,0x14(%rsp)

4012fb: c6 44 24 16 00 movb $0x0,0x16(%rsp)

401300: eb 0d jmp 40130f <send\_msg+0xce>

401302: 48 8d 7c 24 10 lea 0x10(%rsp),%rdi

401307: 48 89 c6 mov %rax,%rsi

40130a: e8 41 f9 ff ff callq 400c50 <strcpy@plt>

40130f: 85 db test %ebx,%ebx

401311: 41 b9 40 1c 40 00 mov $0x401c40,%r9d

401317: b8 38 1c 40 00 mov $0x401c38,%eax

40131c: 4c 0f 45 c8 cmovne %rax,%r9

401320: 8b 05 76 1c 20 00 mov 2104438(%rip),%eax # 602f9c <num\_input\_strings>

401326: 89 04 24 mov %eax,(%rsp)

401329: 4c 8d 44 24 10 lea 0x10(%rsp),%r8

40132e: 8b 0d 2c 13 20 00 mov 2102060(%rip),%ecx # 602660 <bomb\_id>

401334: ba 80 26 60 00 mov $0x602680,%edx

401339: be 49 1c 40 00 mov $0x401c49,%esi

40133e: 4c 89 e7 mov %r12,%rdi

401341: b8 00 00 00 00 mov $0x0,%eax

401346: e8 35 f9 ff ff callq 400c80 <fprintf@plt>

40134b: 83 3d 4a 1c 20 00 00 cmpl $0x0,2104394(%rip) # 602f9c <num\_input\_strings>

401352: 7e 45 jle 401399 <send\_msg+0x158>

401354: bd c0 2f 60 00 mov $0x602fc0,%ebp

401359: bb 00 00 00 00 mov $0x0,%ebx

40135e: 4c 8d 6c 24 10 lea 0x10(%rsp),%r13

401363: 83 c3 01 add $0x1,%ebx

401366: 48 89 2c 24 mov %rbp,(%rsp)

40136a: 41 89 d9 mov %ebx,%r9d

40136d: 4d 89 e8 mov %r13,%r8

401370: 8b 0d ea 12 20 00 mov 2101994(%rip),%ecx # 602660 <bomb\_id>

401376: ba 80 26 60 00 mov $0x602680,%edx

40137b: be 65 1c 40 00 mov $0x401c65,%esi

401380: 4c 89 e7 mov %r12,%rdi

401383: b8 00 00 00 00 mov $0x0,%eax

401388: e8 f3 f8 ff ff callq 400c80 <fprintf@plt>

40138d: 48 83 c5 50 add $0x50,%rbp

401391: 39 1d 05 1c 20 00 cmp %ebx,2104325(%rip) # 602f9c <num\_input\_strings>

401397: 7f ca jg 401363 <send\_msg+0x122>

401399: 4c 89 e7 mov %r12,%rdi

40139c: e8 2f f8 ff ff callq 400bd0 <rewind@plt>

4013a1: 41 b8 13 1e 40 00 mov $0x401e13,%r8d

4013a7: b9 81 1c 40 00 mov $0x401c81,%ecx

4013ac: ba 88 1c 40 00 mov $0x401c88,%edx

4013b1: be 9f 1c 40 00 mov $0x401c9f,%esi

4013b6: bf 00 36 60 00 mov $0x603600,%edi

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

4013c0: e8 cb f7 ff ff callq 400b90 <sprintf@plt>

4013c5: bf 00 36 60 00 mov $0x603600,%edi

4013ca: e8 71 f7 ff ff callq 400b40 <system@plt>

4013cf: 85 c0 test %eax,%eax

4013d1: 74 14 je 4013e7 <send\_msg+0x1a6>

4013d3: bf a8 1c 40 00 mov $0x401ca8,%edi

4013d8: e8 03 f7 ff ff callq 400ae0 <puts@plt>

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

4013e2: e8 09 f7 ff ff callq 400af0 <exit@plt>

4013e7: 4c 89 e7 mov %r12,%rdi

4013ea: e8 71 f8 ff ff callq 400c60 <fclose@plt>

4013ef: 85 c0 test %eax,%eax

4013f1: 74 14 je 401407 <send\_msg+0x1c6>

4013f3: bf c2 1c 40 00 mov $0x401cc2,%edi

4013f8: e8 e3 f6 ff ff callq 400ae0 <puts@plt>

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

401402: e8 e9 f6 ff ff callq 400af0 <exit@plt>

401407: 44 89 f7 mov %r14d,%edi

40140a: e8 21 f7 ff ff callq 400b30 <dup@plt>

40140f: 85 c0 test %eax,%eax

401411: 74 14 je 401427 <send\_msg+0x1e6>

401413: bf db 1c 40 00 mov $0x401cdb,%edi

401418: e8 c3 f6 ff ff callq 400ae0 <puts@plt>

40141d: bf 08 00 00 00 mov $0x8,%edi

401422: e8 c9 f6 ff ff callq 400af0 <exit@plt>

401427: 44 89 f7 mov %r14d,%edi

40142a: e8 91 f6 ff ff callq 400ac0 <close@plt>

40142f: 85 c0 test %eax,%eax

401431: 74 14 je 401447 <send\_msg+0x206>

401433: bf f6 1c 40 00 mov $0x401cf6,%edi

401438: e8 a3 f6 ff ff callq 400ae0 <puts@plt>

40143d: bf 08 00 00 00 mov $0x8,%edi

401442: e8 a9 f6 ff ff callq 400af0 <exit@plt>

401447: 48 83 c4 60 add $0x60,%rsp

40144b: 5b pop %rbx

40144c: 5d pop %rbp

40144d: 41 5c pop %r12

40144f: 41 5d pop %r13

401451: 41 5e pop %r14

401453: c3 retq

0000000000401454 <phase\_defused>:

401454: 53 push %rbx

401455: 48 83 ec 60 sub $0x60,%rsp

401459: bf 01 00 00 00 mov $0x1,%edi

40145e: e8 de fd ff ff callq 401241 <send\_msg>

401463: 83 3d 32 1b 20 00 06 cmpl $0x6,2104114(%rip) # 602f9c <num\_input\_strings>

40146a: 75 69 jne 4014d5 <phase\_defused+0x81>

40146c: 48 8d 5c 24 10 lea 0x10(%rsp),%rbx

401471: 48 8d 54 24 0c lea 0xc(%rsp),%rdx

401476: 48 89 d9 mov %rbx,%rcx

401479: be 0d 1d 40 00 mov $0x401d0d,%esi

40147e: bf b0 30 60 00 mov $0x6030b0,%edi

401483: b8 00 00 00 00 mov $0x0,%eax

401488: e8 23 f7 ff ff callq 400bb0 <sscanf@plt>

40148d: 83 f8 02 cmp $0x2,%eax

401490: 75 2f jne 4014c1 <phase\_defused+0x6d>

401492: be 13 1d 40 00 mov $0x401d13,%esi

401497: 48 89 df mov %rbx,%rdi

40149a: e8 40 fd ff ff callq 4011df <strings\_not\_equal>

40149f: 85 c0 test %eax,%eax

4014a1: 75 1e jne 4014c1 <phase\_defused+0x6d>

4014a3: bf 50 1e 40 00 mov $0x401e50,%edi

4014a8: e8 33 f6 ff ff callq 400ae0 <puts@plt>

4014ad: bf 78 1e 40 00 mov $0x401e78,%edi

4014b2: e8 29 f6 ff ff callq 400ae0 <puts@plt>

4014b7: b8 00 00 00 00 mov $0x0,%eax

4014bc: e8 c4 fa ff ff callq 400f85 <secret\_phase>

4014c1: bf b0 1e 40 00 mov $0x401eb0,%edi

4014c6: e8 15 f6 ff ff callq 400ae0 <puts@plt>

4014cb: bf e0 1e 40 00 mov $0x401ee0,%edi

4014d0: e8 0b f6 ff ff callq 400ae0 <puts@plt>

4014d5: 48 83 c4 60 add $0x60,%rsp

4014d9: 5b pop %rbx

4014da: c3 retq

00000000004014db <explode\_bomb>:

4014db: 48 83 ec 08 sub $0x8,%rsp

4014df: bf 20 1d 40 00 mov $0x401d20,%edi

4014e4: e8 f7 f5 ff ff callq 400ae0 <puts@plt>

4014e9: bf 29 1d 40 00 mov $0x401d29,%edi

4014ee: e8 ed f5 ff ff callq 400ae0 <puts@plt>

4014f3: bf 00 00 00 00 mov $0x0,%edi

4014f8: e8 44 fd ff ff callq 401241 <send\_msg>

4014fd: bf 28 1f 40 00 mov $0x401f28,%edi

401502: e8 d9 f5 ff ff callq 400ae0 <puts@plt>

401507: bf 08 00 00 00 mov $0x8,%edi

40150c: e8 df f5 ff ff callq 400af0 <exit@plt>

0000000000401511 <read\_six\_numbers>:

401511: 48 83 ec 18 sub $0x18,%rsp

401515: 48 8d 4e 04 lea 0x4(%rsi),%rcx

401519: 48 8d 46 14 lea 0x14(%rsi),%rax

40151d: 48 89 44 24 08 mov %rax,0x8(%rsp)

401522: 48 8d 46 10 lea 0x10(%rsi),%rax

401526: 48 89 04 24 mov %rax,(%rsp)

40152a: 4c 8d 4e 0c lea 0xc(%rsi),%r9

40152e: 4c 8d 46 08 lea 0x8(%rsi),%r8

401532: 48 89 f2 mov %rsi,%rdx

401535: be 40 1d 40 00 mov $0x401d40,%esi

40153a: b8 00 00 00 00 mov $0x0,%eax

40153f: e8 6c f6 ff ff callq 400bb0 <sscanf@plt>

401544: 83 f8 05 cmp $0x5,%eax

401547: 7f 05 jg 40154e <read\_six\_numbers+0x3d>

401549: e8 8d ff ff ff callq 4014db <explode\_bomb>

40154e: 48 83 c4 18 add $0x18,%rsp

401552: c3 retq

0000000000401553 <blank\_line>:

401553: 55 push %rbp

401554: 53 push %rbx

401555: 48 83 ec 08 sub $0x8,%rsp

401559: 48 89 fd mov %rdi,%rbp

40155c: eb 1e jmp 40157c <blank\_line+0x29>

40155e: e8 1d f6 ff ff callq 400b80 <\_\_ctype\_b\_loc@plt>

401563: 48 0f be d3 movsbq %bl,%rdx

401567: 48 8b 00 mov (%rax),%rax

40156a: f6 44 50 01 20 testb $0x20,0x1(%rax,%rdx,2)

40156f: 75 07 jne 401578 <blank\_line+0x25>

401571: b8 00 00 00 00 mov $0x0,%eax

401576: eb 11 jmp 401589 <blank\_line+0x36>

401578: 48 83 c5 01 add $0x1,%rbp

40157c: 0f b6 5d 00 movzbl 0x0(%rbp),%ebx

401580: 84 db test %bl,%bl

401582: 75 da jne 40155e <blank\_line+0xb>

401584: b8 01 00 00 00 mov $0x1,%eax

401589: 48 83 c4 08 add $0x8,%rsp

40158d: 5b pop %rbx

40158e: 5d pop %rbp

40158f: c3 retq

0000000000401590 <skip>:

401590: 53 push %rbx

401591: 48 63 3d 04 1a 20 00 movslq 2103812(%rip),%rdi # 602f9c <num\_input\_strings>

401598: 48 8d 3c bf lea (%rdi,%rdi,4),%rdi

40159c: 48 c1 e7 04 shl $0x4,%rdi

4015a0: 48 81 c7 c0 2f 60 00 add $0x602fc0,%rdi

4015a7: 48 8b 15 f2 19 20 00 mov 2103794(%rip),%rdx # 602fa0 <infile>

4015ae: be 50 00 00 00 mov $0x50,%esi

4015b3: e8 98 f5 ff ff callq 400b50 <fgets@plt>

4015b8: 48 89 c3 mov %rax,%rbx

4015bb: 48 85 c0 test %rax,%rax

4015be: 74 0c je 4015cc <skip+0x3c>

4015c0: 48 89 c7 mov %rax,%rdi

4015c3: e8 8b ff ff ff callq 401553 <blank\_line>

4015c8: 85 c0 test %eax,%eax

4015ca: 75 c5 jne 401591 <skip+0x1>

4015cc: 48 89 d8 mov %rbx,%rax

4015cf: 5b pop %rbx

4015d0: c3 retq

00000000004015d1 <read\_line>:

4015d1: 53 push %rbx

4015d2: b8 00 00 00 00 mov $0x0,%eax

4015d7: e8 b4 ff ff ff callq 401590 <skip>

4015dc: 48 85 c0 test %rax,%rax

4015df: 75 66 jne 401647 <read\_line+0x76>

4015e1: 48 8b 05 98 19 20 00 mov 2103704(%rip),%rax # 602f80 <\_\_bss\_start>

4015e8: 48 39 05 b1 19 20 00 cmp %rax,2103729(%rip) # 602fa0 <infile>

4015ef: 75 11 jne 401602 <read\_line+0x31>

4015f1: bf 52 1d 40 00 mov $0x401d52,%edi

4015f6: e8 e5 f4 ff ff callq 400ae0 <puts@plt>

4015fb: e8 db fe ff ff callq 4014db <explode\_bomb>

401600: eb 45 jmp 401647 <read\_line+0x76>

401602: bf 70 1d 40 00 mov $0x401d70,%edi

401607: e8 24 f6 ff ff callq 400c30 <getenv@plt>

40160c: 48 85 c0 test %rax,%rax

40160f: 74 0a je 40161b <read\_line+0x4a>

401611: bf 00 00 00 00 mov $0x0,%edi

401616: e8 d5 f4 ff ff callq 400af0 <exit@plt>

40161b: 48 8b 05 5e 19 20 00 mov 2103646(%rip),%rax # 602f80 <\_\_bss\_start>

401622: 48 89 05 77 19 20 00 mov %rax,2103671(%rip) # 602fa0 <infile>

401629: b8 00 00 00 00 mov $0x0,%eax

40162e: e8 5d ff ff ff callq 401590 <skip>

401633: 48 85 c0 test %rax,%rax

401636: 75 0f jne 401647 <read\_line+0x76>

401638: bf 52 1d 40 00 mov $0x401d52,%edi

40163d: e8 9e f4 ff ff callq 400ae0 <puts@plt>

401642: e8 94 fe ff ff callq 4014db <explode\_bomb>

401647: 48 63 05 4e 19 20 00 movslq 2103630(%rip),%rax # 602f9c <num\_input\_strings>

40164e: 48 8d 04 80 lea (%rax,%rax,4),%rax

401652: 48 c1 e0 04 shl $0x4,%rax

401656: 48 8d b8 c0 2f 60 00 lea 0x602fc0(%rax),%rdi

40165d: fc cld

40165e: 48 c7 c1 ff ff ff ff mov $0xffffffffffffffff,%rcx

401665: b8 00 00 00 00 mov $0x0,%eax

40166a: f2 ae repnz scas %es:(%rdi),%al

40166c: 48 f7 d1 not %rcx

40166f: 8d 59 ff lea 0xffffffffffffffff(%rcx),%ebx

401672: 83 fb 4f cmp $0x4f,%ebx

401675: 75 0f jne 401686 <read\_line+0xb5>

401677: bf 7b 1d 40 00 mov $0x401d7b,%edi

40167c: e8 5f f4 ff ff callq 400ae0 <puts@plt>

401681: e8 55 fe ff ff callq 4014db <explode\_bomb>

401686: 8b 0d 10 19 20 00 mov 2103568(%rip),%ecx # 602f9c <num\_input\_strings>

40168c: 8d 53 ff lea 0xffffffffffffffff(%rbx),%edx

40168f: 48 63 d2 movslq %edx,%rdx

401692: 48 63 c1 movslq %ecx,%rax

401695: 48 8d 04 80 lea (%rax,%rax,4),%rax

401699: 48 c1 e0 04 shl $0x4,%rax

40169d: 48 05 c0 2f 60 00 add $0x602fc0,%rax

4016a3: c6 04 10 00 movb $0x0,(%rax,%rdx,1)

4016a7: 83 c1 01 add $0x1,%ecx

4016aa: 89 0d ec 18 20 00 mov %ecx,2103532(%rip) # 602f9c <num\_input\_strings>

4016b0: 5b pop %rbx

4016b1: c3 retq

00000000004016b2 <invalid\_phase>:

4016b2: 48 83 ec 08 sub $0x8,%rsp

4016b6: 48 89 fe mov %rdi,%rsi

4016b9: bf 96 1d 40 00 mov $0x401d96,%edi

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

4016c3: e8 e8 f3 ff ff callq 400ab0 <printf@plt>

4016c8: bf 08 00 00 00 mov $0x8,%edi

4016cd: e8 1e f4 ff ff callq 400af0 <exit@plt>

00000000004016d2 <sig\_handler>:

4016d2: 48 83 ec 08 sub $0x8,%rsp

4016d6: bf 50 1f 40 00 mov $0x401f50,%edi

4016db: e8 00 f4 ff ff callq 400ae0 <puts@plt>

4016e0: bf 03 00 00 00 mov $0x3,%edi

4016e5: e8 d6 f4 ff ff callq 400bc0 <sleep@plt>

4016ea: bf a7 1d 40 00 mov $0x401da7,%edi

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

4016f4: e8 b7 f3 ff ff callq 400ab0 <printf@plt>

4016f9: 48 8b 3d 88 18 20 00 mov 2103432(%rip),%rdi # 602f88 <stdout@@GLIBC\_2.2.5\>

401700: e8 8b f5 ff ff callq 400c90 <fflush@plt>

401705: bf 01 00 00 00 mov $0x1,%edi

40170a: e8 b1 f4 ff ff callq 400bc0 <sleep@plt>

40170f: bf af 1d 40 00 mov $0x401daf,%edi

401714: e8 c7 f3 ff ff callq 400ae0 <puts@plt>

401719: bf 10 00 00 00 mov $0x10,%edi

40171e: e8 cd f3 ff ff callq 400af0 <exit@plt>

0000000000401723 <open\_clientfd>:

401723: 48 89 5c 24 e8 mov %rbx,0xffffffffffffffe8(%rsp)

401728: 48 89 6c 24 f0 mov %rbp,0xfffffffffffffff0(%rsp)

40172d: 4c 89 64 24 f8 mov %r12,0xfffffffffffffff8(%rsp)

401732: 48 83 ec 28 sub $0x28,%rsp

401736: 48 89 fb mov %rdi,%rbx

401739: 41 89 f4 mov %esi,%r12d

40173c: ba 00 00 00 00 mov $0x0,%edx

401741: be 01 00 00 00 mov $0x1,%esi

401746: bf 02 00 00 00 mov $0x2,%edi

40174b: e8 d0 f4 ff ff callq 400c20 <socket@plt>

401750: 89 c5 mov %eax,%ebp

401752: 85 c0 test %eax,%eax

401754: 79 14 jns 40176a <open\_clientfd+0x47>

401756: bf b7 1d 40 00 mov $0x401db7,%edi

40175b: e8 80 f3 ff ff callq 400ae0 <puts@plt>

401760: bf 08 00 00 00 mov $0x8,%edi

401765: e8 86 f3 ff ff callq 400af0 <exit@plt>

40176a: 48 89 df mov %rbx,%rdi

40176d: e8 5e f3 ff ff callq 400ad0 <gethostbyname@plt>

401772: 48 85 c0 test %rax,%rax

401775: 75 14 jne 40178b <open\_clientfd+0x68>

401777: bf c5 1d 40 00 mov $0x401dc5,%edi

40177c: e8 5f f3 ff ff callq 400ae0 <puts@plt>

401781: bf 08 00 00 00 mov $0x8,%edi

401786: e8 65 f3 ff ff callq 400af0 <exit@plt>

40178b: 48 c7 04 24 00 00 00 movq $0x0,(%rsp)

401792: 00

401793: 48 c7 44 24 08 00 00 movq $0x0,0x8(%rsp)

40179a: 00 00

40179c: 66 c7 04 24 02 00 movw $0x2,(%rsp)

4017a2: 48 8d 74 24 04 lea 0x4(%rsp),%rsi

4017a7: 48 63 50 14 movslq 0x14(%rax),%rdx

4017ab: 48 8b 40 18 mov 0x18(%rax),%rax

4017af: 48 8b 38 mov (%rax),%rdi

4017b2: e8 b9 f3 ff ff callq 400b70 <bcopy@plt>

4017b7: 44 89 e0 mov %r12d,%eax

4017ba: 66 c1 c8 08 ror $0x8,%ax

4017be: 66 89 44 24 02 mov %ax,0x2(%rsp)

4017c3: ba 10 00 00 00 mov $0x10,%edx

4017c8: 48 89 e6 mov %rsp,%rsi

4017cb: 89 ef mov %ebp,%edi

4017cd: e8 0e f4 ff ff callq 400be0 <connect@plt>

4017d2: 85 c0 test %eax,%eax

4017d4: 79 14 jns 4017ea <open\_clientfd+0xc7>

4017d6: bf d3 1d 40 00 mov $0x401dd3,%edi

4017db: e8 00 f3 ff ff callq 400ae0 <puts@plt>

4017e0: bf 08 00 00 00 mov $0x8,%edi

4017e5: e8 06 f3 ff ff callq 400af0 <exit@plt>

4017ea: 89 e8 mov %ebp,%eax

4017ec: 48 8b 5c 24 10 mov 0x10(%rsp),%rbx

4017f1: 48 8b 6c 24 18 mov 0x18(%rsp),%rbp

4017f6: 4c 8b 64 24 20 mov 0x20(%rsp),%r12

4017fb: 48 83 c4 28 add $0x28,%rsp

4017ff: c3 retq

0000000000401800 <initialize\_bomb>:

401800: 55 push %rbp

401801: 53 push %rbx

401802: 48 83 ec 48 sub $0x48,%rsp

401806: be d2 16 40 00 mov $0x4016d2,%esi

40180b: bf 02 00 00 00 mov $0x2,%edi

401810: e8 fb f3 ff ff callq 400c10 <signal@plt>

401815: 48 89 e7 mov %rsp,%rdi

401818: be 40 00 00 00 mov $0x40,%esi

40181d: e8 ce f3 ff ff callq 400bf0 <gethostname@plt>

401822: 85 c0 test %eax,%eax

401824: 75 13 jne 401839 <initialize\_bomb+0x39>

401826: 48 8b 3d d3 14 20 00 mov 2102483(%rip),%rdi # 602d00 <host\_table>

40182d: bb 00 00 00 00 mov $0x0,%ebx

401832: 48 85 ff test %rdi,%rdi

401835: 75 16 jne 40184d <initialize\_bomb+0x4d>

401837: eb 50 jmp 401889 <initialize\_bomb+0x89>

401839: bf e1 1d 40 00 mov $0x401de1,%edi

40183e: e8 9d f2 ff ff callq 400ae0 <puts@plt>

401843: bf 08 00 00 00 mov $0x8,%edi

401848: e8 a3 f2 ff ff callq 400af0 <exit@plt>

40184d: 48 89 e6 mov %rsp,%rsi

401850: e8 ab f2 ff ff callq 400b00 <strcasecmp@plt>

401855: 85 c0 test %eax,%eax

401857: 74 13 je 40186c <initialize\_bomb+0x6c>

401859: 48 8b 3c dd 08 2d 60 mov 0x602d08(,%rbx,8),%rdi

401860: 00

401861: 48 83 c3 01 add $0x1,%rbx

401865: 48 85 ff test %rdi,%rdi

401868: 74 1f je 401889 <initialize\_bomb+0x89>

40186a: eb e1 jmp 40184d <initialize\_bomb+0x4d>

40186c: be 50 00 00 00 mov $0x50,%esi

401871: bf ee 1d 40 00 mov $0x401dee,%edi

401876: e8 a8 fe ff ff callq 401723 <open\_clientfd>

40187b: 89 c7 mov %eax,%edi

40187d: e8 3e f2 ff ff callq 400ac0 <close@plt>

401882: 48 83 c4 48 add $0x48,%rsp

401886: 5b pop %rbx

401887: 5d pop %rbp

401888: c3 retq

401889: bf fc 1d 40 00 mov $0x401dfc,%edi

40188e: e8 4d f2 ff ff callq 400ae0 <puts@plt>

401893: bf 08 00 00 00 mov $0x8,%edi

401898: e8 53 f2 ff ff callq 400af0 <exit@plt>

40189d: 90 nop

40189e: 90 nop

40189f: 90 nop

00000000004018a0 <\_\_libc\_csu\_fini>:

4018a0: f3 c3 repz retq

4018a2: 0f 1f 80 00 00 00 00 nopl 0x0(%rax)

4018a9: 0f 1f 80 00 00 00 00 nopl 0x0(%rax)

00000000004018b0 <\_\_libc\_csu\_init>:

4018b0: 4c 89 64 24 e0 mov %r12,0xffffffffffffffe0(%rsp)

4018b5: 4c 89 6c 24 e8 mov %r13,0xffffffffffffffe8(%rsp)

4018ba: 4c 8d 25 a3 0a 20 00 lea 2099875(%rip),%r12 # 602364 <\_\_fini\_array\_end>

4018c1: 4c 89 74 24 f0 mov %r14,0xfffffffffffffff0(%rsp)

4018c6: 4c 89 7c 24 f8 mov %r15,0xfffffffffffffff8(%rsp)

4018cb: 49 89 f6 mov %rsi,%r14

4018ce: 48 89 5c 24 d0 mov %rbx,0xffffffffffffffd0(%rsp)

4018d3: 48 89 6c 24 d8 mov %rbp,0xffffffffffffffd8(%rsp)

4018d8: 48 83 ec 38 sub $0x38,%rsp

4018dc: 41 89 ff mov %edi,%r15d

4018df: 49 89 d5 mov %rdx,%r13

4018e2: e8 a1 f1 ff ff callq 400a88 <\_init>

4018e7: 48 8d 05 76 0a 20 00 lea 2099830(%rip),%rax # 602364 <\_\_fini\_array\_end>

4018ee: 49 29 c4 sub %rax,%r12

4018f1: 49 c1 fc 03 sar $0x3,%r12

4018f5: 4d 85 e4 test %r12,%r12

4018f8: 74 1e je 401918 <\_\_libc\_csu\_init+0x68>

4018fa: 31 ed xor %ebp,%ebp

4018fc: 48 89 c3 mov %rax,%rbx

4018ff: 90 nop

401900: 48 83 c5 01 add $0x1,%rbp

401904: 4c 89 ea mov %r13,%rdx

401907: 4c 89 f6 mov %r14,%rsi

40190a: 44 89 ff mov %r15d,%edi

40190d: ff 13 callq \*(%rbx)

40190f: 48 83 c3 08 add $0x8,%rbx

401913: 49 39 ec cmp %rbp,%r12

401916: 75 e8 jne 401900 <\_\_libc\_csu\_init+0x50>

401918: 48 8b 5c 24 08 mov 0x8(%rsp),%rbx

40191d: 48 8b 6c 24 10 mov 0x10(%rsp),%rbp

401922: 4c 8b 64 24 18 mov 0x18(%rsp),%r12

401927: 4c 8b 6c 24 20 mov 0x20(%rsp),%r13

40192c: 4c 8b 74 24 28 mov 0x28(%rsp),%r14

401931: 4c 8b 7c 24 30 mov 0x30(%rsp),%r15

401936: 48 83 c4 38 add $0x38,%rsp

40193a: c3 retq

40193b: 90 nop

40193c: 90 nop

40193d: 90 nop

40193e: 90 nop

40193f: 90 nop

0000000000401940 <\_\_do\_global\_ctors\_aux>:

401940: 55 push %rbp

401941: 48 89 e5 mov %rsp,%rbp

401944: 53 push %rbx

401945: bb 68 23 60 00 mov $0x602368,%ebx

40194a: 48 83 ec 08 sub $0x8,%rsp

40194e: 48 8b 05 13 0a 20 00 mov 2099731(%rip),%rax # 602368 <\_\_CTOR\_LIST\_\_>

401955: 48 83 f8 ff cmp $0xffffffffffffffff,%rax

401959: 74 14 je 40196f <\_\_do\_global\_ctors\_aux+0x2f>

40195b: 0f 1f 44 00 00 nopl 0x0(%rax,%rax,1)

401960: 48 83 eb 08 sub $0x8,%rbx

401964: ff d0 callq \*%rax

401966: 48 8b 03 mov (%rbx),%rax

401969: 48 83 f8 ff cmp $0xffffffffffffffff,%rax

40196d: 75 f1 jne 401960 <\_\_do\_global\_ctors\_aux+0x20>

40196f: 48 83 c4 08 add $0x8,%rsp

401973: 5b pop %rbx

401974: c9 leaveq

401975: c3 retq

401976: 90 nop

401977: 90 nop

Disassembly of section .fini:

0000000000401978 <\_fini>:

401978: 48 83 ec 08 sub $0x8,%rsp

40197c: e8 6f f3 ff ff callq 400cf0 <\_\_do\_global\_dtors\_aux>

401981: 48 83 c4 08 add $0x8,%rsp

401985: c3 retq