bomb: file format elf32-i386

Disassembly of section .init:

08049000 <\_init>:

8049000: 53 push %ebx

8049001: 83 ec 08 sub $0x8,%esp

8049004: e8 67 01 00 00 call 8049170 <\_\_x86.get\_pc\_thunk.bx>

8049009: 81 c3 f7 2f 00 00 add $0x2ff7,%ebx

804900f: 8b 83 fc ff ff ff mov -0x4(%ebx),%eax

8049015: 85 c0 test %eax,%eax

8049017: 74 02 je 804901b <\_init+0x1b>

8049019: ff d0 call \*%eax

804901b: 83 c4 08 add $0x8,%esp

804901e: 5b pop %ebx

804901f: c3 ret

Disassembly of section .plt:

08049020 <.plt>:

8049020: ff 35 04 c0 04 08 pushl 0x804c004

8049026: ff 25 08 c0 04 08 jmp \*0x804c008

804902c: 00 00 add %al,(%eax)

...

08049030 <printf@plt>:

8049030: ff 25 0c c0 04 08 jmp \*0x804c00c

8049036: 68 00 00 00 00 push $0x0

804903b: e9 e0 ff ff ff jmp 8049020 <.plt>

08049040 <fflush@plt>:

8049040: ff 25 10 c0 04 08 jmp \*0x804c010

8049046: 68 08 00 00 00 push $0x8

804904b: e9 d0 ff ff ff jmp 8049020 <.plt>

08049050 <fgets@plt>:

8049050: ff 25 14 c0 04 08 jmp \*0x804c014

8049056: 68 10 00 00 00 push $0x10

804905b: e9 c0 ff ff ff jmp 8049020 <.plt>

08049060 <signal@plt>:

8049060: ff 25 18 c0 04 08 jmp \*0x804c018

8049066: 68 18 00 00 00 push $0x18

804906b: e9 b0 ff ff ff jmp 8049020 <.plt>

08049070 <sleep@plt>:

8049070: ff 25 1c c0 04 08 jmp \*0x804c01c

8049076: 68 20 00 00 00 push $0x20

804907b: e9 a0 ff ff ff jmp 8049020 <.plt>

08049080 <getenv@plt>:

8049080: ff 25 20 c0 04 08 jmp \*0x804c020

8049086: 68 28 00 00 00 push $0x28

804908b: e9 90 ff ff ff jmp 8049020 <.plt>

08049090 <puts@plt>:

8049090: ff 25 24 c0 04 08 jmp \*0x804c024

8049096: 68 30 00 00 00 push $0x30

804909b: e9 80 ff ff ff jmp 8049020 <.plt>

080490a0 <exit@plt>:

80490a0: ff 25 28 c0 04 08 jmp \*0x804c028

80490a6: 68 38 00 00 00 push $0x38

80490ab: e9 70 ff ff ff jmp 8049020 <.plt>

080490b0 <strlen@plt>:

80490b0: ff 25 2c c0 04 08 jmp \*0x804c02c

80490b6: 68 40 00 00 00 push $0x40

80490bb: e9 60 ff ff ff jmp 8049020 <.plt>

080490c0 <\_\_libc\_start\_main@plt>:

80490c0: ff 25 30 c0 04 08 jmp \*0x804c030

80490c6: 68 48 00 00 00 push $0x48

80490cb: e9 50 ff ff ff jmp 8049020 <.plt>

080490d0 <\_\_isoc99\_sscanf@plt>:

80490d0: ff 25 34 c0 04 08 jmp \*0x804c034

80490d6: 68 50 00 00 00 push $0x50

80490db: e9 40 ff ff ff jmp 8049020 <.plt>

080490e0 <fopen@plt>:

80490e0: ff 25 38 c0 04 08 jmp \*0x804c038

80490e6: 68 58 00 00 00 push $0x58

80490eb: e9 30 ff ff ff jmp 8049020 <.plt>

080490f0 <strtok@plt>:

80490f0: ff 25 3c c0 04 08 jmp \*0x804c03c

80490f6: 68 60 00 00 00 push $0x60

80490fb: e9 20 ff ff ff jmp 8049020 <.plt>

08049100 <atoi@plt>:

8049100: ff 25 40 c0 04 08 jmp \*0x804c040

8049106: 68 68 00 00 00 push $0x68

804910b: e9 10 ff ff ff jmp 8049020 <.plt>

08049110 <\_\_ctype\_b\_loc@plt>:

8049110: ff 25 44 c0 04 08 jmp \*0x804c044

8049116: 68 70 00 00 00 push $0x70

804911b: e9 00 ff ff ff jmp 8049020 <.plt>

Disassembly of section .text:

08049120 <\_start>:

8049120: 31 ed xor %ebp,%ebp

8049122: 5e pop %esi

8049123: 89 e1 mov %esp,%ecx

8049125: 83 e4 f0 and $0xfffffff0,%esp

8049128: 50 push %eax

8049129: 54 push %esp

804912a: 52 push %edx

804912b: e8 23 00 00 00 call 8049153 <\_start+0x33>

8049130: 81 c3 d0 2e 00 00 add $0x2ed0,%ebx

8049136: 8d 83 c0 df ff ff lea -0x2040(%ebx),%eax

804913c: 50 push %eax

804913d: 8d 83 60 df ff ff lea -0x20a0(%ebx),%eax

8049143: 50 push %eax

8049144: 51 push %ecx

8049145: 56 push %esi

8049146: c7 c0 32 92 04 08 mov $0x8049232,%eax

804914c: 50 push %eax

804914d: e8 6e ff ff ff call 80490c0 <\_\_libc\_start\_main@plt>

8049152: f4 hlt

8049153: 8b 1c 24 mov (%esp),%ebx

8049156: c3 ret

8049157: 66 90 xchg %ax,%ax

8049159: 66 90 xchg %ax,%ax

804915b: 66 90 xchg %ax,%ax

804915d: 66 90 xchg %ax,%ax

804915f: 90 nop

08049160 <\_dl\_relocate\_static\_pie>:

8049160: c3 ret

8049161: 66 90 xchg %ax,%ax

8049163: 66 90 xchg %ax,%ax

8049165: 66 90 xchg %ax,%ax

8049167: 66 90 xchg %ax,%ax

8049169: 66 90 xchg %ax,%ax

804916b: 66 90 xchg %ax,%ax

804916d: 66 90 xchg %ax,%ax

804916f: 90 nop

08049170 <\_\_x86.get\_pc\_thunk.bx>:

8049170: 8b 1c 24 mov (%esp),%ebx

8049173: c3 ret

8049174: 66 90 xchg %ax,%ax

8049176: 66 90 xchg %ax,%ax

8049178: 66 90 xchg %ax,%ax

804917a: 66 90 xchg %ax,%ax

804917c: 66 90 xchg %ax,%ax

804917e: 66 90 xchg %ax,%ax

08049180 <deregister\_tm\_clones>:

8049180: b8 a0 c2 04 08 mov $0x804c2a0,%eax

8049185: 3d a0 c2 04 08 cmp $0x804c2a0,%eax

804918a: 74 24 je 80491b0 <deregister\_tm\_clones+0x30>

804918c: b8 00 00 00 00 mov $0x0,%eax

8049191: 85 c0 test %eax,%eax

8049193: 74 1b je 80491b0 <deregister\_tm\_clones+0x30>

8049195: 55 push %ebp

8049196: 89 e5 mov %esp,%ebp

8049198: 83 ec 14 sub $0x14,%esp

804919b: 68 a0 c2 04 08 push $0x804c2a0

80491a0: ff d0 call \*%eax

80491a2: 83 c4 10 add $0x10,%esp

80491a5: c9 leave

80491a6: c3 ret

80491a7: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi

80491ae: 66 90 xchg %ax,%ax

80491b0: c3 ret

80491b1: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi

80491b8: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi

80491bf: 90 nop

080491c0 <register\_tm\_clones>:

80491c0: b8 a0 c2 04 08 mov $0x804c2a0,%eax

80491c5: 2d a0 c2 04 08 sub $0x804c2a0,%eax

80491ca: c1 f8 02 sar $0x2,%eax

80491cd: 89 c2 mov %eax,%edx

80491cf: c1 ea 1f shr $0x1f,%edx

80491d2: 01 d0 add %edx,%eax

80491d4: d1 f8 sar %eax

80491d6: 74 20 je 80491f8 <register\_tm\_clones+0x38>

80491d8: ba 00 00 00 00 mov $0x0,%edx

80491dd: 85 d2 test %edx,%edx

80491df: 74 17 je 80491f8 <register\_tm\_clones+0x38>

80491e1: 55 push %ebp

80491e2: 89 e5 mov %esp,%ebp

80491e4: 83 ec 10 sub $0x10,%esp

80491e7: 50 push %eax

80491e8: 68 a0 c2 04 08 push $0x804c2a0

80491ed: ff d2 call \*%edx

80491ef: 83 c4 10 add $0x10,%esp

80491f2: c9 leave

80491f3: c3 ret

80491f4: 8d 74 26 00 lea 0x0(%esi,%eiz,1),%esi

80491f8: c3 ret

80491f9: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi

08049200 <\_\_do\_global\_dtors\_aux>:

8049200: 80 3d a8 c2 04 08 00 cmpb $0x0,0x804c2a8

8049207: 75 17 jne 8049220 <\_\_do\_global\_dtors\_aux+0x20>

8049209: 55 push %ebp

804920a: 89 e5 mov %esp,%ebp

804920c: 83 ec 08 sub $0x8,%esp

804920f: e8 6c ff ff ff call 8049180 <deregister\_tm\_clones>

8049214: c6 05 a8 c2 04 08 01 movb $0x1,0x804c2a8

804921b: c9 leave

804921c: c3 ret

804921d: 8d 76 00 lea 0x0(%esi),%esi

8049220: c3 ret

8049221: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi

8049228: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi

804922f: 90 nop

08049230 <frame\_dummy>:

8049230: eb 8e jmp 80491c0 <register\_tm\_clones>

08049232 <main>:

8049232: 8d 4c 24 04 lea 0x4(%esp),%ecx

8049236: 83 e4 f0 and $0xfffffff0,%esp

8049239: ff 71 fc pushl -0x4(%ecx)

804923c: 55 push %ebp

804923d: 89 e5 mov %esp,%ebp

804923f: 53 push %ebx

8049240: 51 push %ecx

8049241: 83 ec 10 sub $0x10,%esp

8049244: 89 cb mov %ecx,%ebx

8049246: 83 3b 01 cmpl $0x1,(%ebx)

8049249: 75 0c jne 8049257 <main+0x25>

804924b: a1 a0 c2 04 08 mov 0x804c2a0,%eax

8049250: a3 b0 c2 04 08 mov %eax,0x804c2b0

8049255: eb 75 jmp 80492cc <main+0x9a>

8049257: 83 3b 02 cmpl $0x2,(%ebx)

804925a: 75 50 jne 80492ac <main+0x7a>

804925c: 8b 43 04 mov 0x4(%ebx),%eax

804925f: 83 c0 04 add $0x4,%eax

8049262: 8b 00 mov (%eax),%eax

8049264: 83 ec 08 sub $0x8,%esp

8049267: 68 08 a0 04 08 push $0x804a008

804926c: 50 push %eax

804926d: e8 6e fe ff ff call 80490e0 <fopen@plt>

8049272: 83 c4 10 add $0x10,%esp

8049275: a3 b0 c2 04 08 mov %eax,0x804c2b0

804927a: a1 b0 c2 04 08 mov 0x804c2b0,%eax

804927f: 85 c0 test %eax,%eax

8049281: 75 49 jne 80492cc <main+0x9a>

8049283: 8b 43 04 mov 0x4(%ebx),%eax

8049286: 83 c0 04 add $0x4,%eax

8049289: 8b 10 mov (%eax),%edx

804928b: 8b 43 04 mov 0x4(%ebx),%eax

804928e: 8b 00 mov (%eax),%eax

8049290: 83 ec 04 sub $0x4,%esp

8049293: 52 push %edx

8049294: 50 push %eax

8049295: 68 0a a0 04 08 push $0x804a00a

804929a: e8 91 fd ff ff call 8049030 <printf@plt>

804929f: 83 c4 10 add $0x10,%esp

80492a2: 83 ec 0c sub $0xc,%esp

80492a5: 6a 08 push $0x8

80492a7: e8 f4 fd ff ff call 80490a0 <exit@plt>

80492ac: 8b 43 04 mov 0x4(%ebx),%eax

80492af: 8b 00 mov (%eax),%eax

80492b1: 83 ec 08 sub $0x8,%esp

80492b4: 50 push %eax

80492b5: 68 27 a0 04 08 push $0x804a027

80492ba: e8 71 fd ff ff call 8049030 <printf@plt>

80492bf: 83 c4 10 add $0x10,%esp

80492c2: 83 ec 0c sub $0xc,%esp

80492c5: 6a 08 push $0x8

80492c7: e8 d4 fd ff ff call 80490a0 <exit@plt>

80492cc: e8 dc 09 00 00 call 8049cad <initialize\_bomb>

80492d1: 83 ec 0c sub $0xc,%esp

80492d4: 68 44 a0 04 08 push $0x804a044

80492d9: e8 b2 fd ff ff call 8049090 <puts@plt>

80492de: 83 c4 10 add $0x10,%esp

80492e1: 83 ec 0c sub $0xc,%esp

80492e4: 68 80 a0 04 08 push $0x804a080

80492e9: e8 a2 fd ff ff call 8049090 <puts@plt>

80492ee: 83 c4 10 add $0x10,%esp

80492f1: e8 71 0a 00 00 call 8049d67 <read\_line>

80492f6: 89 45 f4 mov %eax,-0xc(%ebp)

80492f9: 83 ec 0c sub $0xc,%esp

80492fc: ff 75 f4 pushl -0xc(%ebp)

80492ff: e8 54 01 00 00 call 8049458 <phase\_0>

8049304: 83 c4 10 add $0x10,%esp

8049307: 85 c0 test %eax,%eax

8049309: 74 15 je 8049320 <main+0xee>

804930b: e8 c3 0b 00 00 call 8049ed3 <phase\_defused>

8049310: 83 ec 0c sub $0xc,%esp

8049313: 68 ac a0 04 08 push $0x804a0ac

8049318: e8 73 fd ff ff call 8049090 <puts@plt>

804931d: 83 c4 10 add $0x10,%esp

8049320: e8 42 0a 00 00 call 8049d67 <read\_line>

8049325: 89 45 f4 mov %eax,-0xc(%ebp)

8049328: 83 ec 0c sub $0xc,%esp

804932b: ff 75 f4 pushl -0xc(%ebp)

804932e: e8 55 01 00 00 call 8049488 <phase\_1>

8049333: 83 c4 10 add $0x10,%esp

8049336: 85 c0 test %eax,%eax

8049338: 74 15 je 804934f <main+0x11d>

804933a: e8 94 0b 00 00 call 8049ed3 <phase\_defused>

804933f: 83 ec 0c sub $0xc,%esp

8049342: 68 d4 a0 04 08 push $0x804a0d4

8049347: e8 44 fd ff ff call 8049090 <puts@plt>

804934c: 83 c4 10 add $0x10,%esp

804934f: e8 13 0a 00 00 call 8049d67 <read\_line>

8049354: 89 45 f4 mov %eax,-0xc(%ebp)

8049357: 83 ec 0c sub $0xc,%esp

804935a: ff 75 f4 pushl -0xc(%ebp)

804935d: e8 98 01 00 00 call 80494fa <phase\_2>

8049362: 83 c4 10 add $0x10,%esp

8049365: 85 c0 test %eax,%eax

8049367: 74 15 je 804937e <main+0x14c>

8049369: e8 65 0b 00 00 call 8049ed3 <phase\_defused>

804936e: 83 ec 0c sub $0xc,%esp

8049371: 68 fd a0 04 08 push $0x804a0fd

8049376: e8 15 fd ff ff call 8049090 <puts@plt>

804937b: 83 c4 10 add $0x10,%esp

804937e: e8 e4 09 00 00 call 8049d67 <read\_line>

8049383: 89 45 f4 mov %eax,-0xc(%ebp)

8049386: 83 ec 0c sub $0xc,%esp

8049389: ff 75 f4 pushl -0xc(%ebp)

804938c: e8 f5 01 00 00 call 8049586 <phase\_3>

8049391: 83 c4 10 add $0x10,%esp

8049394: 85 c0 test %eax,%eax

8049396: 74 15 je 80493ad <main+0x17b>

8049398: e8 36 0b 00 00 call 8049ed3 <phase\_defused>

804939d: 83 ec 0c sub $0xc,%esp

80493a0: 68 1b a1 04 08 push $0x804a11b

80493a5: e8 e6 fc ff ff call 8049090 <puts@plt>

80493aa: 83 c4 10 add $0x10,%esp

80493ad: e8 b5 09 00 00 call 8049d67 <read\_line>

80493b2: 89 45 f4 mov %eax,-0xc(%ebp)

80493b5: 83 ec 0c sub $0xc,%esp

80493b8: ff 75 f4 pushl -0xc(%ebp)

80493bb: e8 ff 02 00 00 call 80496bf <phase\_4>

80493c0: 83 c4 10 add $0x10,%esp

80493c3: 85 c0 test %eax,%eax

80493c5: 74 15 je 80493dc <main+0x1aa>

80493c7: e8 07 0b 00 00 call 8049ed3 <phase\_defused>

80493cc: 83 ec 0c sub $0xc,%esp

80493cf: 68 2c a1 04 08 push $0x804a12c

80493d4: e8 b7 fc ff ff call 8049090 <puts@plt>

80493d9: 83 c4 10 add $0x10,%esp

80493dc: e8 86 09 00 00 call 8049d67 <read\_line>

80493e1: 89 45 f4 mov %eax,-0xc(%ebp)

80493e4: 83 ec 0c sub $0xc,%esp

80493e7: ff 75 f4 pushl -0xc(%ebp)

80493ea: e8 ee 03 00 00 call 80497dd <phase\_5>

80493ef: 83 c4 10 add $0x10,%esp

80493f2: 85 c0 test %eax,%eax

80493f4: 74 15 je 804940b <main+0x1d9>

80493f6: e8 d8 0a 00 00 call 8049ed3 <phase\_defused>

80493fb: 83 ec 0c sub $0xc,%esp

80493fe: 68 50 a1 04 08 push $0x804a150

8049403: e8 88 fc ff ff call 8049090 <puts@plt>

8049408: 83 c4 10 add $0x10,%esp

804940b: e8 57 09 00 00 call 8049d67 <read\_line>

8049410: 89 45 f4 mov %eax,-0xc(%ebp)

8049413: 83 ec 0c sub $0xc,%esp

8049416: ff 75 f4 pushl -0xc(%ebp)

8049419: e8 36 04 00 00 call 8049854 <phase\_6>

804941e: 83 c4 10 add $0x10,%esp

8049421: 85 c0 test %eax,%eax

8049423: 74 05 je 804942a <main+0x1f8>

8049425: e8 a9 0a 00 00 call 8049ed3 <phase\_defused>

804942a: b8 00 00 00 00 mov $0x0,%eax

804942f: 8d 65 f8 lea -0x8(%ebp),%esp

8049432: 59 pop %ecx

8049433: 5b pop %ebx

8049434: 5d pop %ebp

8049435: 8d 61 fc lea -0x4(%ecx),%esp

8049438: c3 ret

08049439 <UVGWDIJP>:

8049439: 55 push %ebp

804943a: 89 e5 mov %esp,%ebp

804943c: 83 ec 04 sub $0x4,%esp

804943f: db 45 08 fildl 0x8(%ebp)

8049442: db 45 0c fildl 0xc(%ebp)

8049445: de c9 fmulp %st,%st(1)

8049447: 8b 45 08 mov 0x8(%ebp),%eax

804944a: 99 cltd

804944b: f7 7d 0c idivl 0xc(%ebp)

804944e: 89 45 fc mov %eax,-0x4(%ebp)

8049451: db 45 fc fildl -0x4(%ebp)

8049454: de e9 fsubrp %st,%st(1)

8049456: c9 leave

8049457: c3 ret

08049458 <phase\_0>:

8049458: 55 push %ebp

8049459: 89 e5 mov %esp,%ebp

804945b: 83 ec 08 sub $0x8,%esp

804945e: 83 ec 08 sub $0x8,%esp

8049461: 68 c4 a1 04 08 push $0x804a1c4

8049466: ff 75 08 pushl 0x8(%ebp)

8049469: e8 d4 07 00 00 call 8049c42 <strings\_not\_equal>

804946e: 83 c4 10 add $0x10,%esp

8049471: 85 c0 test %eax,%eax

8049473: 74 0c je 8049481 <phase\_0+0x29>

8049475: e8 30 0a 00 00 call 8049eaa <explode\_bomb>

804947a: b8 00 00 00 00 mov $0x0,%eax

804947f: eb 05 jmp 8049486 <phase\_0+0x2e>

8049481: b8 01 00 00 00 mov $0x1,%eax

8049486: c9 leave

8049487: c3 ret

08049488 <phase\_1>:

8049488: 55 push %ebp

8049489: 89 e5 mov %esp,%ebp

804948b: 83 ec 18 sub $0x18,%esp

804948e: c7 45 f4 e4 ea 58 09 movl $0x958eae4,-0xc(%ebp)

8049495: db 45 f4 fildl -0xc(%ebp)

8049498: d9 5d f0 fstps -0x10(%ebp)//156822240 0x4d158eae

804949b: 8d 45 e8 lea -0x18(%ebp),%eax

804949e: 50 push %eax

804949f: 8d 45 ec lea -0x14(%ebp),%eax //3.99124597e-34

80494a2: 50 push %eax

80494a3: 68 e5 a1 04 08 push $0x804a1e5 //0x25206425 1.39117181e-16

80494a8: ff 75 08 pushl 0x8(%ebp) //3.99124597e-34

80494ab: e8 20 fc ff ff call 80490d0 <\_\_isoc99\_sscanf@plt>

80494b0: 83 c4 10 add $0x10,%esp

80494b3: 83 f8 02 cmp $0x2,%eax //输入2个数字

80494b6: 74 0c je 80494c4 <phase\_1+0x3c>

80494b8: e8 ed 09 00 00 call 8049eaa <explode\_bomb>

80494bd: b8 00 00 00 00 mov $0x0,%eax

80494c2: eb 34 jmp 80494f8 <phase\_1+0x70>

80494c4: 8d 45 f0 lea -0x10(%ebp),%eax //156822240 0x4d158eae

80494c7: 0f b7 00 movzwl (%eax),%eax //36526

80494ca: 0f bf d0 movswl %ax,%edx //-29010

80494cd: 8b 45 ec mov -0x14(%ebp),%eax //1819043138 0x6c6c6542

80494d0: 39 c2 cmp %eax,%edx

80494d2: 75 13 jne 80494e7 <phase\_1+0x5f>//这里要相等，不等爆炸

80494d4: 8d 45 f0 lea -0x10(%ebp),%eax //1293258414 0x4d158eae

80494d7: 83 c0 02 add $0x2,%eax //1293258416 0x4d158eb1

80494da: 0f b7 00 movzwl (%eax),%eax

80494dd: 0f bf d0 movswl %ax,%edx

80494e0: 8b 45 e8 mov -0x18(%ebp),%eax

80494e3: 39 c2 cmp %eax,%edx

80494e5: 74 0c je 80494f3 <phase\_1+0x6b>

80494e7: e8 be 09 00 00 call 8049eaa <explode\_bomb>

80494ec: b8 00 00 00 00 mov $0x0,%eax

80494f1: eb 05 jmp 80494f8 <phase\_1+0x70>

80494f3: b8 01 00 00 00 mov $0x1,%eax

80494f8: c9 leave

80494f9: c3 ret

080494fa <phase\_2>:

80494fa: 55 push %ebp

80494fb: 89 e5 mov %esp,%ebp

80494fd: 83 ec 38 sub $0x38,%esp

8049500: 83 ec 04 sub $0x4,%esp

8049503: 6a 09 push $0x9

8049505: 8d 45 d0 lea -0x30(%ebp),%eax

8049508: 50 push %eax //-12104

8049509: ff 75 08 pushl 0x8(%ebp) //(void \*) 0xffffd0f0 ->0x0804c360

804950c: e8 77 06 00 00 call 8049b88 <read\_n\_numbers>

8049511: 83 c4 10 add $0x10,%esp

8049514: 85 c0 test %eax,%eax

8049516: 75 07 jne 804951f <phase\_2+0x25>

8049518: b8 00 00 00 00 mov $0x0,%eax

804951d: eb 65 jmp 8049584 <phase\_2+0x8a>

804951f: 8b 45 d0 mov -0x30(%ebp),%eax

8049522: 83 f8 18 cmp $0x18,%eax

8049525: 75 08 jne 804952f <phase\_2+0x35>

8049527: 8b 45 d4 mov -0x2c(%ebp),%eax

804952a: 83 f8 31 cmp $0x31,%eax

804952d: 74 0c je 804953b <phase\_2+0x41>

804952f: e8 76 09 00 00 call 8049eaa <explode\_bomb>

8049534: b8 00 00 00 00 mov $0x0,%eax

8049539: eb 49 jmp 8049584 <phase\_2+0x8a>

804953b: c7 45 f4 02 00 00 00 movl $0x2,-0xc(%ebp)

8049542: eb 35 jmp 8049579 <phase\_2+0x7f>

8049544: 8b 45 f4 mov -0xc(%ebp),%eax

8049547: 8b 44 85 d0 mov -0x30(%ebp,%eax,4),%eax //input

804954b: 8b 55 f4 mov -0xc(%ebp),%edx //循环次数i

804954e: 83 ea 02 sub $0x2,%edx

8049551: 8b 54 95 d0 mov -0x30(%ebp,%edx,4),%edx //input[i-2]

8049555: 89 d1 mov %edx,%ecx //input[i-2]

8049557: d1 f9 sar %ecx //input[i-2]/2

8049559: 8b 55 f4 mov -0xc(%ebp),%edx //i

804955c: 83 ea 01 sub $0x1,%edx //i-1

804955f: 8b 54 95 d0 mov -0x30(%ebp,%edx,4),%edx //input[i-1]

8049563: 01 ca add %ecx,%edx //input[i]=input[i-1]+input[i-2]>>1

8049565: 39 d0 cmp %edx,%eax

8049567: 74 0c je 8049575 <phase\_2+0x7b>

8049569: e8 3c 09 00 00 call 8049eaa <explode\_bomb>

804956e: b8 00 00 00 00 mov $0x0,%eax

8049573: eb 0f jmp 8049584 <phase\_2+0x8a>

8049575: 83 45 f4 01 addl $0x1,-0xc(%ebp)

8049579: 83 7d f4 08 cmpl $0x8,-0xc(%ebp) < 8

804957d: 7e c5 jle 8049544 <phase\_2+0x4a>

804957f: b8 01 00 00 00 mov $0x1,%eax

8049584: c9 leave

8049585: c3 ret

08049586 <phase\_3>:

8049586: 55 push %ebp

8049587: 89 e5 mov %esp,%ebp

8049589: 83 ec 18 sub $0x18,%esp

804958c: 8d 45 e8 lea -0x18(%ebp),%eax

804958f: 50 push %eax

8049590: 8d 45 ec lea -0x14(%ebp),%eax

8049593: 50 push %eax

8049594: 68 e5 a1 04 08 push $0x804a1e5

8049599: ff 75 08 pushl 0x8(%ebp)

804959c: e8 2f fb ff ff call 80490d0 <\_\_isoc99\_sscanf@plt>

80495a1: 83 c4 10 add $0x10,%esp

80495a4: 89 45 f0 mov %eax,-0x10(%ebp)

80495a7: 83 7d f0 01 cmpl $0x1,-0x10(%ebp)

80495ab: 7f 0f jg 80495bc <phase\_3+0x36>

80495ad: e8 f8 08 00 00 call 8049eaa <explode\_bomb>

80495b2: b8 00 00 00 00 mov $0x0,%eax

80495b7: e9 8e 00 00 00 jmp 804964a <phase\_3+0xc4>

80495bc: c7 45 f4 00 00 00 00 movl $0x0,-0xc(%ebp)

80495c3: 8b 45 ec mov -0x14(%ebp),%eax

80495c6: 2d ce 00 00 00 sub $0xce,%eax //-206

80495cb: 83 f8 08 cmp $0x8,%eax //input[0]>8 bomb

80495ce: 77 55 ja 8049625 <phase\_3+0x9f>

80495d0: 8b 04 85 ec a1 04 08 mov 0x804a1ec(,%eax,4),%eax

80495d7: ff e0 jmp \*%eax

80495d9: 81 45 f4 96 00 00 00 addl $0x96,-0xc(%ebp)

80495e0: 81 45 f4 37 01 00 00 addl $0x137,-0xc(%ebp)

80495e7: 81 6d f4 96 00 00 00 subl $0x96,-0xc(%ebp)

80495ee: 81 45 f4 96 00 00 00 addl $0x96,-0xc(%ebp)

80495f5: 81 45 f4 37 01 00 00 addl $0x137,-0xc(%ebp)

80495fc: 81 6d f4 96 00 00 00 subl $0x96,-0xc(%ebp)

8049603: 81 45 f4 37 01 00 00 addl $0x137,-0xc(%ebp)

804960a: 81 6d f4 37 01 00 00 subl $0x137,-0xc(%ebp)

8049611: 81 45 f4 96 00 00 00 addl $0x96,-0xc(%ebp)

8049618: 90 nop

8049619: 8b 45 ec mov -0x14(%ebp),%eax //input

804961c: 3d d4 00 00 00 cmp $0xd4,%eax //input<212 bomb

8049621: 7f 16 jg 8049639 <phase\_3+0xb3>

8049623: eb 0c jmp 8049631 <phase\_3+0xab>

8049625: e8 80 08 00 00 call 8049eaa <explode\_bomb>

804962a: b8 00 00 00 00 mov $0x0,%eax

804962f: eb 19 jmp 804964a <phase\_3+0xc4>

8049631: 8b 45 e8 mov -0x18(%ebp),%eax input[1]

8049634: 39 45 f4 cmp %eax,-0xc(%ebp)

8049637: 74 0c je 8049645 <phase\_3+0xbf>

8049639: e8 6c 08 00 00 call 8049eaa <explode\_bomb>

804963e: b8 00 00 00 00 mov $0x0,%eax

8049643: eb 05 jmp 804964a <phase\_3+0xc4>

8049645: b8 01 00 00 00 mov $0x1,%eax

804964a: c9 leave

804964b: c3 ret

0804964c <func4>:

804964c: 55 push %ebp

804964d: 89 e5 mov %esp,%ebp

804964f: 83 ec 18 sub $0x18,%esp

8049652: 8b 55 0c mov 0xc(%ebp),%edx //input[0]

8049655: 8b 45 10 mov 0x10(%ebp),%eax //input[1]

8049658: 01 d0 add %edx,%eax //input[0]+input[1]

804965a: 89 c2 mov %eax,%edx

804965c: c1 ea 1f shr $0x1f,%edx //(input[0]+input[1])>>31

804965f: 01 d0 add %edx,%eax

//((input[0]+input[1])>>31) + input[0]+input[1]

8049661: d1 f8 sar %eax //(((input[0]+input[1])>>31) + input[0]+input[1]) >> 1

8049663: 89 45 f4 mov %eax,-0xc(%ebp)

8049666: 8b 45 0c mov 0xc(%ebp),%eax

8049669: 3b 45 10 cmp 0x10(%ebp),%eax //input[0] < input[1]

804966c: 7c 13 jl 8049681 <func4+0x35>

804966e: 8b 45 10 mov 0x10(%ebp),%eax

//input[1]

8049671: 8d 14 85 00 00 00 00 lea 0x0(,%eax,4),%edx

//4\*input[1]

8049678: 8b 45 08 mov 0x8(%ebp),%eax //0xffffd038

804967b: 01 d0 add %edx,%eax //4\*input[1](=25)+0xffffd038=0xffffd09c

804967d: 8b 00 mov (%eax),%eax

804967f: eb 3c jmp 80496bd <func4+0x71>

8049681: 83 ec 04 sub $0x4,%esp

8049684: ff 75 f4 pushl -0xc(%ebp)

8049687: ff 75 0c pushl 0xc(%ebp)

804968a: ff 75 08 pushl 0x8(%ebp)

804968d: e8 ba ff ff ff call 804964c <func4>

8049692: 83 c4 10 add $0x10,%esp

8049695: 89 45 f0 mov %eax,-0x10(%ebp)

8049698: 8b 45 f4 mov -0xc(%ebp),%eax

804969b: 83 c0 01 add $0x1,%eax

804969e: 83 ec 04 sub $0x4,%esp

80496a1: ff 75 10 pushl 0x10(%ebp)

80496a4: 50 push %eax

80496a5: ff 75 08 pushl 0x8(%ebp)

80496a8: e8 9f ff ff ff call 804964c <func4>

80496ad: 83 c4 10 add $0x10,%esp

80496b0: 89 45 ec mov %eax,-0x14(%ebp)

80496b3: 8b 45 ec mov -0x14(%ebp),%eax

80496b6: 39 45 f0 cmp %eax,-0x10(%ebp)

80496b9: 0f 4d 45 f0 cmovge -0x10(%ebp),%eax

80496bd: c9 leave

80496be: c3 ret

080496bf <phase\_4>:

80496bf: 55 push %ebp

80496c0: 89 e5 mov %esp,%ebp

80496c2: 57 push %edi

80496c3: 56 push %esi

80496c4: 53 push %ebx

80496c5: 81 ec ac 00 00 00 sub $0xac,%esp

80496cb: 8d 85 50 ff ff ff lea -0xb0(%ebp),%eax

80496d1: bb 20 a2 04 08 mov $0x804a220,%ebx

80496d6: ba 25 00 00 00 mov $0x25,%edx

80496db: 89 c7 mov %eax,%edi

80496dd: 89 de mov %ebx,%esi

80496df: 89 d1 mov %edx,%ecx

80496e1: f3 a5 rep movsl %ds:(%esi),%es:(%edi)

80496e3: 8d 85 48 ff ff ff lea -0xb8(%ebp),%eax

80496e9: 50 push %eax

80496ea: 8d 85 4c ff ff ff lea -0xb4(%ebp),%eax

80496f0: 50 push %eax

80496f1: 68 e5 a1 04 08 push $0x804a1e5

80496f6: ff 75 08 pushl 0x8(%ebp)

80496f9: e8 d2 f9 ff ff call 80490d0 <\_\_isoc99\_sscanf@plt>

80496fe: 83 c4 10 add $0x10,%esp

8049701: 89 45 e4 mov %eax,-0x1c(%ebp)

8049704: 83 7d e4 02 cmpl $0x2,-0x1c(%ebp)

8049708: 74 0f je 8049719 <phase\_4+0x5a>

804970a: e8 9b 07 00 00 call 8049eaa <explode\_bomb>

804970f: b8 00 00 00 00 mov $0x0,%eax

8049714: e9 bc 00 00 00 jmp 80497d5 <phase\_4+0x116>

8049719: 8b 95 48 ff ff ff mov -0xb8(%ebp),%edx

804971f: 8b 85 4c ff ff ff mov -0xb4(%ebp),%eax

8049725: 83 ec 04 sub $0x4,%esp

8049728: 52 push %edx input[1]

8049729: 50 push %eax input[0]

804972a: 8d 85 50 ff ff ff lea -0xb0(%ebp),%eax

8049730: 50 push %eax

8049731: e8 16 ff ff ff call 804964c <func4>

8049736: 83 c4 10 add $0x10,%esp

8049739: 3d 9f 01 00 00 cmp $0x19f,%eax //415

804973e: 74 0f je 804974f <phase\_4+0x90>

8049740: e8 65 07 00 00 call 8049eaa <explode\_bomb>

8049745: b8 00 00 00 00 mov $0x0,%eax

804974a: e9 86 00 00 00 jmp 80497d5 <phase\_4+0x116>

804974f: 8b 85 4c ff ff ff mov -0xb4(%ebp),%eax //input[0]

8049755: 85 c0 test %eax,%eax

8049757: 7e 36 jle 804978f <phase\_4+0xd0>

8049759: 8b 85 48 ff ff ff mov -0xb8(%ebp),%eax //input[0]

804975f: 8b 95 4c ff ff ff mov -0xb4(%ebp),%edx //input[1]

8049765: 83 ea 01 sub $0x1,%edx //input[1]-1

8049768: 83 ec 04 sub $0x4,%esp

804976b: 50 push %eax

804976c: 52 push %edx

804976d: 8d 85 50 ff ff ff lea -0xb0(%ebp),%eax //185

8049773: 50 push %eax

8049774: e8 d3 fe ff ff call 804964c <func4>

8049779: 83 c4 10 add $0x10,%esp

804977c: 3d 9f 01 00 00 cmp $0x19f,%eax //415

8049781: 75 0c jne 804978f <phase\_4+0xd0>

8049783: e8 22 07 00 00 call 8049eaa <explode\_bomb>

8049788: b8 00 00 00 00 mov $0x0,%eax

804978d: eb 46 jmp 80497d5 <phase\_4+0x116>

804978f: 8b 85 48 ff ff ff mov -0xb8(%ebp),%eax //input[1]

8049795: 83 f8 23 cmp $0x23,%eax

8049798: 7f 36 jg 80497d0 <phase\_4+0x111>

804979a: 8b 85 48 ff ff ff mov -0xb8(%ebp),%eax //input[1]

80497a0: 8d 50 01 lea 0x1(%eax),%edx //input[1]+1

80497a3: 8b 85 4c ff ff ff mov -0xb4(%ebp),%eax //input[0]

80497a9: 83 ec 04 sub $0x4,%esp

80497ac: 52 push %edx

80497ad: 50 push %eax

80497ae: 8d 85 50 ff ff ff lea -0xb0(%ebp),%eax //\*=185

80497b4: 50 push %eax

80497b5: e8 92 fe ff ff call 804964c <func4> //fun4(input[0], input[1]+1)

80497ba: 83 c4 10 add $0x10,%esp

80497bd: 3d 9f 01 00 00 cmp $0x19f,%eax

80497c2: 75 0c jne 80497d0 <phase\_4+0x111>

80497c4: e8 e1 06 00 00 call 8049eaa <explode\_bomb>

80497c9: b8 00 00 00 00 mov $0x0,%eax

80497ce: eb 05 jmp 80497d5 <phase\_4+0x116>

80497d0: b8 01 00 00 00 mov $0x1,%eax

80497d5: 8d 65 f4 lea -0xc(%ebp),%esp

80497d8: 5b pop %ebx

80497d9: 5e pop %esi

80497da: 5f pop %edi

80497db: 5d pop %ebp

80497dc: c3 ret

080497dd <x >:

80497dd: 55 push %ebp

80497de: 89 e5 mov %esp,%ebp

80497e0: 83 ec 18 sub $0x18,%esp

80497e3: 83 ec 0c sub $0xc,%esp

80497e6: ff 75 08 pushl 0x8(%ebp)

80497e9: e8 28 04 00 00 call 8049c16 <string\_length>

80497ee: 83 c4 10 add $0x10,%esp

80497f1: 89 45 ec mov %eax,-0x14(%ebp)

80497f4: 83 7d ec 08 cmpl $0x8,-0x14(%ebp)

80497f8: 74 0c je 8049806 <phase\_5+0x29> //输入的字串长度为8

80497fa: e8 ab 06 00 00 call 8049eaa <explode\_bomb>

80497ff: b8 00 00 00 00 mov $0x0,%eax

8049804: eb 4c jmp 8049852 <phase\_5+0x75>

8049806: c7 45 f0 00 00 00 00 movl $0x0,-0x10(%ebp) //res=0;

804980d: c7 45 f4 00 00 00 00 movl $0x0,-0xc(%ebp) //i = 0;

8049814: eb 1f jmp 8049835 <phase\_5+0x58>

8049816: 8b 55 f4 mov -0xc(%ebp),%edx //i

8049819: 8b 45 08 mov 0x8(%ebp),%eax //char\* input

804981c: 01 d0 add %edx,%eax

804981e: 0f b6 00 movzbl (%eax),%eax //input[i]

8049821: 0f be c0 movsbl %al,%eax //input[i]

8049824: 83 e0 0f and $0xf,%eax //input[i]&0xf

8049827: 8b 04 85 60 c2 04 08 mov 0x804c260(,%eax,4),%eax

804982e: 01 45 f0 add %eax,-0x10(%ebp)//res+=?

8049831: 83 45 f4 01 addl $0x1,-0xc(%ebp) //i++

8049835: 83 7d f4 07 cmpl $0x7,-0xc(%ebp) //while(i < 7)

8049839: 7e db jle 8049816 <phase\_5+0x39>

804983b: 83 7d f0 47 cmpl $0x47,-0x10(%ebp)

804983f: 74 0c je 804984d <phase\_5+0x70>

8049841: e8 64 06 00 00 call 8049eaa <explode\_bomb>

8049846: b8 00 00 00 00 mov $0x0,%eax

804984b: eb 05 jmp 8049852 <phase\_5+0x75>

804984d: b8 01 00 00 00 mov $0x1,%eax

8049852: c9 leave

8049853: c3 ret

08049854 <phase\_6>:

8049854: 55 push %ebp

8049855: 89 e5 mov %esp,%ebp

8049857: 83 ec 48 sub $0x48,%esp

804985a: c7 45 e8 90 c1 04 08 movl $0x804c190,-0x18(%ebp)

8049861: 83 ec 08 sub $0x8,%esp

8049864: 8d 45 d0 lea -0x30(%ebp),%eax

8049867: 50 push %eax

8049868: ff 75 08 pushl 0x8(%ebp)

804986b: e8 b9 02 00 00 call 8049b29 <read\_six\_numbers>

8049870: 83 c4 10 add $0x10,%esp

8049873: 85 c0 test %eax,%eax

8049875: 75 0a jne 8049881 <phase\_6+0x2d>

8049877: b8 00 00 00 00 mov $0x0,%eax

804987c: e9 37 01 00 00 jmp 80499b8 <phase\_6+0x164>

8049881: c7 45 f0 00 00 00 00 movl $0x0,-0x10(%ebp) //i = 0

8049888: eb 60 jmp 80498ea <phase\_6+0x96>

804988a: 8b 45 f0 mov -0x10(%ebp),%eax //i

804988d: 8b 44 85 d0 mov -0x30(%ebp,%eax,4),%eax

8049891: 85 c0 test %eax,%eax

8049893: 7e 0c jle 80498a1 <phase\_6+0x4d>

8049895: 8b 45 f0 mov -0x10(%ebp),%eax

8049898: 8b 44 85 d0 mov -0x30(%ebp,%eax,4),%eax

804989c: 83 f8 06 cmp $0x6,%eax

804989f: 7e 0f jle 80498b0 <phase\_6+0x5c>

80498a1: e8 04 06 00 00 call 8049eaa <explode\_bomb>

80498a6: b8 00 00 00 00 mov $0x0,%eax

80498ab: e9 08 01 00 00 jmp 80499b8 <phase\_6+0x164>

80498b0: 8b 45 f0 mov -0x10(%ebp),%eax

80498b3: 83 c0 01 add $0x1,%eax

80498b6: 89 45 ec mov %eax,-0x14(%ebp)

80498b9: eb 25 jmp 80498e0 <phase\_6+0x8c>

80498bb: 8b 45 f0 mov -0x10(%ebp),%eax

80498be: 8b 54 85 d0 mov -0x30(%ebp,%eax,4),%edx

80498c2: 8b 45 ec mov -0x14(%ebp),%eax

80498c5: 8b 44 85 d0 mov -0x30(%ebp,%eax,4),%eax

80498c9: 39 c2 cmp %eax,%edx

80498cb: 75 0f jne 80498dc <phase\_6+0x88>

80498cd: e8 d8 05 00 00 call 8049eaa <explode\_bomb>

80498d2: b8 00 00 00 00 mov $0x0,%eax

80498d7: e9 dc 00 00 00 jmp 80499b8 <phase\_6+0x164>

80498dc: 83 45 ec 01 addl $0x1,-0x14(%ebp)

80498e0: 83 7d ec 05 cmpl $0x5,-0x14(%ebp)

80498e4: 7e d5 jle 80498bb <phase\_6+0x67>

80498e6: 83 45 f0 01 addl $0x1,-0x10(%ebp)

80498ea: 83 7d f0 05 cmpl $0x5,-0x10(%ebp)

80498ee: 7e 9a jle 804988a <phase\_6+0x36> //while (i <= 5)

80498f0: c7 45 f0 00 00 00 00 movl $0x0,-0x10(%ebp) //i = 0

80498f7: eb 36 jmp 804992f <phase\_6+0xdb>

80498f9: 8b 45 e8 mov -0x18(%ebp),%eax

80498fc: 89 45 f4 mov %eax,-0xc(%ebp)

80498ff: c7 45 ec 01 00 00 00 movl $0x1,-0x14(%ebp)

8049906: eb 0d jmp 8049915 <phase\_6+0xc1>

8049908: 8b 45 f4 mov -0xc(%ebp),%eax

804990b: 8b 40 08 mov 0x8(%eax),%eax

804990e: 89 45 f4 mov %eax,-0xc(%ebp)

8049911: 83 45 ec 01 addl $0x1,-0x14(%ebp)

8049915: 8b 45 f0 mov -0x10(%ebp),%eax

8049918: 8b 44 85 d0 mov -0x30(%ebp,%eax,4),%eax

804991c: 39 45 ec cmp %eax,-0x14(%ebp)

804991f: 7c e7 jl 8049908 <phase\_6+0xb4>

8049921: 8b 45 f0 mov -0x10(%ebp),%eax

8049924: 8b 55 f4 mov -0xc(%ebp),%edx

8049927: 89 54 85 b8 mov %edx,-0x48(%ebp,%eax,4)

804992b: 83 45 f0 01 addl $0x1,-0x10(%ebp)

804992f: 83 7d f0 05 cmpl $0x5,-0x10(%ebp)

8049933: 7e c4 jle 80498f9 <phase\_6+0xa5> //while(i <= 5)

8049935: 8b 45 b8 mov -0x48(%ebp),%eax

8049938: 89 45 e8 mov %eax,-0x18(%ebp)

804993b: 8b 45 e8 mov -0x18(%ebp),%eax

804993e: 89 45 f4 mov %eax,-0xc(%ebp)

8049941: c7 45 f0 01 00 00 00 movl $0x1,-0x10(%ebp) //i = 1

8049948: eb 1a jmp 8049964 <phase\_6+0x110>

804994a: 8b 45 f0 mov -0x10(%ebp),%eax

804994d: 8b 54 85 b8 mov -0x48(%ebp,%eax,4),%edx

8049951: 8b 45 f4 mov -0xc(%ebp),%eax

8049954: 89 50 08 mov %edx,0x8(%eax)

8049957: 8b 45 f4 mov -0xc(%ebp),%eax

804995a: 8b 40 08 mov 0x8(%eax),%eax

804995d: 89 45 f4 mov %eax,-0xc(%ebp)

8049960: 83 45 f0 01 addl $0x1,-0x10(%ebp)

8049964: 83 7d f0 05 cmpl $0x5,-0x10(%ebp)

8049968: 7e e0 jle 804994a <phase\_6+0xf6> //while(i <= 5)

804996a: 8b 45 f4 mov -0xc(%ebp),%eax

804996d: c7 40 08 00 00 00 00 movl $0x0,0x8(%eax)

8049974: 8b 45 e8 mov -0x18(%ebp),%eax

8049977: 89 45 f4 mov %eax,-0xc(%ebp)

804997a: c7 45 f0 00 00 00 00 movl $0x0,-0x10(%ebp) //i=0

8049981: eb 2a jmp 80499ad <phase\_6+0x159>

8049983: 8b 45 f4 mov -0xc(%ebp),%eax

8049986: 8b 10 mov (%eax),%edx

8049988: 8b 45 f4 mov -0xc(%ebp),%eax

804998b: 8b 40 08 mov 0x8(%eax),%eax //->next

804998e: 8b 00 mov (%eax),%eax //->next->d

8049990: 39 c2 cmp %eax,%edx

8049992: 7d 0c jge 80499a0 <phase\_6+0x14c>

8049994: e8 11 05 00 00 call 8049eaa <explode\_bomb>

8049999: b8 00 00 00 00 mov $0x0,%eax

804999e: eb 18 jmp 80499b8 <phase\_6+0x164>

80499a0: 8b 45 f4 mov -0xc(%ebp),%eax

80499a3: 8b 40 08 mov 0x8(%eax),%eax

80499a6: 89 45 f4 mov %eax,-0xc(%ebp)

80499a9: 83 45 f0 01 addl $0x1,-0x10(%ebp) //i++;

80499ad: 83 7d f0 04 cmpl $0x4,-0x10(%ebp) //while(i<=4)

80499b1: 7e d0 jle 8049983 <phase\_6+0x12f>

80499b3: b8 01 00 00 00 mov $0x1,%eax

80499b8: c9 leave

80499b9: c3 ret

080499ba <fun7>:

80499ba: 55 push %ebp

80499bb: 89 e5 mov %esp,%ebp

80499bd: 83 ec 08 sub $0x8,%esp

80499c0: 83 7d 08 00 cmpl $0x0,0x8(%ebp)

80499c4: 75 07 jne 80499cd <fun7+0x13>

80499c6: b8 ff ff ff ff mov $0xffffffff,%eax

80499cb: eb 4e jmp 8049a1b <fun7+0x61>

80499cd: 8b 45 08 mov 0x8(%ebp),%eax //\*’D’

80499d0: 8b 00 mov (%eax),%eax //’$’

80499d2: 39 45 0c cmp %eax,0xc(%ebp)

80499d5: 7d 19 jge 80499f0 <fun7+0x36>

80499d7: 8b 45 08 mov 0x8(%ebp),%eax

80499da: 8b 40 04 mov 0x4(%eax),%eax

80499dd: 83 ec 08 sub $0x8,%esp

80499e0: ff 75 0c pushl 0xc(%ebp)

80499e3: 50 push %eax

80499e4: e8 d1 ff ff ff call 80499ba <fun7>

80499e9: 83 c4 10 add $0x10,%esp

80499ec: 01 c0 add %eax,%eax

80499ee: eb 2b jmp 8049a1b <fun7+0x61>

80499f0: 8b 45 08 mov 0x8(%ebp),%eax

80499f3: 8b 00 mov (%eax),%eax

80499f5: 39 45 0c cmp %eax,0xc(%ebp)

80499f8: 75 07 jne 8049a01 <fun7+0x47>

80499fa: b8 00 00 00 00 mov $0x0,%eax

80499ff: eb 1a jmp 8049a1b <fun7+0x61>

8049a01: 8b 45 08 mov 0x8(%ebp),%eax

8049a04: 8b 40 08 mov 0x8(%eax),%eax

8049a07: 83 ec 08 sub $0x8,%esp

8049a0a: ff 75 0c pushl 0xc(%ebp)

8049a0d: 50 push %eax

8049a0e: e8 a7 ff ff ff call 80499ba <fun7>

8049a13: 83 c4 10 add $0x10,%esp

8049a16: 01 c0 add %eax,%eax

8049a18: 83 c0 01 add $0x1,%eax

8049a1b: c9 leave

8049a1c: c3 ret

08049a1d <secret\_phase>:

8049a1d: 55 push %ebp

8049a1e: 89 e5 mov %esp,%ebp

8049a20: 83 ec 18 sub $0x18,%esp

8049a23: e8 3f 03 00 00 call 8049d67 <read\_line>

8049a28: 89 45 f4 mov %eax,-0xc(%ebp)

8049a2b: 83 ec 0c sub $0xc,%esp

8049a2e: ff 75 f4 pushl -0xc(%ebp)

8049a31: e8 ca f6 ff ff call 8049100 <atoi@plt>

8049a36: 83 c4 10 add $0x10,%esp

8049a39: 89 45 f0 mov %eax,-0x10(%ebp)

8049a3c: 83 7d f0 00 cmpl $0x0,-0x10(%ebp)

8049a40: 7e 09 jle 8049a4b <secret\_phase+0x2e>

8049a42: 81 7d f0 e9 03 00 00 cmpl $0x3e9,-0x10(%ebp)

8049a49: 7e 0c jle 8049a57 <secret\_phase+0x3a>

8049a4b: e8 5a 04 00 00 call 8049eaa <explode\_bomb>

8049a50: b8 00 00 00 00 mov $0x0,%eax

8049a55: eb 42 jmp 8049a99 <secret\_phase+0x7c>

8049a57: 83 ec 08 sub $0x8,%esp

8049a5a: ff 75 f0 pushl -0x10(%ebp)

8049a5d: 68 44 c2 04 08 push $0x804c244

8049a62: e8 53 ff ff ff call 80499ba <fun7>

8049a67: 83 c4 10 add $0x10,%esp

8049a6a: 89 45 ec mov %eax,-0x14(%ebp)

8049a6d: 83 7d ec 00 cmpl $0x0,-0x14(%ebp)

8049a71: 74 0c je 8049a7f <secret\_phase+0x62>

8049a73: e8 32 04 00 00 call 8049eaa <explode\_bomb>

8049a78: b8 00 00 00 00 mov $0x0,%eax

8049a7d: eb 1a jmp 8049a99 <secret\_phase+0x7c>

8049a7f: 83 ec 0c sub $0xc,%esp

8049a82: 68 b4 a2 04 08 push $0x804a2b4

8049a87: e8 04 f6 ff ff call 8049090 <puts@plt>

8049a8c: 83 c4 10 add $0x10,%esp

8049a8f: e8 3f 04 00 00 call 8049ed3 <phase\_defused>

8049a94: b8 01 00 00 00 mov $0x1,%eax

8049a99: c9 leave

8049a9a: c3 ret

08049a9b <sig\_handler>:

8049a9b: 55 push %ebp

8049a9c: 89 e5 mov %esp,%ebp

8049a9e: 83 ec 08 sub $0x8,%esp

8049aa1: 83 ec 0c sub $0xc,%esp

8049aa4: 68 dc a2 04 08 push $0x804a2dc

8049aa9: e8 e2 f5 ff ff call 8049090 <puts@plt>

8049aae: 83 c4 10 add $0x10,%esp

8049ab1: 83 ec 0c sub $0xc,%esp

8049ab4: 6a 03 push $0x3

8049ab6: e8 b5 f5 ff ff call 8049070 <sleep@plt>

8049abb: 83 c4 10 add $0x10,%esp

8049abe: 83 ec 0c sub $0xc,%esp

8049ac1: 68 14 a3 04 08 push $0x804a314

8049ac6: e8 65 f5 ff ff call 8049030 <printf@plt>

8049acb: 83 c4 10 add $0x10,%esp

8049ace: a1 a4 c2 04 08 mov 0x804c2a4,%eax

8049ad3: 83 ec 0c sub $0xc,%esp

8049ad6: 50 push %eax

8049ad7: e8 64 f5 ff ff call 8049040 <fflush@plt>

8049adc: 83 c4 10 add $0x10,%esp

8049adf: 83 ec 0c sub $0xc,%esp

8049ae2: 6a 01 push $0x1

8049ae4: e8 87 f5 ff ff call 8049070 <sleep@plt>

8049ae9: 83 c4 10 add $0x10,%esp

8049aec: 83 ec 0c sub $0xc,%esp

8049aef: 68 1c a3 04 08 push $0x804a31c

8049af4: e8 97 f5 ff ff call 8049090 <puts@plt>

8049af9: 83 c4 10 add $0x10,%esp

8049afc: 83 ec 0c sub $0xc,%esp

8049aff: 6a 10 push $0x10

8049b01: e8 9a f5 ff ff call 80490a0 <exit@plt>

08049b06 <invalid\_phase>:

8049b06: 55 push %ebp

8049b07: 89 e5 mov %esp,%ebp

8049b09: 83 ec 08 sub $0x8,%esp

8049b0c: 83 ec 08 sub $0x8,%esp

8049b0f: ff 75 08 pushl 0x8(%ebp)

8049b12: 68 24 a3 04 08 push $0x804a324

8049b17: e8 14 f5 ff ff call 8049030 <printf@plt>

8049b1c: 83 c4 10 add $0x10,%esp

8049b1f: 83 ec 0c sub $0xc,%esp

8049b22: 6a 08 push $0x8

8049b24: e8 77 f5 ff ff call 80490a0 <exit@plt>

08049b29 <read\_six\_numbers>:

8049b29: 55 push %ebp

8049b2a: 89 e5 mov %esp,%ebp

8049b2c: 56 push %esi

8049b2d: 53 push %ebx

8049b2e: 83 ec 10 sub $0x10,%esp

8049b31: 8b 45 0c mov 0xc(%ebp),%eax

8049b34: 8d 70 14 lea 0x14(%eax),%esi

8049b37: 8b 45 0c mov 0xc(%ebp),%eax

8049b3a: 8d 58 10 lea 0x10(%eax),%ebx

8049b3d: 8b 45 0c mov 0xc(%ebp),%eax

8049b40: 8d 48 0c lea 0xc(%eax),%ecx

8049b43: 8b 45 0c mov 0xc(%ebp),%eax

8049b46: 8d 50 08 lea 0x8(%eax),%edx

8049b49: 8b 45 0c mov 0xc(%ebp),%eax

8049b4c: 83 c0 04 add $0x4,%eax

8049b4f: 56 push %esi

8049b50: 53 push %ebx

8049b51: 51 push %ecx

8049b52: 52 push %edx

8049b53: 50 push %eax

8049b54: ff 75 0c pushl 0xc(%ebp)

8049b57: 68 35 a3 04 08 push $0x804a335

8049b5c: ff 75 08 pushl 0x8(%ebp)

8049b5f: e8 6c f5 ff ff call 80490d0 <\_\_isoc99\_sscanf@plt>

8049b64: 83 c4 20 add $0x20,%esp

8049b67: 89 45 f4 mov %eax,-0xc(%ebp)

8049b6a: 83 7d f4 05 cmpl $0x5,-0xc(%ebp)

8049b6e: 7f 0c jg 8049b7c <read\_six\_numbers+0x53>

8049b70: e8 35 03 00 00 call 8049eaa <explode\_bomb>

8049b75: b8 00 00 00 00 mov $0x0,%eax

8049b7a: eb 05 jmp 8049b81 <read\_six\_numbers+0x58>

8049b7c: b8 01 00 00 00 mov $0x1,%eax

8049b81: 8d 65 f8 lea -0x8(%ebp),%esp

8049b84: 5b pop %ebx

8049b85: 5e pop %esi

8049b86: 5d pop %ebp

8049b87: c3 ret

08049b88 <read\_n\_numbers>:

8049b88: 55 push %ebp

8049b89: 89 e5 mov %esp,%ebp

8049b8b: 83 ec 18 sub $0x18,%esp

8049b8e: c7 45 f0 00 00 00 00 movl $0x0,-0x10(%ebp)

8049b95: eb 70 jmp 8049c07 <read\_n\_numbers+0x7f>

8049b97: 83 7d f0 00 cmpl $0x0,-0x10(%ebp) 0!=input

8049b9b: 75 18 jne 8049bb5 <read\_n\_numbers+0x2d>

8049b9d: 83 ec 08 sub $0x8,%esp

8049ba0: 68 47 a3 04 08 push $0x804a347

8049ba5: ff 75 08 pushl 0x8(%ebp)

8049ba8: e8 43 f5 ff ff call 80490f0 <strtok@plt>

8049bad: 83 c4 10 add $0x10,%esp

8049bb0: 89 45 f4 mov %eax,-0xc(%ebp) //134529888

8049bb3: eb 15 jmp 8049bca <read\_n\_numbers+0x42>

8049bb5: 83 ec 08 sub $0x8,%esp

8049bb8: 68 47 a3 04 08 push $0x804a347

8049bbd: 6a 00 push $0x0

8049bbf: e8 2c f5 ff ff call 80490f0 <strtok@plt>

8049bc4: 83 c4 10 add $0x10,%esp

8049bc7: 89 45 f4 mov %eax,-0xc(%ebp)

8049bca: 83 7d f4 00 cmpl $0x0,-0xc(%ebp) =0 bomb!

8049bce: 74 27 je 8049bf7 <read\_n\_numbers+0x6f>

8049bd0: 8b 45 f0 mov -0x10(%ebp),%eax //0

8049bd3: 8d 14 85 00 00 00 00 lea 0x0(,%eax,4),%edx //0

8049bda: 8b 45 0c mov 0xc(%ebp),%eax //-12104

8049bdd: 01 d0 add %edx,%eax

8049bdf: 83 ec 04 sub $0x4,%esp

8049be2: 50 push %eax

8049be3: 68 4b a3 04 08 push $0x804a34b

8049be8: ff 75 f4 pushl -0xc(%ebp)

8049beb: e8 e0 f4 ff ff call 80490d0 <\_\_isoc99\_sscanf@plt>

8049bf0: 83 c4 10 add $0x10,%esp

8049bf3: 85 c0 test %eax,%eax

8049bf5: 7f 0c jg 8049c03 <read\_n\_numbers+0x7b>

8049bf7: e8 ae 02 00 00 call 8049eaa <explode\_bomb>

8049bfc: b8 00 00 00 00 mov $0x0,%eax

8049c01: eb 11 jmp 8049c14 <read\_n\_numbers+0x8c>

8049c03: 83 45 f0 01 addl $0x1,-0x10(%ebp)

8049c07: 8b 45 f0 mov -0x10(%ebp),%eax ->input

8049c0a: 3b 45 10 cmp 0x10(%ebp),%eax 9<input

8049c0d: 7c 88 jl 8049b97 <read\_n\_numbers+0xf>

8049c0f: b8 01 00 00 00 mov $0x1,%eax

8049c14: c9 leave

8049c15: c3 ret

08049c16 <string\_length>:

8049c16: 55 push %ebp

8049c17: 89 e5 mov %esp,%ebp

8049c19: 83 ec 10 sub $0x10,%esp

8049c1c: 8b 45 08 mov 0x8(%ebp),%eax

8049c1f: 89 45 f8 mov %eax,-0x8(%ebp)

8049c22: c7 45 fc 00 00 00 00 movl $0x0,-0x4(%ebp)

8049c29: eb 08 jmp 8049c33 <string\_length+0x1d>

8049c2b: 83 45 f8 01 addl $0x1,-0x8(%ebp)

8049c2f: 83 45 fc 01 addl $0x1,-0x4(%ebp)

8049c33: 8b 45 f8 mov -0x8(%ebp),%eax

8049c36: 0f b6 00 movzbl (%eax),%eax

8049c39: 84 c0 test %al,%al

8049c3b: 75 ee jne 8049c2b <string\_length+0x15>

8049c3d: 8b 45 fc mov -0x4(%ebp),%eax

8049c40: c9 leave

8049c41: c3 ret

08049c42 <strings\_not\_equal>:

8049c42: 55 push %ebp

8049c43: 89 e5 mov %esp,%ebp

8049c45: 53 push %ebx

8049c46: 83 ec 10 sub $0x10,%esp

8049c49: ff 75 08 pushl 0x8(%ebp)

8049c4c: e8 c5 ff ff ff call 8049c16 <string\_length>

8049c51: 83 c4 04 add $0x4,%esp

8049c54: 89 c3 mov %eax,%ebx

8049c56: ff 75 0c pushl 0xc(%ebp)

8049c59: e8 b8 ff ff ff call 8049c16 <string\_length>

8049c5e: 83 c4 04 add $0x4,%esp

8049c61: 39 c3 cmp %eax,%ebx

8049c63: 74 07 je 8049c6c <strings\_not\_equal+0x2a>

8049c65: b8 01 00 00 00 mov $0x1,%eax

8049c6a: eb 3c jmp 8049ca8 <strings\_not\_equal+0x66>

8049c6c: 8b 45 08 mov 0x8(%ebp),%eax

8049c6f: 89 45 f8 mov %eax,-0x8(%ebp)

8049c72: 8b 45 0c mov 0xc(%ebp),%eax

8049c75: 89 45 f4 mov %eax,-0xc(%ebp)

8049c78: eb 1f jmp 8049c99 <strings\_not\_equal+0x57>

8049c7a: 8b 45 f8 mov -0x8(%ebp),%eax

8049c7d: 0f b6 10 movzbl (%eax),%edx

8049c80: 8b 45 f4 mov -0xc(%ebp),%eax

8049c83: 0f b6 00 movzbl (%eax),%eax

8049c86: 38 c2 cmp %al,%dl

8049c88: 74 07 je 8049c91 <strings\_not\_equal+0x4f>

8049c8a: b8 01 00 00 00 mov $0x1,%eax

8049c8f: eb 17 jmp 8049ca8 <strings\_not\_equal+0x66>

8049c91: 83 45 f8 01 addl $0x1,-0x8(%ebp)

8049c95: 83 45 f4 01 addl $0x1,-0xc(%ebp)

8049c99: 8b 45 f8 mov -0x8(%ebp),%eax

8049c9c: 0f b6 00 movzbl (%eax),%eax

8049c9f: 84 c0 test %al,%al

8049ca1: 75 d7 jne 8049c7a <strings\_not\_equal+0x38>

8049ca3: b8 00 00 00 00 mov $0x0,%eax

8049ca8: 8b 5d fc mov -0x4(%ebp),%ebx

8049cab: c9 leave

8049cac: c3 ret

08049cad <initialize\_bomb>:

8049cad: 55 push %ebp

8049cae: 89 e5 mov %esp,%ebp

8049cb0: 83 ec 08 sub $0x8,%esp

8049cb3: 83 ec 08 sub $0x8,%esp

8049cb6: 68 9b 9a 04 08 push $0x8049a9b

8049cbb: 6a 02 push $0x2

8049cbd: e8 9e f3 ff ff call 8049060 <signal@plt>

8049cc2: 83 c4 10 add $0x10,%esp

8049cc5: 90 nop

8049cc6: c9 leave

8049cc7: c3 ret

08049cc8 <initialize\_bomb\_solve>:

8049cc8: 55 push %ebp

8049cc9: 89 e5 mov %esp,%ebp

8049ccb: 90 nop

8049ccc: 5d pop %ebp

8049ccd: c3 ret

08049cce <blank\_line>:

8049cce: 55 push %ebp

8049ccf: 89 e5 mov %esp,%ebp

8049cd1: 83 ec 08 sub $0x8,%esp

8049cd4: eb 30 jmp 8049d06 <blank\_line+0x38>

8049cd6: e8 35 f4 ff ff call 8049110 <\_\_ctype\_b\_loc@plt>

8049cdb: 8b 08 mov (%eax),%ecx

8049cdd: 8b 45 08 mov 0x8(%ebp),%eax

8049ce0: 8d 50 01 lea 0x1(%eax),%edx

8049ce3: 89 55 08 mov %edx,0x8(%ebp)

8049ce6: 0f b6 00 movzbl (%eax),%eax

8049ce9: 0f be c0 movsbl %al,%eax

8049cec: 01 c0 add %eax,%eax

8049cee: 01 c8 add %ecx,%eax

8049cf0: 0f b7 00 movzwl (%eax),%eax

8049cf3: 0f b7 c0 movzwl %ax,%eax

8049cf6: 25 00 20 00 00 and $0x2000,%eax

8049cfb: 85 c0 test %eax,%eax

8049cfd: 75 07 jne 8049d06 <blank\_line+0x38>

8049cff: b8 00 00 00 00 mov $0x0,%eax

8049d04: eb 0f jmp 8049d15 <blank\_line+0x47>

8049d06: 8b 45 08 mov 0x8(%ebp),%eax

8049d09: 0f b6 00 movzbl (%eax),%eax

8049d0c: 84 c0 test %al,%al

8049d0e: 75 c6 jne 8049cd6 <blank\_line+0x8>

8049d10: b8 01 00 00 00 mov $0x1,%eax

8049d15: c9 leave

8049d16: c3 ret

08049d17 <skip>:

8049d17: 55 push %ebp

8049d18: 89 e5 mov %esp,%ebp

8049d1a: 83 ec 18 sub $0x18,%esp

8049d1d: 8b 0d b0 c2 04 08 mov 0x804c2b0,%ecx

8049d23: 8b 15 ac c2 04 08 mov 0x804c2ac,%edx

8049d29: 89 d0 mov %edx,%eax

8049d2b: c1 e0 02 shl $0x2,%eax

8049d2e: 01 d0 add %edx,%eax

8049d30: c1 e0 04 shl $0x4,%eax

8049d33: 05 c0 c2 04 08 add $0x804c2c0,%eax

8049d38: 83 ec 04 sub $0x4,%esp

8049d3b: 51 push %ecx

8049d3c: 6a 50 push $0x50

8049d3e: 50 push %eax

8049d3f: e8 0c f3 ff ff call 8049050 <fgets@plt>

8049d44: 83 c4 10 add $0x10,%esp

8049d47: 89 45 f4 mov %eax,-0xc(%ebp)

8049d4a: 83 7d f4 00 cmpl $0x0,-0xc(%ebp)

8049d4e: 74 12 je 8049d62 <skip+0x4b>

8049d50: 83 ec 0c sub $0xc,%esp

8049d53: ff 75 f4 pushl -0xc(%ebp)

8049d56: e8 73 ff ff ff call 8049cce <blank\_line>

8049d5b: 83 c4 10 add $0x10,%esp

8049d5e: 85 c0 test %eax,%eax

8049d60: 75 bb jne 8049d1d <skip+0x6>

8049d62: 8b 45 f4 mov -0xc(%ebp),%eax

8049d65: c9 leave

8049d66: c3 ret

08049d67 <read\_line>:

8049d67: 55 push %ebp

8049d68: 89 e5 mov %esp,%ebp

8049d6a: 83 ec 18 sub $0x18,%esp

8049d6d: e8 a5 ff ff ff call 8049d17 <skip>

8049d72: 89 45 f4 mov %eax,-0xc(%ebp)

8049d75: 83 7d f4 00 cmpl $0x0,-0xc(%ebp)

8049d79: 75 79 jne 8049df4 <read\_line+0x8d>

8049d7b: 8b 15 b0 c2 04 08 mov 0x804c2b0,%edx

8049d81: a1 a0 c2 04 08 mov 0x804c2a0,%eax

8049d86: 39 c2 cmp %eax,%edx

8049d88: 75 1a jne 8049da4 <read\_line+0x3d>

8049d8a: 83 ec 0c sub $0xc,%esp

8049d8d: 68 4e a3 04 08 push $0x804a34e

8049d92: e8 f9 f2 ff ff call 8049090 <puts@plt>

8049d97: 83 c4 10 add $0x10,%esp

8049d9a: 83 ec 0c sub $0xc,%esp

8049d9d: 6a 08 push $0x8

8049d9f: e8 fc f2 ff ff call 80490a0 <exit@plt>

8049da4: 83 ec 0c sub $0xc,%esp

8049da7: 68 6c a3 04 08 push $0x804a36c

8049dac: e8 cf f2 ff ff call 8049080 <getenv@plt>

8049db1: 83 c4 10 add $0x10,%esp

8049db4: 85 c0 test %eax,%eax

8049db6: 74 0a je 8049dc2 <read\_line+0x5b>

8049db8: 83 ec 0c sub $0xc,%esp

8049dbb: 6a 00 push $0x0

8049dbd: e8 de f2 ff ff call 80490a0 <exit@plt>

8049dc2: a1 a0 c2 04 08 mov 0x804c2a0,%eax

8049dc7: a3 b0 c2 04 08 mov %eax,0x804c2b0

8049dcc: e8 46 ff ff ff call 8049d17 <skip>

8049dd1: 89 45 f4 mov %eax,-0xc(%ebp)

8049dd4: 83 7d f4 00 cmpl $0x0,-0xc(%ebp)

8049dd8: 75 1a jne 8049df4 <read\_line+0x8d>

8049dda: 83 ec 0c sub $0xc,%esp

8049ddd: 68 4e a3 04 08 push $0x804a34e

8049de2: e8 a9 f2 ff ff call 8049090 <puts@plt>

8049de7: 83 c4 10 add $0x10,%esp

8049dea: 83 ec 0c sub $0xc,%esp

8049ded: 6a 00 push $0x0

8049def: e8 ac f2 ff ff call 80490a0 <exit@plt>

8049df4: 8b 15 ac c2 04 08 mov 0x804c2ac,%edx

8049dfa: 89 d0 mov %edx,%eax

8049dfc: c1 e0 02 shl $0x2,%eax

8049dff: 01 d0 add %edx,%eax

8049e01: c1 e0 04 shl $0x4,%eax

8049e04: 05 c0 c2 04 08 add $0x804c2c0,%eax

8049e09: 83 ec 0c sub $0xc,%esp

8049e0c: 50 push %eax

8049e0d: e8 9e f2 ff ff call 80490b0 <strlen@plt>

8049e12: 83 c4 10 add $0x10,%esp

8049e15: 89 45 f0 mov %eax,-0x10(%ebp)

8049e18: 83 7d f0 4e cmpl $0x4e,-0x10(%ebp)

8049e1c: 7e 4d jle 8049e6b <read\_line+0x104>

8049e1e: 83 ec 0c sub $0xc,%esp

8049e21: 68 77 a3 04 08 push $0x804a377

8049e26: e8 65 f2 ff ff call 8049090 <puts@plt>

8049e2b: 83 c4 10 add $0x10,%esp

8049e2e: 8b 15 ac c2 04 08 mov 0x804c2ac,%edx

8049e34: 8d 42 01 lea 0x1(%edx),%eax

8049e37: a3 ac c2 04 08 mov %eax,0x804c2ac

8049e3c: 89 d0 mov %edx,%eax

8049e3e: c1 e0 02 shl $0x2,%eax

8049e41: 01 d0 add %edx,%eax

8049e43: c1 e0 04 shl $0x4,%eax

8049e46: 05 c0 c2 04 08 add $0x804c2c0,%eax

8049e4b: c7 00 2a 2a 2a 74 movl $0x742a2a2a,(%eax)

8049e51: c7 40 04 72 75 6e 63 movl $0x636e7572,0x4(%eax)

8049e58: c7 40 08 61 74 65 64 movl $0x64657461,0x8(%eax)

8049e5f: c7 40 0c 2a 2a 2a 00 movl $0x2a2a2a,0xc(%eax)

8049e66: e8 3f 00 00 00 call 8049eaa <explode\_bomb>

8049e6b: 8b 15 ac c2 04 08 mov 0x804c2ac,%edx

8049e71: 8b 45 f0 mov -0x10(%ebp),%eax

8049e74: 8d 48 ff lea -0x1(%eax),%ecx

8049e77: 89 d0 mov %edx,%eax

8049e79: c1 e0 02 shl $0x2,%eax

8049e7c: 01 d0 add %edx,%eax

8049e7e: c1 e0 04 shl $0x4,%eax

8049e81: 01 c8 add %ecx,%eax

8049e83: 05 c0 c2 04 08 add $0x804c2c0,%eax

8049e88: c6 00 00 movb $0x0,(%eax)

8049e8b: 8b 15 ac c2 04 08 mov 0x804c2ac,%edx

8049e91: 8d 42 01 lea 0x1(%edx),%eax

8049e94: a3 ac c2 04 08 mov %eax,0x804c2ac

8049e99: 89 d0 mov %edx,%eax

8049e9b: c1 e0 02 shl $0x2,%eax

8049e9e: 01 d0 add %edx,%eax

8049ea0: c1 e0 04 shl $0x4,%eax

8049ea3: 05 c0 c2 04 08 add $0x804c2c0,%eax

8049ea8: c9 leave

8049ea9: c3 ret

08049eaa <explode\_bomb>:

8049eaa: 55 push %ebp

8049eab: 89 e5 mov %esp,%ebp

8049ead: 83 ec 08 sub $0x8,%esp

8049eb0: 83 ec 0c sub $0xc,%esp

8049eb3: 68 92 a3 04 08 push $0x804a392

8049eb8: e8 d3 f1 ff ff call 8049090 <puts@plt>

8049ebd: 83 c4 10 add $0x10,%esp

8049ec0: 83 ec 0c sub $0xc,%esp

8049ec3: 68 9b a3 04 08 push $0x804a39b

8049ec8: e8 c3 f1 ff ff call 8049090 <puts@plt>

8049ecd: 83 c4 10 add $0x10,%esp

8049ed0: 90 nop

8049ed1: c9 leave

8049ed2: c3 ret

08049ed3 <phase\_defused>:

8049ed3: 55 push %ebp

8049ed4: 89 e5 mov %esp,%ebp

8049ed6: 83 ec 68 sub $0x68,%esp

8049ed9: a1 ac c2 04 08 mov 0x804c2ac,%eax

8049ede: 83 f8 07 cmp $0x7,%eax

8049ee1: 75 77 jne 8049f5a <phase\_defused+0x87>

8049ee3: 83 ec 0c sub $0xc,%esp

8049ee6: 8d 45 a4 lea -0x5c(%ebp),%eax

8049ee9: 50 push %eax

8049eea: 8d 45 9c lea -0x64(%ebp),%eax

8049eed: 50 push %eax

8049eee: 8d 45 a0 lea -0x60(%ebp),%eax

8049ef1: 50 push %eax

8049ef2: 68 b2 a3 04 08 push $0x804a3b2

8049ef7: 68 00 c4 04 08 push $0x804c400

8049efc: e8 cf f1 ff ff call 80490d0 <\_\_isoc99\_sscanf@plt>

8049f01: 83 c4 20 add $0x20,%esp

8049f04: 89 45 f4 mov %eax,-0xc(%ebp)

8049f07: 83 7d f4 03 cmpl $0x3,-0xc(%ebp)

8049f0b: 75 3d jne 8049f4a <phase\_defused+0x77>

8049f0d: 83 ec 08 sub $0x8,%esp

8049f10: 68 bb a3 04 08 push $0x804a3bb

8049f15: 8d 45 a4 lea -0x5c(%ebp),%eax input

8049f18: 50 push %eax

8049f19: e8 24 fd ff ff call 8049c42 <strings\_not\_equal>

8049f1e: 83 c4 10 add $0x10,%esp

8049f21: 85 c0 test %eax,%eax

8049f23: 75 25 jne 8049f4a <phase\_defused+0x77>

8049f25: 83 ec 0c sub $0xc,%esp

8049f28: 68 c4 a3 04 08 push $0x804a3c4

8049f2d: e8 5e f1 ff ff call 8049090 <puts@plt>

8049f32: 83 c4 10 add $0x10,%esp

8049f35: 83 ec 0c sub $0xc,%esp

8049f38: 68 ec a3 04 08 push $0x804a3ec

8049f3d: e8 4e f1 ff ff call 8049090 <puts@plt>

8049f42: 83 c4 10 add $0x10,%esp

8049f45: e8 d3 fa ff ff call 8049a1d <secret\_phase>

8049f4a: 83 ec 0c sub $0xc,%esp

8049f4d: 68 24 a4 04 08 push $0x804a424

8049f52: e8 39 f1 ff ff call 8049090 <puts@plt>

8049f57: 83 c4 10 add $0x10,%esp

8049f5a: 90 nop

8049f5b: c9 leave

8049f5c: c3 ret

8049f5d: 66 90 xchg %ax,%ax

8049f5f: 90 nop

08049f60 <\_\_libc\_csu\_init>:

8049f60: 55 push %ebp

8049f61: 57 push %edi

8049f62: 56 push %esi

8049f63: 53 push %ebx

8049f64: e8 07 f2 ff ff call 8049170 <\_\_x86.get\_pc\_thunk.bx>

8049f69: 81 c3 97 20 00 00 add $0x2097,%ebx

8049f6f: 83 ec 0c sub $0xc,%esp

8049f72: 8b 6c 24 28 mov 0x28(%esp),%ebp

8049f76: e8 85 f0 ff ff call 8049000 <\_init>

8049f7b: 8d b3 10 ff ff ff lea -0xf0(%ebx),%esi

8049f81: 8d 83 0c ff ff ff lea -0xf4(%ebx),%eax

8049f87: 29 c6 sub %eax,%esi

8049f89: c1 fe 02 sar $0x2,%esi

8049f8c: 74 1f je 8049fad <\_\_libc\_csu\_init+0x4d>

8049f8e: 31 ff xor %edi,%edi

8049f90: 83 ec 04 sub $0x4,%esp

8049f93: 55 push %ebp

8049f94: ff 74 24 2c pushl 0x2c(%esp)

8049f98: ff 74 24 2c pushl 0x2c(%esp)

8049f9c: ff 94 bb 0c ff ff ff call \*-0xf4(%ebx,%edi,4)

8049fa3: 83 c7 01 add $0x1,%edi

8049fa6: 83 c4 10 add $0x10,%esp

8049fa9: 39 fe cmp %edi,%esi

8049fab: 75 e3 jne 8049f90 <\_\_libc\_csu\_init+0x30>

8049fad: 83 c4 0c add $0xc,%esp

8049fb0: 5b pop %ebx

8049fb1: 5e pop %esi

8049fb2: 5f pop %edi

8049fb3: 5d pop %ebp

8049fb4: c3 ret

8049fb5: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi

8049fbc: 8d 74 26 00 lea 0x0(%esi,%eiz,1),%esi

08049fc0 <\_\_libc\_csu\_fini>:

8049fc0: c3 ret

Disassembly of section .fini:

08049fc4 <\_fini>:

8049fc4: 53 push %ebx

8049fc5: 83 ec 08 sub $0x8,%esp

8049fc8: e8 a3 f1 ff ff call 8049170 <\_\_x86.get\_pc\_thunk.bx>

8049fcd: 81 c3 33 20 00 00 add $0x2033,%ebx

8049fd3: 83 c4 08 add $0x8,%esp

8049fd6: 5b pop %ebx

8049fd7: c3 ret