Binary Bomb CSCI 2021 P3 Prob 2 Guide

Guide made 11-10-2021 by Alice Zhang

Helpful Links

Phases 1-6 outlined + more info if you're into this stuff:
http://zpalexander.com/binary-bomb-lab-phase-1/

Another set of guides on bombs for phases 1-7 (7 is the secret phase):
https://caminek.rocks/tag/#binary-bomb

Notes and Tips

My notes

Jump to the bookmarked sections to avoid scrolling through 75 painful pages of assembly. Yes, I did just copy my entire bomb into this file (no I don't recommend doing that).

My notes are formatted like so:
Abc = my comments
Abc = assembly commands I think are important

General tips

Set a breakpoint at explode bomb
b explode_bomb

Make sure to always put soemthing in for the next phase before testing input for the current phase. People have blown up bombs a ton of times because of this issues. Don't put extra spaces at the end of a line.

Pay attention to all the **cmp jl je jne etc** commands. Usually before you explode a bomb you'll have a comparison statement so the first thing I always do is just look out for those.

You don't have to understand what each command is doing but you do need to understand why your code is jumping from one place to another. Like know where your going but not necessarily why each step is taken and you'll be okay.

Take notes if you need to so you can keep track of general flow. Here's a useful command if you want to look at all the assembly
objdump -d bomb > bombFileName
This dumps all the assmebly code of the bomb into a fiile so you can have a ton of fun looking at it.

If all else fails, you can download another bomb. This doesn't always work so I'd do that as a last resort. But if you get super stuck don't keep grinding at it. Crying over a binary bomb will not help you become better at cs. Trust me. Just wait for help or download another bomb.

Disclaimer

Everyone's bomb's are different but some phases like phase 1, 2, and 6 stay the same for everyone (or that's what I've heard). Work with other people. It's helpful.

```
b
o
m
b
:
f
i
l
e
f
o
r
m
a
t
e
l
f
6
4
-
x
8
6
```

Yeah I don't know why I have this either. Guess it's a vertical version of the bomb title. Hilarious

Disassembly of section .init:


```
0000000000003000 <_init>:
    3000:    f3 0f 1e fa              endbr64
    3004:    48 83 ec 08              sub    $0x8,%rsp
    3008:    48 8b 05 d9 4f 00 00     mov    0x4fd9(%rip),%rax      # 7fe8
<__gmon_start__>
    300f:    48 85 c0                 test   %rax,%rax
    3012:    74 02                    je     3016 <_init+0x16>
    3014:    ff d0                    callq  *%rax
    3016:    48 83 c4 08              add    $0x8,%rsp
    301a:    c3                       retq
```


Disassembly of section .plt:


```
0000000000003020 <.plt>:
    3020:    ff 35 c2 4e 00 00        pushq  0x4ec2(%rip)        # 7ee8
<_GLOBAL_OFFSET_TABLE_+0x8>
    3026:    f2 ff 25 c3 4e 00 00     bnd jmpq *0x4ec3(%rip)        # 7ef0
<_GLOBAL_OFFSET_TABLE_+0x10>
    302d:    0f 1f 00                 nopl   (%rax)
    3030:    f3 0f 1e fa              endbr64
    3034:    68 00 00 00 00           pushq  $0x0
    3039:    f2 e9 e1 ff ff ff        bnd jmpq 3020 <.plt>
    303f:    90                       nop
    3040:    f3 0f 1e fa              endbr64
    3044:    68 01 00 00 00           pushq  $0x1
```

```
3049:    f2 e9 d1 ff ff ff         bnd jmpq 3020 <.plt>

304f:    90                        nop

3050:    f3 0f 1e fa               endbr64

3054:    68 02 00 00 00            pushq  $0x2

3059:    f2 e9 c1 ff ff ff         bnd jmpq 3020 <.plt>

305f:    90                        nop

3060:    f3 0f 1e fa               endbr64

3064:    68 03 00 00 00            pushq  $0x3

3069:    f2 e9 b1 ff ff ff         bnd jmpq 3020 <.plt>

306f:    90                        nop

3070:    f3 0f 1e fa               endbr64

3074:    68 04 00 00 00            pushq  $0x4

3079:    f2 e9 a1 ff ff ff         bnd jmpq 3020 <.plt>

307f:    90                        nop

3080:    f3 0f 1e fa               endbr64

3084:    68 05 00 00 00            pushq  $0x5

3089:    f2 e9 91 ff ff ff         bnd jmpq 3020 <.plt>

308f:    90                        nop

3090:    f3 0f 1e fa               endbr64

3094:    68 06 00 00 00            pushq  $0x6

3099:    f2 e9 81 ff ff ff         bnd jmpq 3020 <.plt>

309f:    90                        nop

30a0:    f3 0f 1e fa               endbr64

30a4:    68 07 00 00 00            pushq  $0x7

30a9:    f2 e9 71 ff ff ff         bnd jmpq 3020 <.plt>

30af:    90                        nop

30b0:    f3 0f 1e fa               endbr64

30b4:    68 08 00 00 00            pushq  $0x8

30b9:    f2 e9 61 ff ff ff         bnd jmpq 3020 <.plt>

30bf:    90                        nop

30c0:    f3 0f 1e fa               endbr64

30c4:    68 09 00 00 00            pushq  $0x9
```

```
30c9:    f2 e9 51 ff ff ff        bnd jmpq 3020 <.plt>

30cf:    90                       nop

30d0:    f3 0f 1e fa              endbr64

30d4:    68 0a 00 00 00           pushq  $0xa

30d9:    f2 e9 41 ff ff ff        bnd jmpq 3020 <.plt>

30df:    90                       nop

30e0:    f3 0f 1e fa              endbr64

30e4:    68 0b 00 00 00           pushq  $0xb

30e9:    f2 e9 31 ff ff ff        bnd jmpq 3020 <.plt>

30ef:    90                       nop

30f0:    f3 0f 1e fa              endbr64

30f4:    68 0c 00 00 00           pushq  $0xc

30f9:    f2 e9 21 ff ff ff        bnd jmpq 3020 <.plt>

30ff:    90                       nop

3100:    f3 0f 1e fa              endbr64

3104:    68 0d 00 00 00           pushq  $0xd

3109:    f2 e9 11 ff ff ff        bnd jmpq 3020 <.plt>

310f:    90                       nop

3110:    f3 0f 1e fa              endbr64

3114:    68 0e 00 00 00           pushq  $0xe

3119:    f2 e9 01 ff ff ff        bnd jmpq 3020 <.plt>

311f:    90                       nop

3120:    f3 0f 1e fa              endbr64

3124:    68 0f 00 00 00           pushq  $0xf

3129:    f2 e9 f1 fe ff ff        bnd jmpq 3020 <.plt>

312f:    90                       nop

3130:    f3 0f 1e fa              endbr64

3134:    68 10 00 00 00           pushq  $0x10

3139:    f2 e9 e1 fe ff ff        bnd jmpq 3020 <.plt>

313f:    90                       nop

3140:    f3 0f 1e fa              endbr64

3144:    68 11 00 00 00           pushq  $0x11
```

```
3149:    f2 e9 d1 fe ff ff          bnd jmpq 3020 <.plt>
314f:    90                          nop
3150:    f3 0f 1e fa                endbr64
3154:    68 12 00 00 00             pushq  $0x12
3159:    f2 e9 c1 fe ff ff          bnd jmpq 3020 <.plt>
315f:    90                          nop
3160:    f3 0f 1e fa                endbr64
3164:    68 13 00 00 00             pushq  $0x13
3169:    f2 e9 b1 fe ff ff          bnd jmpq 3020 <.plt>
316f:    90                          nop
3170:    f3 0f 1e fa                endbr64
3174:    68 14 00 00 00             pushq  $0x14
3179:    f2 e9 a1 fe ff ff          bnd jmpq 3020 <.plt>
317f:    90                          nop
3180:    f3 0f 1e fa                endbr64
3184:    68 15 00 00 00             pushq  $0x15
3189:    f2 e9 91 fe ff ff          bnd jmpq 3020 <.plt>
318f:    90                          nop
3190:    f3 0f 1e fa                endbr64
3194:    68 16 00 00 00             pushq  $0x16
3199:    f2 e9 81 fe ff ff          bnd jmpq 3020 <.plt>
319f:    90                          nop
31a0:    f3 0f 1e fa                endbr64
31a4:    68 17 00 00 00             pushq  $0x17
31a9:    f2 e9 71 fe ff ff          bnd jmpq 3020 <.plt>
31af:    90                          nop
31b0:    f3 0f 1e fa                endbr64
31b4:    68 18 00 00 00             pushq  $0x18
31b9:    f2 e9 61 fe ff ff          bnd jmpq 3020 <.plt>
31bf:    90                          nop
31c0:    f3 0f 1e fa                endbr64
31c4:    68 19 00 00 00             pushq  $0x19
```

```
    31c9:    f2 e9 51 fe ff ff        bnd jmpq 3020 <.plt>

    31cf:    90                       nop

    31d0:    f3 0f 1e fa              endbr64

    31d4:    68 1a 00 00 00           pushq  $0x1a

    31d9:    f2 e9 41 fe ff ff        bnd jmpq 3020 <.plt>

    31df:    90                       nop

    31e0:    f3 0f 1e fa              endbr64

    31e4:    68 1b 00 00 00           pushq  $0x1b

    31e9:    f2 e9 31 fe ff ff        bnd jmpq 3020 <.plt>

    31ef:    90                       nop
```

Disassembly of section .plt.got:


```
00000000000031f0 <__cxa_finalize@plt>:

    31f0:    f3 0f 1e fa              endbr64

    31f4:    f2 ff 25 fd 4d 00 00     bnd jmpq *0x4dfd(%rip)        # 7ff8
<__cxa_finalize@GLIBC_2.2.5>
    31fb:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)
```


Disassembly of section .plt.sec:


```
0000000000003200 <getenv@plt>:

    3200:    f3 0f 1e fa              endbr64

    3204:    f2 ff 25 ed 4c 00 00     bnd jmpq *0x4ced(%rip)        # 7ef8
<getenv@GLIBC_2.2.5>
    320b:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)
```


```
0000000000003210 <__snprintf_chk@plt>:

    3210:    f3 0f 1e fa              endbr64

    3214:    f2 ff 25 e5 4c 00 00     bnd jmpq *0x4ce5(%rip)        # 7f00
<__snprintf_chk@GLIBC_2.3.4>
```

```
 321b:     0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)


0000000000003220 <strcasecmp@plt>:
   3220:     f3 0f 1e fa              endbr64
   3224:     f2 ff 25 dd 4c 00 00     bnd jmpq *0x4cdd(%rip)        # 7f08
<strcasecmp@GLIBC_2.2.5>
   322b:     0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)


0000000000003230 <__errno_location@plt>:
   3230:     f3 0f 1e fa              endbr64
   3234:     f2 ff 25 d5 4c 00 00     bnd jmpq *0x4cd5(%rip)        # 7f10
<__errno_location@GLIBC_2.2.5>
   323b:     0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)


0000000000003240 <strcpy@plt>:
   3240:     f3 0f 1e fa              endbr64
   3244:     f2 ff 25 cd 4c 00 00     bnd jmpq *0x4ccd(%rip)        # 7f18
<strcpy@GLIBC_2.2.5>
   324b:     0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)


0000000000003250 <puts@plt>:
   3250:     f3 0f 1e fa              endbr64
   3254:     f2 ff 25 c5 4c 00 00     bnd jmpq *0x4cc5(%rip)        # 7f20
<puts@GLIBC_2.2.5>
   325b:     0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)


0000000000003260 <write@plt>:
   3260:     f3 0f 1e fa              endbr64
   3264:     f2 ff 25 bd 4c 00 00     bnd jmpq *0x4cbd(%rip)        # 7f28
<write@GLIBC_2.2.5>
   326b:     0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)
```

```
0000000000003270 <__stack_chk_fail@plt>:
    3270:    f3 0f 1e fa              endbr64
    3274:    f2 ff 25 b5 4c 00 00     bnd jmpq *0x4cb5(%rip)        # 7f30
<__stack_chk_fail@GLIBC_2.4>
    327b:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)


0000000000003280 <alarm@plt>:
    3280:    f3 0f 1e fa              endbr64
    3284:    f2 ff 25 ad 4c 00 00     bnd jmpq *0x4cad(%rip)        # 7f38
<alarm@GLIBC_2.2.5>
    328b:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)


0000000000003290 <close@plt>:
    3290:    f3 0f 1e fa              endbr64
    3294:    f2 ff 25 a5 4c 00 00     bnd jmpq *0x4ca5(%rip)        # 7f40
<close@GLIBC_2.2.5>
    329b:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)


00000000000032a0 <read@plt>:
    32a0:    f3 0f 1e fa              endbr64
    32a4:    f2 ff 25 9d 4c 00 00     bnd jmpq *0x4c9d(%rip)        # 7f48
<read@GLIBC_2.2.5>
    32ab:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)


00000000000032b0 <fgets@plt>:
    32b0:    f3 0f 1e fa              endbr64
    32b4:    f2 ff 25 95 4c 00 00     bnd jmpq *0x4c95(%rip)        # 7f50
<fgets@GLIBC_2.2.5>
    32bb:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)


00000000000032c0 <signal@plt>:
    32c0:    f3 0f 1e fa              endbr64
```

```
    32c4:    f2 ff 25 8d 4c 00 00    bnd jmpq *0x4c8d(%rip)        # 7f58
<signal@GLIBC_2.2.5>
    32cb:    0f 1f 44 00 00          nopl   0x0(%rax,%rax,1)


00000000000032d0 <gethostbyname@plt>:

    32d0:    f3 0f 1e fa             endbr64

    32d4:    f2 ff 25 85 4c 00 00    bnd jmpq *0x4c85(%rip)        # 7f60
<gethostbyname@GLIBC_2.2.5>
    32db:    0f 1f 44 00 00          nopl   0x0(%rax,%rax,1)


00000000000032e0 <__memmove_chk@plt>:

    32e0:    f3 0f 1e fa             endbr64

    32e4:    f2 ff 25 7d 4c 00 00    bnd jmpq *0x4c7d(%rip)        # 7f68
<__memmove_chk@GLIBC_2.3.4>
    32eb:    0f 1f 44 00 00          nopl   0x0(%rax,%rax,1)


00000000000032f0 <strtol@plt>:

    32f0:    f3 0f 1e fa             endbr64

    32f4:    f2 ff 25 75 4c 00 00    bnd jmpq *0x4c75(%rip)        # 7f70
<strtol@GLIBC_2.2.5>
    32fb:    0f 1f 44 00 00          nopl   0x0(%rax,%rax,1)


0000000000003300 <fflush@plt>:

    3300:    f3 0f 1e fa             endbr64

    3304:    f2 ff 25 6d 4c 00 00    bnd jmpq *0x4c6d(%rip)        # 7f78
<fflush@GLIBC_2.2.5>
    330b:    0f 1f 44 00 00          nopl   0x0(%rax,%rax,1)


0000000000003310 <__isoc99_sscanf@plt>:

    3310:    f3 0f 1e fa             endbr64

    3314:    f2 ff 25 65 4c 00 00    bnd jmpq *0x4c65(%rip)        # 7f80
<__isoc99_sscanf@GLIBC_2.7>
    331b:    0f 1f 44 00 00          nopl   0x0(%rax,%rax,1)
```

```
0000000000003320 <__printf_chk@plt>:

   3320:    f3 0f 1e fa              endbr64
   3324:    f2 ff 25 5d 4c 00 00     bnd jmpq *0x4c5d(%rip)        # 7f88
<__printf_chk@GLIBC_2.3.4>
   332b:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)




0000000000003330 <fopen@plt>:

   3330:    f3 0f 1e fa              endbr64
   3334:    f2 ff 25 55 4c 00 00     bnd jmpq *0x4c55(%rip)        # 7f90
<fopen@GLIBC_2.2.5>
   333b:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)




0000000000003340 <gethostname@plt>:

   3340:    f3 0f 1e fa              endbr64
   3344:    f2 ff 25 4d 4c 00 00     bnd jmpq *0x4c4d(%rip)        # 7f98
<gethostname@GLIBC_2.2.5>
   334b:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)




0000000000003350 <exit@plt>:

   3350:    f3 0f 1e fa              endbr64
   3354:    f2 ff 25 45 4c 00 00     bnd jmpq *0x4c45(%rip)        # 7fa0
<exit@GLIBC_2.2.5>
   335b:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)




0000000000003360 <connect@plt>:

   3360:    f3 0f 1e fa              endbr64
   3364:    f2 ff 25 3d 4c 00 00     bnd jmpq *0x4c3d(%rip)        # 7fa8
<connect@GLIBC_2.2.5>
   336b:    0f 1f 44 00 00           nopl   0x0(%rax,%rax,1)




0000000000003370 <__fprintf_chk@plt>:
```

```
   3370:     f3 0f 1e fa                endbr64
   3374:     f2 ff 25 35 4c 00 00       bnd jmpq *0x4c35(%rip)        # 7fb0
<__fprintf_chk@GLIBC_2.3.4>
   337b:     0f 1f 44 00 00             nopl   0x0(%rax,%rax,1)


0000000000003380 <sleep@plt>:
   3380:     f3 0f 1e fa                endbr64
   3384:     f2 ff 25 2d 4c 00 00       bnd jmpq *0x4c2d(%rip)        # 7fb8
<sleep@GLIBC_2.2.5>
   338b:     0f 1f 44 00 00             nopl   0x0(%rax,%rax,1)


0000000000003390 <__ctype_b_loc@plt>:
   3390:     f3 0f 1e fa                endbr64
   3394:     f2 ff 25 25 4c 00 00       bnd jmpq *0x4c25(%rip)        # 7fc0
<__ctype_b_loc@GLIBC_2.3>
   339b:     0f 1f 44 00 00             nopl   0x0(%rax,%rax,1)


00000000000033a0 <__sprintf_chk@plt>:
   33a0:     f3 0f 1e fa                endbr64
   33a4:     f2 ff 25 1d 4c 00 00       bnd jmpq *0x4c1d(%rip)        # 7fc8
<__sprintf_chk@GLIBC_2.3.4>
   33ab:     0f 1f 44 00 00             nopl   0x0(%rax,%rax,1)


00000000000033b0 <socket@plt>:
   33b0:     f3 0f 1e fa                endbr64
   33b4:     f2 ff 25 15 4c 00 00       bnd jmpq *0x4c15(%rip)        # 7fd0
<socket@GLIBC_2.2.5>
   33bb:     0f 1f 44 00 00             nopl   0x0(%rax,%rax,1)


Disassembly of section .text:


00000000000033c0 <_start>:
```

```
   33c0:    f3 0f 1e fa                endbr64

   33c4:    31 ed                      xor    %ebp,%ebp

   33c6:    49 89 d1                   mov    %rdx,%r9

   33c9:    5e                         pop    %rsi

   33ca:    48 89 e2                   mov    %rsp,%rdx

   33cd:    48 83 e4 f0                and    $0xfffffffffffffff0,%rsp

   33d1:    50                         push   %rax

   33d2:    54                         push   %rsp

   33d3:    4c 8d 05 f6 1a 00 00       lea    0x1af6(%rip),%r8        # 4ed0
<__libc_csu_fini>
   33da:    48 8d 0d 7f 1a 00 00       lea    0x1a7f(%rip),%rcx       # 4e60
<__libc_csu_init>
   33e1:    48 8d 3d c1 00 00 00       lea    0xc1(%rip),%rdi         # 34a9 <main>

   33e8:    ff 15 f2 4b 00 00          callq  *0x4bf2(%rip)           # 7fe0
<__libc_start_main@GLIBC_2.2.5>
   33ee:    f4                         hlt

   33ef:    90                         nop




00000000000033f0 <deregister_tm_clones>:
   33f0:    48 8d 3d 89 5e 00 00       lea    0x5e89(%rip),%rdi       # 9280
<stdout@@GLIBC_2.2.5>
   33f7:    48 8d 05 82 5e 00 00       lea    0x5e82(%rip),%rax       # 9280
<stdout@@GLIBC_2.2.5>
   33fe:    48 39 f8                   cmp    %rdi,%rax

   3401:    74 15                      je     3418 <deregister_tm_clones+0x28>

   3403:    48 8b 05 ce 4b 00 00       mov    0x4bce(%rip),%rax       # 7fd8
<_ITM_deregisterTMCloneTable>
   340a:    48 85 c0                   test   %rax,%rax

   340d:    74 09                      je     3418 <deregister_tm_clones+0x28>

   340f:    ff e0                      jmpq   *%rax

   3411:    0f 1f 80 00 00 00 00       nopl   0x0(%rax)

   3418:    c3                         retq

   3419:    0f 1f 80 00 00 00 00       nopl   0x0(%rax)
```

```
0000000000003420 <register_tm_clones>:
    3420:    48 8d 3d 59 5e 00 00        lea    0x5e59(%rip),%rdi        # 9280
<stdout@@GLIBC_2.2.5>
    3427:    48 8d 35 52 5e 00 00        lea    0x5e52(%rip),%rsi        # 9280
<stdout@@GLIBC_2.2.5>
    342e:    48 29 fe                    sub    %rdi,%rsi

    3431:    48 89 f0                    mov    %rsi,%rax

    3434:    48 c1 ee 3f                 shr    $0x3f,%rsi

    3438:    48 c1 f8 03                 sar    $0x3,%rax

    343c:    48 01 c6                    add    %rax,%rsi

    343f:    48 d1 fe                    sar    %rsi

    3442:    74 14                       je     3458 <register_tm_clones+0x38>

    3444:    48 8b 05 a5 4b 00 00        mov    0x4ba5(%rip),%rax        # 7ff0
<_ITM_registerTMCloneTable>
    344b:    48 85 c0                    test   %rax,%rax

    344e:    74 08                       je     3458 <register_tm_clones+0x38>

    3450:    ff e0                       jmpq   *%rax

    3452:    66 0f 1f 44 00 00           nopw   0x0(%rax,%rax,1)

    3458:    c3                          retq

    3459:    0f 1f 80 00 00 00 00        nopl   0x0(%rax)




0000000000003460 <__do_global_dtors_aux>:
    3460:    f3 0f 1e fa                 endbr64

    3464:    80 3d 3d 5e 00 00 00        cmpb   $0x0,0x5e3d(%rip)        # 92a8
<completed.8060>
    346b:    75 2b                       jne    3498 <__do_global_dtors_aux+0x38>

    346d:    55                          push   %rbp

    346e:    48 83 3d 82 4b 00 00        cmpq   $0x0,0x4b82(%rip)        # 7ff8
<__cxa_finalize@GLIBC_2.2.5>
    3475:    00

    3476:    48 89 e5                    mov    %rsp,%rbp

    3479:    74 0c                       je     3487 <__do_global_dtors_aux+0x27>

    347b:    48 8b 3d 86 4b 00 00        mov    0x4b86(%rip),%rdi        # 8008 <__dso_handle>

    3482:    e8 69 fd ff ff              callq  31f0 <__cxa_finalize@plt>
```

```
    3487:      e8 64 ff ff ff          callq  33f0 <deregister_tm_clones>
    348c:      c6 05 15 5e 00 00 01    movb   $0x1,0x5e15(%rip)        # 92a8
<completed.8060>
    3493:      5d                      pop    %rbp
    3494:      c3                      retq
    3495:      0f 1f 00                nopl   (%rax)
    3498:      c3                      retq
    3499:      0f 1f 80 00 00 00 00    nopl   0x0(%rax)


00000000000034a0 <frame_dummy>:
    34a0:      f3 0f 1e fa             endbr64
    34a4:      e9 77 ff ff ff          jmpq   3420 <register_tm_clones>


00000000000034a9 <main>:
    34a9:      f3 0f 1e fa             endbr64
    34ad:      53                      push   %rbx
    34ae:      83 ff 01                cmp    $0x1,%edi
    34b1:      0f 84 f8 00 00 00       je     35af <main+0x106>
    34b7:      48 89 f3                mov    %rsi,%rbx
    34ba:      83 ff 02                cmp    $0x2,%edi
    34bd:      0f 85 21 01 00 00       jne    35e4 <main+0x13b>
    34c3:      48 8b 7e 08             mov    0x8(%rsi),%rdi
    34c7:      48 8d 35 7d 20 00 00    lea    0x207d(%rip),%rsi        # 554b
<array.3481+0x36b>
    34ce:      e8 5d fe ff ff          callq  3330 <fopen@plt>
    34d3:      48 89 05 d6 5d 00 00    mov    %rax,0x5dd6(%rip)        # 92b0 <infile>
    34da:      48 85 c0                test   %rax,%rax
    34dd:      0f 84 df 00 00 00       je     35c2 <main+0x119>
    34e3:      e8 de 06 00 00          callq  3bc6 <initialize_bomb>
    34e8:      48 8d 3d 99 1b 00 00    lea    0x1b99(%rip),%rdi        # 5088
<_IO_stdin_used+0x88>
    34ef:      e8 5c fd ff ff          callq  3250 <puts@plt>
```

```
  34f4:    48 8d 3d cd 1b 00 00       lea    0x1bcd(%rip),%rdi        # 50c8
<_IO_stdin_used+0xc8>
  34fb:    e8 50 fd ff ff             callq  3250 <puts@plt>

  3500:    e8 32 0a 00 00             callq  3f37 <read_line>

  3505:    48 89 c7                   mov    %rax,%rdi

  3508:    e8 fa 00 00 00             callq  3607 <phase_1>

  350d:    e8 6d 0b 00 00             callq  407f <phase_defused>

  3512:    48 8d 3d df 1b 00 00       lea    0x1bdf(%rip),%rdi        # 50f8
<_IO_stdin_used+0xf8>
  3519:    e8 32 fd ff ff             callq  3250 <puts@plt>

  351e:    e8 14 0a 00 00             callq  3f37 <read_line>

  3523:    48 89 c7                   mov    %rax,%rdi

  3526:    e8 00 01 00 00             callq  362b <phase_2>

  352b:    e8 4f 0b 00 00             callq  407f <phase_defused>

  3530:    48 8d 3d 04 1b 00 00       lea    0x1b04(%rip),%rdi        # 503b
<_IO_stdin_used+0x3b>
  3537:    e8 14 fd ff ff             callq  3250 <puts@plt>

  353c:    e8 f6 09 00 00             callq  3f37 <read_line>

  3541:    48 89 c7                   mov    %rax,%rdi

  3544:    e8 56 01 00 00             callq  369f <phase_3>

  3549:    e8 31 0b 00 00             callq  407f <phase_defused>

  354e:    48 8d 3d 04 1b 00 00       lea    0x1b04(%rip),%rdi        # 5059
<_IO_stdin_used+0x59>
  3555:    e8 f6 fc ff ff             callq  3250 <puts@plt>

  355a:    e8 d8 09 00 00             callq  3f37 <read_line>

  355f:    48 89 c7                   mov    %rax,%rdi

  3562:    e8 4f 02 00 00             callq  37b6 <phase_4>

  3567:    e8 13 0b 00 00             callq  407f <phase_defused>

  356c:    48 8d 3d b5 1b 00 00       lea    0x1bb5(%rip),%rdi        # 5128
<_IO_stdin_used+0x128>
  3573:    e8 d8 fc ff ff             callq  3250 <puts@plt>

  3578:    e8 ba 09 00 00             callq  3f37 <read_line>

  357d:    48 89 c7                   mov    %rax,%rdi

  3580:    e8 a6 02 00 00             callq  382b <phase_5>
```

```
    3585:       e8 f5 0a 00 00                  callq  407f <phase_defused>

    358a:       48 8d 3d d7 1a 00 00            lea    0x1ad7(%rip),%rdi        # 5068
<_IO_stdin_used+0x68>
    3591:       e8 ba fc ff ff                  callq  3250 <puts@plt>

    3596:       e8 9c 09 00 00                  callq  3f37 <read_line>

    359b:       48 89 c7                        mov    %rax,%rdi

    359e:       e8 14 03 00 00                  callq  38b7 <phase_6>

    35a3:       e8 d7 0a 00 00                  callq  407f <phase_defused>

    35a8:       b8 00 00 00 00                  mov    $0x0,%eax

    35ad:       5b                              pop    %rbx

    35ae:       c3                              retq

    35af:       48 8b 05 da 5c 00 00            mov    0x5cda(%rip),%rax        # 9290
<stdin@@GLIBC_2.2.5>
    35b6:       48 89 05 f3 5c 00 00            mov    %rax,0x5cf3(%rip)        # 92b0 <infile>

    35bd:       e9 21 ff ff ff                  jmpq   34e3 <main+0x3a>

    35c2:       48 8b 4b 08                     mov    0x8(%rbx),%rcx

    35c6:       48 8b 13                        mov    (%rbx),%rdx

    35c9:       48 8d 35 34 1a 00 00            lea    0x1a34(%rip),%rsi        # 5004
<_IO_stdin_used+0x4>
    35d0:       bf 01 00 00 00                  mov    $0x1,%edi

    35d5:       e8 46 fd ff ff                  callq  3320 <__printf_chk@plt>

    35da:       bf 08 00 00 00                  mov    $0x8,%edi

    35df:       e8 6c fd ff ff                  callq  3350 <exit@plt>

    35e4:       48 8b 16                        mov    (%rsi),%rdx

    35e7:       48 8d 35 33 1a 00 00            lea    0x1a33(%rip),%rsi        # 5021
<_IO_stdin_used+0x21>
    35ee:       bf 01 00 00 00                  mov    $0x1,%edi

    35f3:       b8 00 00 00 00                  mov    $0x0,%eax

    35f8:       e8 23 fd ff ff                  callq  3320 <__printf_chk@plt>

    35fd:       bf 08 00 00 00                  mov    $0x8,%edi

    3602:       e8 49 fd ff ff                  callq  3350 <exit@plt>
```

Phase 1 | match the word

This one you just need to do **x/s $rsi** at the cmp line and then copy that string and put it as your input

```
0000000000003607 <phase_1>:

   3607:     f3 0f 1e fa                 endbr64

   360b:     48 83 ec 08  print out rsp here   sub    $0x8,%rsp

   360f:     48 8d 35 3a 1b 00 00         lea    0x1b3a(%rip),%rsi         # 5150
<_IO_stdin_used+0x150>
   3616:     e8 4b 05 00 00              callq  3b66 <strings_not_equal>

   361b:     85 c0                      test   %eax,%eax

   361d:     75 05                      jne    3624 <phase_1+0x1d>

   361f:     48 83 c4 08                add    $0x8,%rsp

   3623:     c3                         retq

   3624:     e8 87 08 00 00              callq  3eb0 <explode_bomb>

   3629:     eb f4                      jmp    361f <phase_1+0x18>
```

Phase_2 | number sequence

This one you need to get the first 2 numbers to pass the cmp statements and then go through the for loop and change the input then rerun with the breakpoint each time

A shortcut (if you're lucky and get an easy sequence) is to just find the first 3 numbers and then look up the sequence online

```
000000000000362b <phase_2>:

   362b:     f3 0f 1e fa                 endbr64

   362f:     55                         push   %rbp

   3630:     53                         push   %rbx

   3631:     48 83 ec 28                sub    $0x28,%rsp

   3635:     64 48 8b 04 25 28 00         mov    %fs:0x28,%rax

   363c:     00 00

   363e:     48 89 44 24 18              mov    %rax,0x18(%rsp)

   3643:     31 c0                      xor    %eax,%eax

   3645:     48 89 e6                   mov    %rsp,%rsi
```

```
3648:     e8 a5 08 00 00            callq  3ef2 <read_six_numbers>

364d:     83 3c 24 00    arg1 = 0   cmpl   $0x0,(%rsp)

3651:     75 07                     jne    365a <phase_2+0x2f>

3653:     83 7c 24 04 01  arg2 = 1  cmpl   $0x1,0x4(%rsp)

3658:     74 05                     je     365f <phase_2+0x34>

365a:     e8 51 08 00 00            callq  3eb0 <explode_bomb>

365f:     48 89 e3                  mov    %rsp,%rbx

3662:     48 8d 6c 24 10            lea    0x10(%rsp),%rbp

3667:     eb 0e                     jmp    3677 <phase_2+0x4c>

3669:     e8 42 08 00 00            callq  3eb0 <explode_bomb>

366e:     48 83 c3 04               add    $0x4,%rbx

3672:     48 39 eb                  cmp    %rbp,%rbx

3675:     74 0c                     je     3683 <phase_2+0x58>

3677:     8b 43 04                  mov    0x4(%rbx),%eax

367a:     03 03                     add    (%rbx),%eax

367c:     39 43 08    arg3-arg6 = whatever eax is here      cmp    %eax,0x8(%rbx)

367f:     74 ed                     je     366e <phase_2+0x43>

3681:     eb e6                     jmp    3669 <phase_2+0x3e>

3683:     48 8b 44 24 18            mov    0x18(%rsp),%rax

3688:     64 48 33 04 25 28 00      xor    %fs:0x28,%rax

368f:     00 00

3691:     75 07                     jne    369a <phase_2+0x6f>

3693:     48 83 c4 28               add    $0x28,%rsp

3697:     5b                        pop    %rbx

3698:     5d                        pop    %rbp

3699:     c3                        retq

369a:     e8 d1 fb ff ff            callq  3270 <__stack_chk_fail@plt>
```

Phase_3 | cipher

Ignore the unimaginative naming of this phase

This phase has two numbers and you basically just need to get both numbers to pass the cmp statements

```
000000000000369f <phase_3>:

   369f:    f3 0f 1e fa                 endbr64

   36a3:    48 83 ec 18                 sub     $0x18,%rsp

   36a7:    64 48 8b 04 25 28 00        mov     %fs:0x28,%rax

   36ae:    00 00

   36b0:    48 89 44 24 08              mov     %rax,0x8(%rsp)

   36b5:    31 c0                       xor     %eax,%eax

   36b7:    48 8d 4c 24 04              lea     0x4(%rsp),%rcx

   36bc:    48 89 e2                    mov     %rsp,%rdx

   36bf:    48 8d 35 1e 1e 00 00        lea     0x1e1e(%rip),%rsi        # 54e4
<array.3481+0x304>
   36c6:    e8 45 fc ff ff             callq   3310 <__isoc99_sscanf@plt>

   36cb:    83 f8 01      2 inputs      cmp     $0x1,%eax

   36ce:    7e 1e                       jle     36ee <phase_3+0x4f>

   36d0:    83 3c 24 07                 cmpl    $0x7,(%rsp)

   36d4:    0f 87 90 00 00 00           ja      376a <phase_3+0xcb>

   36da:    8b 04 24                    mov     (%rsp),%eax

   36dd:    48 8d 15 dc 1a 00 00        lea     0x1adc(%rip),%rdx        # 51c0
<_IO_stdin_used+0x1c0>
   36e4:    48 63 04 82                 movslq  (%rdx,%rax,4),%rax

   36e8:    48 01 d0                    add     %rdx,%rax

   36eb:    3e ff e0                    notrack jmpq *%rax

   36ee:    e8 bd 07 00 00             callq   3eb0 <explode_bomb>

   36f3:    eb db                       jmp     36d0 <phase_3+0x31>

   36f5:    b8 69 02 00 00              mov     $0x269,%eax

   36fa:    2d 99 02 00 00              sub     $0x299,%eax

   36ff:    05 ca 01 00 00              add     $0x1ca,%eax

   3704:    83 e8 6f                    sub     $0x6f,%eax

   3707:    83 c0 6f                    add     $0x6f,%eax

   370a:    83 e8 6f                    sub     $0x6f,%eax

   370d:    83 c0 6f                    add     $0x6f,%eax
```

```
3710:    83 e8 6f                  sub    $0x6f,%eax

3713:    83 3c 24 05               cmpl   $0x5,(%rsp)

3717:    7f 06                     jg     371f <phase_3+0x80>

3719:    39 44 24 04               cmp    %eax,0x4(%rsp)

371d:    74 05                     je     3724 <phase_3+0x85>

371f:    e8 8c 07 00 00            callq  3eb0 <explode_bomb>

3724:    48 8b 44 24 08            mov    0x8(%rsp),%rax

3729:    64 48 33 04 25 28 00      xor    %fs:0x28,%rax

3730:    00 00

3732:    75 42                     jne    3776 <phase_3+0xd7>

3734:    48 83 c4 18               add    $0x18,%rsp

3738:    c3                        retq

3739:    b8 00 00 00 00            mov    $0x0,%eax

373e:    eb ba                     jmp    36fa <phase_3+0x5b>

3740:    b8 00 00 00 00            mov    $0x0,%eax

3745:    eb b8                     jmp    36ff <phase_3+0x60>

3747:    b8 00 00 00 00            mov    $0x0,%eax

374c:    eb b6                     jmp    3704 <phase_3+0x65>

374e:    b8 00 00 00 00            mov    $0x0,%eax

3753:    eb b2                     jmp    3707 <phase_3+0x68>

3755:    b8 00 00 00 00            mov    $0x0,%eax

375a:    eb ae                     jmp    370a <phase_3+0x6b>

375c:    b8 00 00 00 00            mov    $0x0,%eax

3761:    eb aa                     jmp    370d <phase_3+0x6e>

3763:    b8 00 00 00 00            mov    $0x0,%eax

3768:    eb a6                     jmp    3710 <phase_3+0x71>

376a:    e8 41 07 00 00            callq  3eb0 <explode_bomb>

376f:    b8 00 00 00 00            mov    $0x0,%eax

3774:    eb 9d                     jmp    3713 <phase_3+0x74>

3776:    e8 f5 fa ff ff            callq  3270 <__stack_chk_fail@plt>
```

```
000000000000377b <func4>:

   377b:       f3 0f 1e fa             endbr64

   377f:       b8 00 00 00 00          mov    $0x0,%eax

   3784:       85 ff                   test   %edi,%edi

   3786:       7e 2d                   jle    37b5 <func4+0x3a>

   3788:       41 54                   push   %r12

   378a:       55                      push   %rbp

   378b:       53                      push   %rbx

   378c:       89 fb                   mov    %edi,%ebx

   378e:       89 f5                   mov    %esi,%ebp

   3790:       89 f0                   mov    %esi,%eax

   3792:       83 ff 01                cmp    $0x1,%edi

   3795:       74 19                   je     37b0 <func4+0x35>

   3797:       8d 7f ff                lea    -0x1(%rdi),%edi

   379a:       e8 dc ff ff ff          callq  377b <func4>

   379f:       44 8d 24 28             lea    (%rax,%rbp,1),%r12d

   37a3:       8d 7b fe                lea    -0x2(%rbx),%edi

   37a6:       89 ee                   mov    %ebp,%esi

   37a8:       e8 ce ff ff ff          callq  377b <func4>

   37ad:       44 01 e0                add    %r12d,%eax

   37b0:       5b                      pop    %rbx

   37b1:       5d                      pop    %rbp

   37b2:       41 5c                   pop    %r12

   37b4:       c3                      retq

   37b5:       c3                      retq
```

Phase_4 | I don't even know

This one can vary. If you get a super long func4, it's probably a palindrome. Try just like two number sets like 54345 and 65456 or something about that.

Otherwise you might get a one argument palindrome. In that case try something liek 65456

Otherwise you might just get two numbers like mine. I had 216 and 4.

```
00000000000037b6 <phase_4>:
    37b6:    f3 0f 1e fa                endbr64
    37ba:    48 83 ec 18                sub    $0x18,%rsp
    37be:    64 48 8b 04 25 28 00       mov    %fs:0x28,%rax
    37c5:    00 00
    37c7:    48 89 44 24 08             mov    %rax,0x8(%rsp)
    37cc:    31 c0                      xor    %eax,%eax
    37ce:    48 89 e1                   mov    %rsp,%rcx
    37d1:    48 8d 54 24 04             lea    0x4(%rsp),%rdx
    37d6:    48 8d 35 07 1d 00 00       lea    0x1d07(%rip),%rsi        # 54e4
<array.3481+0x304>
    37dd:    e8 2e fb ff ff             callq  3310 <__isoc99_sscanf@plt>
    37e2:    83 f8 02        2 inputs   cmp    $0x2,%eax
    37e5:    75 0b                      jne    37f2 <phase_4+0x3c>
    37e7:    8b 04 24                   mov    (%rsp),%eax
    37ea:    83 e8 02                   sub    $0x2,%eax
    37ed:    83 f8 02                   cmp    $0x2,%eax
    37f0:    76 05                      jbe    37f7 <phase_4+0x41>
    37f2:    e8 b9 06 00 00             callq  3eb0 <explode_bomb>
    37f7:    8b 34 24                   mov    (%rsp),%esi
    37fa:    bf 08 00 00 00             mov    $0x8,%edi
    37ff:    e8 77 ff ff ff             callq  377b <func4>
    3804:    39 44 24 04                cmp    %eax,0x4(%rsp)
    3808:    75 15                      jne    381f <phase_4+0x69>
    380a:    48 8b 44 24 08             mov    0x8(%rsp),%rax
    380f:    64 48 33 04 25 28 00       xor    %fs:0x28,%rax
    3816:    00 00
    3818:    75 0c                      jne    3826 <phase_4+0x70>
    381a:    48 83 c4 18                add    $0x18,%rsp
    381e:    c3                         retq
    381f:    e8 8c 06 00 00             callq  3eb0 <explode_bomb>
```

```
   3824:      eb e4                          jmp     380a <phase_4+0x54>

   3826:      e8 45 fa ff ff                 callq   3270 <__stack_chk_fail@plt>
```

Phase_5 | Indexing or whatever

This one I had to do **x/Indexd $reg** where Index stands for a specific index.

Since integers are 4 bytes I did multiples of 4 for indexes so for example **x/5d $rg** I do 5 instead of 4 since index starts at 0.

So in the end I figured out that I needed the memory address of ecx to match like 0x32 and that was 50 in decimal so my numbers had to index into this array and then add up to 50.

My final answer was: 444288

```
000000000000382b <phase_5>:
   382b:      f3 0f 1e fa                    endbr64

   382f:      53                             push    %rbx

   3830:      48 83 ec 60                    sub     $0x60,%rsp

   3834:      64 48 8b 04 25 28 00           mov     %fs:0x28,%rax

   383b:      00 00

   383d:      48 89 44 24 58                 mov     %rax,0x58(%rsp)

   3842:      31 c0                          xor     %eax,%eax

   3844:      48 89 e3                       mov     %rsp,%rbx

   3847:      48 89 da                       mov     %rbx,%rdx

   384a:      48 8d 35 02 1d 00 00           lea     0x1d02(%rip),%rsi         # 5553
<array.3481+0x373>
   3851:      e8 ba fa ff ff                 callq   3310 <__isoc99_sscanf@plt>

   3856:      48 89 df                       mov     %rbx,%rdi
```

<mark>   3859:   e8 e7 02 00 00   input = 1 arg   callq   3b45 <string_length></mark>

<mark>   385e: 83 f8 06   length of input has to = 6   cmp $0x6,%eax</mark>

```
   3861:      75 41                          jne     38a4 <phase_5+0x79>

   3863:      48 89 e0                       mov     %rsp,%rax

   3866:      48 8d 7c 24 06                 lea     0x6(%rsp),%rdi

   386b:      b9 00 00 00 00                 mov     $0x0,%ecx
```

```
3870:      48 8d 35 69 19 00 00      lea     0x1969(%rip),%rsi        # 51e0 <array.3481>

3877:      0f b6 10                  movzbl (%rax),%edx

387a:      83 e2 0f                  and     $0xf,%edx

387d:      03 0c 96     indexing with input numbers add     (%rsi,%rdx,4),%ecx

3880:      48 83 c0 01               add     $0x1,%rax

3884:      48 39 f8                  cmp     %rdi,%rax

3887:      75 ee                     jne     3877 <phase_5+0x4c>


3889:      83 f9 32     memory add. of ecx has to = 0x32 cmp     $0x32,%ecx

388c:      75 1d                     jne     38ab <phase_5+0x80>

388e:      48 8b 44 24 58            mov     0x58(%rsp),%rax

3893:      64 48 33 04 25 28 00      xor     %fs:0x28,%rax

389a:      00 00

389c:      75 14                     jne     38b2 <phase_5+0x87>

389e:      48 83 c4 60               add     $0x60,%rsp

38a2:      5b                        pop     %rbx

38a3:      c3                        retq

38a4:      e8 07 06 00 00            callq   3eb0 <explode_bomb>

38a9:      eb b8                     jmp     3863 <phase_5+0x38>

38ab:      e8 00 06 00 00            callq   3eb0 <explode_bomb>

38b0:      eb dc                     jmp     388e <phase_5+0x63>

38b2:      e8 b9 f9 ff ff            callq   3270 <__stack_chk_fail@plt>
```

Phase_6 | binary tree

The guides I linked on top had a good overview of this. It's a binary tree. I didn't do this.

```
00000000000038b7 <phase_6>:

38b7:      f3 0f 1e fa               endbr64

38bb:      41 57                     push    %r15

38bd:      41 56                     push    %r14

38bf:      41 55                     push    %r13
```

```
38c1:     41 54                    push   %r12

38c3:     55                       push   %rbp

38c4:     53                       push   %rbx

38c5:     48 83 ec 68              sub    $0x68,%rsp

38c9:     64 48 8b 04 25 28 00     mov    %fs:0x28,%rax

38d0:     00 00

38d2:     48 89 44 24 58           mov    %rax,0x58(%rsp)

38d7:     31 c0                    xor    %eax,%eax

38d9:     49 89 e6                 mov    %rsp,%r14

38dc:     4c 89 f6                 mov    %r14,%rsi

38df:     e8 0e 06 00 00           callq  3ef2 <read_six_numbers>

38e4:     4d 89 f4                 mov    %r14,%r12

38e7:     41 bf 01 00 00 00        mov    $0x1,%r15d

38ed:     49 89 e5                 mov    %rsp,%r13

38f0:     e9 c1 00 00 00           jmpq   39b6 <phase_6+0xff>

38f5:     e8 b6 05 00 00           callq  3eb0 <explode_bomb>

38fa:     e9 c9 00 00 00           jmpq   39c8 <phase_6+0x111>

38ff:     e8 ac 05 00 00           callq  3eb0 <explode_bomb>

3904:     48 83 c3 01              add    $0x1,%rbx

3908:     83 fb 05                 cmp    $0x5,%ebx

390b:     0f 8f 9d 00 00 00        jg     39ae <phase_6+0xf7>

3911:     41 8b 44 9d 00           mov    0x0(%r13,%rbx,4),%eax

3916:     39 45 00                 cmp    %eax,0x0(%rbp)

3919:     75 e9                    jne    3904 <phase_6+0x4d>

391b:     eb e2                    jmp    38ff <phase_6+0x48>

391d:     49 8d 4c 24 18           lea    0x18(%r12),%rcx

3922:     ba 07 00 00 00           mov    $0x7,%edx

3927:     89 d0                    mov    %edx,%eax

3929:     41 2b 04 24              sub    (%r12),%eax

392d:     41 89 04 24              mov    %eax,(%r12)

3931:     49 83 c4 04              add    $0x4,%r12

3935:     4c 39 e1                 cmp    %r12,%rcx
```

```
3938:    75 ed                      jne    3927 <phase_6+0x70>

393a:    be 00 00 00 00            mov    $0x0,%esi

393f:    8b 0c b4                  mov    (%rsp,%rsi,4),%ecx

3942:    b8 01 00 00 00            mov    $0x1,%eax

3947:    48 8d 15 e2 48 00 00      lea    0x48e2(%rip),%rdx        # 8230 <node1>

394e:    83 f9 01                  cmp    $0x1,%ecx

3951:    7e 0b                     jle    395e <phase_6+0xa7>

3953:    48 8b 52 08               mov    0x8(%rdx),%rdx

3957:    83 c0 01                  add    $0x1,%eax

395a:    39 c8                     cmp    %ecx,%eax

395c:    75 f5                     jne    3953 <phase_6+0x9c>

395e:    48 89 54 f4 20            mov    %rdx,0x20(%rsp,%rsi,8)

3963:    48 83 c6 01               add    $0x1,%rsi

3967:    48 83 fe 06               cmp    $0x6,%rsi

396b:    75 d2                     jne    393f <phase_6+0x88>

396d:    48 8b 5c 24 20            mov    0x20(%rsp),%rbx

3972:    48 8b 44 24 28            mov    0x28(%rsp),%rax

3977:    48 89 43 08               mov    %rax,0x8(%rbx)

397b:    48 8b 54 24 30            mov    0x30(%rsp),%rdx

3980:    48 89 50 08               mov    %rdx,0x8(%rax)

3984:    48 8b 44 24 38            mov    0x38(%rsp),%rax

3989:    48 89 42 08               mov    %rax,0x8(%rdx)

398d:    48 8b 54 24 40            mov    0x40(%rsp),%rdx

3992:    48 89 50 08               mov    %rdx,0x8(%rax)

3996:    48 8b 44 24 48            mov    0x48(%rsp),%rax

399b:    48 89 42 08               mov    %rax,0x8(%rdx)

399f:    48 c7 40 08 00 00 00      movq   $0x0,0x8(%rax)

39a6:    00

39a7:    bd 05 00 00 00            mov    $0x5,%ebp

39ac:    eb 35                     jmp    39e3 <phase_6+0x12c>

39ae:    49 83 c7 01               add    $0x1,%r15

39b2:    49 83 c6 04               add    $0x4,%r14
```

```
39b6:    4c 89 f5                mov    %r14,%rbp
39b9:    41 8b 06                mov    (%r14),%eax
39bc:    83 e8 01                sub    $0x1,%eax
39bf:    83 f8 05                cmp    $0x5,%eax
39c2:    0f 87 2d ff ff ff       ja     38f5 <phase_6+0x3e>
39c8:    41 83 ff 05             cmp    $0x5,%r15d
39cc:    0f 8f 4b ff ff ff       jg     391d <phase_6+0x66>
39d2:    4c 89 fb                mov    %r15,%rbx
39d5:    e9 37 ff ff ff          jmpq   3911 <phase_6+0x5a>
39da:    48 8b 5b 08             mov    0x8(%rbx),%rbx
39de:    83 ed 01                sub    $0x1,%ebp
39e1:    74 11                   je     39f4 <phase_6+0x13d>
39e3:    48 8b 43 08             mov    0x8(%rbx),%rax
39e7:    8b 00                   mov    (%rax),%eax
39e9:    39 03                   cmp    %eax,(%rbx)
39eb:    7d ed                   jge    39da <phase_6+0x123>
39ed:    e8 be 04 00 00          callq  3eb0 <explode_bomb>
39f2:    eb e6                   jmp    39da <phase_6+0x123>
39f4:    48 8b 44 24 58          mov    0x58(%rsp),%rax
39f9:    64 48 33 04 25 28 00    xor    %fs:0x28,%rax
3a00:    00 00
3a02:    75 0f                   jne    3a13 <phase_6+0x15c>
3a04:    48 83 c4 68             add    $0x68,%rsp
3a08:    5b                      pop    %rbx
3a09:    5d                      pop    %rbp
3a0a:    41 5c                   pop    %r12
3a0c:    41 5d                   pop    %r13
3a0e:    41 5e                   pop    %r14
3a10:    41 5f                   pop    %r15
3a12:    c3                      retq
3a13:    e8 58 f8 ff ff          callq  3270 <__stack_chk_fail@plt>
```

```
0000000000003a18 <fun7>:

  3a18:    f3 0f 1e fa                endbr64
  3a1c:    48 85 ff                   test   %rdi,%rdi
  3a1f:    74 32                      je     3a53 <fun7+0x3b>
  3a21:    48 83 ec 08                sub    $0x8,%rsp
  3a25:    8b 17                      mov    (%rdi),%edx
  3a27:    39 f2                      cmp    %esi,%edx
  3a29:    7f 0c                      jg     3a37 <fun7+0x1f>
  3a2b:    b8 00 00 00 00             mov    $0x0,%eax
  3a30:    75 12                      jne    3a44 <fun7+0x2c>
  3a32:    48 83 c4 08                add    $0x8,%rsp
  3a36:    c3                         retq
  3a37:    48 8b 7f 08                mov    0x8(%rdi),%rdi
  3a3b:    e8 d8 ff ff ff             callq  3a18 <fun7>
  3a40:    01 c0                      add    %eax,%eax
  3a42:    eb ee                      jmp    3a32 <fun7+0x1a>
  3a44:    48 8b 7f 10                mov    0x10(%rdi),%rdi
  3a48:    e8 cb ff ff ff             callq  3a18 <fun7>
  3a4d:    8d 44 00 01                lea    0x1(%rax,%rax,1),%eax
  3a51:    eb df                      jmp    3a32 <fun7+0x1a>
  3a53:    b8 ff ff ff ff             mov    $0xffffffff,%eax
  3a58:    c3                         retq
```

Phase_7 | secret phase

Yeah I skipped this. Look at the guides for this

```
0000000000003a59 <secret_phase>:

  3a59:    f3 0f 1e fa                endbr64
  3a5d:    53                         push   %rbx
  3a5e:    e8 d4 04 00 00             callq  3f37 <read_line>
```

```
   3a63:    48 89 c7                    mov    %rax,%rdi

   3a66:    ba 0a 00 00 00              mov    $0xa,%edx

   3a6b:    be 00 00 00 00             mov    $0x0,%esi

   3a70:    e8 7b f8 ff ff             callq  32f0 <strtol@plt>

   3a75:    48 89 c3                    mov    %rax,%rbx

   3a78:    8d 40 ff                    lea    -0x1(%rax),%eax

   3a7b:    3d e8 03 00 00             cmp    $0x3e8,%eax

   3a80:    77 26                       ja     3aa8 <secret_phase+0x4f>

   3a82:    89 de                       mov    %ebx,%esi

   3a84:    48 8d 3d c5 46 00 00        lea    0x46c5(%rip),%rdi        # 8150 <n1>

   3a8b:    e8 88 ff ff ff             callq  3a18 <fun7>

   3a90:    83 f8 01                    cmp    $0x1,%eax

   3a93:    75 1a                       jne    3aaf <secret_phase+0x56>

   3a95:    48 8d 3d ec 16 00 00        lea    0x16ec(%rip),%rdi        # 5188
<_IO_stdin_used+0x188>
   3a9c:    e8 af f7 ff ff             callq  3250 <puts@plt>

   3aa1:    e8 d9 05 00 00             callq  407f <phase_defused>

   3aa6:    5b                          pop    %rbx

   3aa7:    c3                          retq

   3aa8:    e8 03 04 00 00             callq  3eb0 <explode_bomb>

   3aad:    eb d3                       jmp    3a82 <secret_phase+0x29>

   3aaf:    e8 fc 03 00 00             callq  3eb0 <explode_bomb>

   3ab4:    eb df                       jmp    3a95 <secret_phase+0x3c>


0000000000003ab6 <sig_handler>:

   3ab6:    f3 0f 1e fa                 endbr64

   3aba:    50                          push   %rax

   3abb:    58                          pop    %rax

   3abc:    48 83 ec 08                 sub    $0x8,%rsp

   3ac0:    48 8d 3d 59 17 00 00        lea    0x1759(%rip),%rdi        # 5220
<array.3481+0x40>
   3ac7:    e8 84 f7 ff ff             callq  3250 <puts@plt>
```

```
   3acc:    bf 03 00 00 00            mov     $0x3,%edi
   3ad1:    e8 aa f8 ff ff            callq   3380 <sleep@plt>
   3ad6:    48 8d 35 61 19 00 00      lea     0x1961(%rip),%rsi      # 543e
<array.3481+0x25e>
   3add:    bf 01 00 00 00            mov     $0x1,%edi
   3ae2:    b8 00 00 00 00            mov     $0x0,%eax
   3ae7:    e8 34 f8 ff ff            callq   3320 <__printf_chk@plt>
   3aec:    48 8b 3d 8d 57 00 00      mov     0x578d(%rip),%rdi      # 9280
<stdout@@GLIBC_2.2.5>
   3af3:    e8 08 f8 ff ff            callq   3300 <fflush@plt>
   3af8:    bf 01 00 00 00            mov     $0x1,%edi
   3afd:    e8 7e f8 ff ff            callq   3380 <sleep@plt>
   3b02:    48 8d 3d 3d 19 00 00      lea     0x193d(%rip),%rdi      # 5446
<array.3481+0x266>
   3b09:    e8 42 f7 ff ff            callq   3250 <puts@plt>
   3b0e:    bf 10 00 00 00            mov     $0x10,%edi
   3b13:    e8 38 f8 ff ff            callq   3350 <exit@plt>


0000000000003b18 <invalid_phase>:
   3b18:    f3 0f 1e fa               endbr64
   3b1c:    50                        push    %rax
   3b1d:    58                        pop     %rax
   3b1e:    48 83 ec 08               sub     $0x8,%rsp
   3b22:    48 89 fa                  mov     %rdi,%rdx
   3b25:    48 8d 35 22 19 00 00      lea     0x1922(%rip),%rsi      # 544e
<array.3481+0x26e>
   3b2c:    bf 01 00 00 00            mov     $0x1,%edi
   3b31:    b8 00 00 00 00            mov     $0x0,%eax
   3b36:    e8 e5 f7 ff ff            callq   3320 <__printf_chk@plt>
   3b3b:    bf 08 00 00 00            mov     $0x8,%edi
   3b40:    e8 0b f8 ff ff            callq   3350 <exit@plt>


0000000000003b45 <string_length>:
```

```
3b45:      f3 0f 1e fa                endbr64

3b49:      80 3f 00                   cmpb   $0x0,(%rdi)

3b4c:      74 12                      je     3b60 <string_length+0x1b>

3b4e:      b8 00 00 00 00             mov    $0x0,%eax

3b53:      48 83 c7 01                add    $0x1,%rdi

3b57:      83 c0 01                   add    $0x1,%eax

3b5a:      80 3f 00                   cmpb   $0x0,(%rdi)

3b5d:      75 f4                      jne    3b53 <string_length+0xe>

3b5f:      c3                         retq

3b60:      b8 00 00 00 00             mov    $0x0,%eax

3b65:      c3                         retq


0000000000003b66 <strings_not_equal>:

3b66:      f3 0f 1e fa                endbr64

3b6a:      41 54                      push   %r12

3b6c:      55                         push   %rbp

3b6d:      53                         push   %rbx

3b6e:      48 89 fb                   mov    %rdi,%rbx

3b71:      48 89 f5                   mov    %rsi,%rbp

3b74:      e8 cc ff ff ff             callq  3b45 <string_length>

3b79:      41 89 c4                   mov    %eax,%r12d

3b7c:      48 89 ef                   mov    %rbp,%rdi

3b7f:      e8 c1 ff ff ff             callq  3b45 <string_length>

3b84:      89 c2                      mov    %eax,%edx

3b86:      b8 01 00 00 00             mov    $0x1,%eax

3b8b:      41 39 d4                   cmp    %edx,%r12d

3b8e:      75 31                      jne    3bc1 <strings_not_equal+0x5b>

3b90:      0f b6 13                   movzbl (%rbx),%edx

3b93:      84 d2                      test   %dl,%dl

3b95:      74 1e                      je     3bb5 <strings_not_equal+0x4f>

3b97:      b8 00 00 00 00             mov    $0x0,%eax
```

```
3b9c:      38 54 05 00              cmp    %dl,0x0(%rbp,%rax,1)

3ba0:      75 1a                    jne    3bbc <strings_not_equal+0x56>

3ba2:      48 83 c0 01              add    $0x1,%rax

3ba6:      0f b6 14 03              movzbl (%rbx,%rax,1),%edx

3baa:      84 d2                    test   %dl,%dl

3bac:      75 ee                    jne    3b9c <strings_not_equal+0x36>

3bae:      b8 00 00 00 00           mov    $0x0,%eax

3bb3:      eb 0c                    jmp    3bc1 <strings_not_equal+0x5b>

3bb5:      b8 00 00 00 00           mov    $0x0,%eax

3bba:      eb 05                    jmp    3bc1 <strings_not_equal+0x5b>

3bbc:      b8 01 00 00 00           mov    $0x1,%eax

3bc1:      5b                       pop    %rbx

3bc2:      5d                       pop    %rbp

3bc3:      41 5c                    pop    %r12

3bc5:      c3                       retq


0000000000003bc6 <initialize_bomb>:

3bc6:      f3 0f 1e fa              endbr64

3bca:      55                       push   %rbp

3bcb:      53                       push   %rbx

3bcc:      48 81 ec 00 10 00 00     sub    $0x1000,%rsp

3bd3:      48 83 0c 24 00           orq    $0x0,(%rsp)

3bd8:      48 81 ec 00 10 00 00     sub    $0x1000,%rsp

3bdf:      48 83 0c 24 00           orq    $0x0,(%rsp)

3be4:      48 83 ec 58              sub    $0x58,%rsp

3be8:      64 48 8b 04 25 28 00     mov    %fs:0x28,%rax

3bef:      00 00

3bf1:      48 89 84 24 48 20 00     mov    %rax,0x2048(%rsp)

3bf8:      00

3bf9:      31 c0                    xor    %eax,%eax

3bfb:      48 8d 35 b4 fe ff ff     lea    -0x14c(%rip),%rsi        # 3ab6 <sig_handler>
```

```
3c02:      bf 02 00 00 00              mov     $0x2,%edi

3c07:      e8 b4 f6 ff ff              callq   32c0 <signal@plt>

3c0c:      48 89 e7                    mov     %rsp,%rdi

3c0f:      be 40 00 00 00              mov     $0x40,%esi

3c14:      e8 27 f7 ff ff              callq   3340 <gethostname@plt>

3c19:      85 c0                       test    %eax,%eax

3c1b:      0f 85 9b 00 00 00           jne     3cbc <initialize_bomb+0xf6>

3c21:      48 8b 3d 58 46 00 00        mov     0x4658(%rip),%rdi      # 8280 <host_table>

3c28:      48 8d 1d 59 46 00 00        lea     0x4659(%rip),%rbx      # 8288
<host_table+0x8>
3c2f:      48 89 e5                    mov     %rsp,%rbp

3c32:      48 85 ff                    test    %rdi,%rdi

3c35:      74 1d                       je      3c54 <initialize_bomb+0x8e>

3c37:      48 89 ee                    mov     %rbp,%rsi

3c3a:      e8 e1 f5 ff ff              callq   3220 <strcasecmp@plt>

3c3f:      85 c0                       test    %eax,%eax

3c41:      0f 84 b0 00 00 00           je      3cf7 <initialize_bomb+0x131>

3c47:      48 83 c3 08                 add     $0x8,%rbx

3c4b:      48 8b 7b f8                 mov     -0x8(%rbx),%rdi

3c4f:      48 85 ff                    test    %rdi,%rdi

3c52:      75 e3                       jne     3c37 <initialize_bomb+0x71>

3c54:      48 89 e2                    mov     %rsp,%rdx

3c57:      48 8d 35 32 16 00 00        lea     0x1632(%rip),%rsi      # 5290
<array.3481+0xb0>
3c5e:      bf 01 00 00 00              mov     $0x1,%edi

3c63:      b8 00 00 00 00              mov     $0x0,%eax

3c68:      e8 b3 f6 ff ff              callq   3320 <__printf_chk@plt>

3c6d:      48 8d 3d 0b 18 00 00        lea     0x180b(%rip),%rdi      # 547f
<array.3481+0x29f>
3c74:      e8 d7 f5 ff ff              callq   3250 <puts@plt>

3c79:      48 8b 15 00 46 00 00        mov     0x4600(%rip),%rdx      # 8280 <host_table>

3c80:      48 8d 1d 01 46 00 00        lea     0x4601(%rip),%rbx      # 8288
<host_table+0x8>
```

```
3c87:    48 8d 2d d1 17 00 00    lea    0x17d1(%rip),%rbp       # 545f
<array.3481+0x27f>
3c8e:    48 85 d2                test   %rdx,%rdx
3c91:    74 1f                   je     3cb2 <initialize_bomb+0xec>
3c93:    48 89 ee                mov    %rbp,%rsi
3c96:    bf 01 00 00 00          mov    $0x1,%edi
3c9b:    b8 00 00 00 00          mov    $0x0,%eax
3ca0:    e8 7b f6 ff ff          callq  3320 <__printf_chk@plt>
3ca5:    48 83 c3 08             add    $0x8,%rbx
3ca9:    48 8b 53 f8             mov    -0x8(%rbx),%rdx
3cad:    48 85 d2                test   %rdx,%rdx
3cb0:    75 e1                   jne    3c93 <initialize_bomb+0xcd>
3cb2:    bf 08 00 00 00          mov    $0x8,%edi
3cb7:    e8 94 f6 ff ff          callq  3350 <exit@plt>
3cbc:    48 8d 3d 95 15 00 00    lea    0x1595(%rip),%rdi       # 5258
<array.3481+0x78>
3cc3:    e8 88 f5 ff ff          callq  3250 <puts@plt>
3cc8:    bf 08 00 00 00          mov    $0x8,%edi
3ccd:    e8 7e f6 ff ff          callq  3350 <exit@plt>
3cd2:    48 8d 54 24 40          lea    0x40(%rsp),%rdx
3cd7:    48 8d 35 87 17 00 00    lea    0x1787(%rip),%rsi       # 5465
<array.3481+0x285>
3cde:    bf 01 00 00 00          mov    $0x1,%edi
3ce3:    b8 00 00 00 00          mov    $0x0,%eax
3ce8:    e8 33 f6 ff ff          callq  3320 <__printf_chk@plt>
3ced:    bf 08 00 00 00          mov    $0x8,%edi
3cf2:    e8 59 f6 ff ff          callq  3350 <exit@plt>
3cf7:    48 8d 7c 24 40          lea    0x40(%rsp),%rdi
3cfc:    e8 ea 0e 00 00          callq  4beb <init_driver>
3d01:    85 c0                   test   %eax,%eax
3d03:    78 cd                   js     3cd2 <initialize_bomb+0x10c>
3d05:    48 8b 84 24 48 20 00    mov    0x2048(%rsp),%rax
3d0c:    00
```

```
3d0d:      64 48 33 04 25 28 00        xor      %fs:0x28,%rax
3d14:      00 00
3d16:      75 0a                       jne      3d22 <initialize_bomb+0x15c>
3d18:      48 81 c4 58 20 00 00        add      $0x2058,%rsp
3d1f:      5b                          pop      %rbx
3d20:      5d                          pop      %rbp
3d21:      c3                          retq
3d22:      e8 49 f5 ff ff              callq    3270 <__stack_chk_fail@plt>


0000000000003d27 <initialize_bomb_solve>:
3d27:      f3 0f 1e fa                 endbr64
3d2b:      c3                          retq


0000000000003d2c <blank_line>:
3d2c:      f3 0f 1e fa                 endbr64
3d30:      55                          push     %rbp
3d31:      53                          push     %rbx
3d32:      48 83 ec 08                 sub      $0x8,%rsp
3d36:      48 89 fd                    mov      %rdi,%rbp
3d39:      0f b6 5d 00                 movzbl   0x0(%rbp),%ebx
3d3d:      84 db                       test     %bl,%bl
3d3f:      74 1e                       je       3d5f <blank_line+0x33>
3d41:      e8 4a f6 ff ff              callq    3390 <__ctype_b_loc@plt>
3d46:      48 83 c5 01                 add      $0x1,%rbp
3d4a:      48 0f be db                 movsbq   %bl,%rbx
3d4e:      48 8b 00                    mov      (%rax),%rax
3d51:      f6 44 58 01 20              testb    $0x20,0x1(%rax,%rbx,2)
3d56:      75 e1                       jne      3d39 <blank_line+0xd>
3d58:      b8 00 00 00 00              mov      $0x0,%eax
3d5d:      eb 05                       jmp      3d64 <blank_line+0x38>
3d5f:      b8 01 00 00 00              mov      $0x1,%eax
```

```
  3d64:     48 83 c4 08                 add    $0x8,%rsp

  3d68:     5b                          pop    %rbx

  3d69:     5d                          pop    %rbp

  3d6a:     c3                          retq


0000000000003d6b <skip>:

  3d6b:     f3 0f 1e fa                 endbr64

  3d6f:     55                          push   %rbp

  3d70:     53                          push   %rbx

  3d71:     48 83 ec 08                 sub    $0x8,%rsp

  3d75:     48 8d 2d 44 55 00 00        lea    0x5544(%rip),%rbp        # 92c0
<input_strings>
  3d7c:     48 63 05 29 55 00 00        movslq 0x5529(%rip),%rax        # 92ac
<num_input_strings>
  3d83:     48 8d 3c 80                 lea    (%rax,%rax,4),%rdi

  3d87:     48 c1 e7 04                 shl    $0x4,%rdi

  3d8b:     48 01 ef                    add    %rbp,%rdi

  3d8e:     48 8b 15 1b 55 00 00        mov    0x551b(%rip),%rdx        # 92b0 <infile>

  3d95:     be 50 00 00 00              mov    $0x50,%esi

  3d9a:     e8 11 f5 ff ff              callq  32b0 <fgets@plt>

  3d9f:     48 89 c3                    mov    %rax,%rbx

  3da2:     48 85 c0                    test   %rax,%rax

  3da5:     74 0c                       je     3db3 <skip+0x48>

  3da7:     48 89 c7                    mov    %rax,%rdi

  3daa:     e8 7d ff ff ff              callq  3d2c <blank_line>

  3daf:     85 c0                       test   %eax,%eax

  3db1:     75 c9                       jne    3d7c <skip+0x11>

  3db3:     48 89 d8                    mov    %rbx,%rax

  3db6:     48 83 c4 08                 add    $0x8,%rsp

  3dba:     5b                          pop    %rbx

  3dbb:     5d                          pop    %rbp

  3dbc:     c3                          retq
```

```
0000000000003dbd <send_msg>:

   3dbd:    f3 0f 1e fa                endbr64
   3dc1:    53                         push   %rbx
   3dc2:    4c 8d 9c 24 00 c0 ff       lea    -0x4000(%rsp),%r11
   3dc9:    ff
   3dca:    48 81 ec 00 10 00 00       sub    $0x1000,%rsp
   3dd1:    48 83 0c 24 00             orq    $0x0,(%rsp)
   3dd6:    4c 39 dc                   cmp    %r11,%rsp
   3dd9:    75 ef                      jne    3dca <send_msg+0xd>
   3ddb:    48 83 ec 10                sub    $0x10,%rsp
   3ddf:    64 48 8b 04 25 28 00       mov    %fs:0x28,%rax
   3de6:    00 00
   3de8:    48 89 84 24 08 40 00       mov    %rax,0x4008(%rsp)
   3def:    00
   3df0:    31 c0                      xor    %eax,%eax
   3df2:    8b 15 b4 54 00 00          mov    0x54b4(%rip),%edx        # 92ac
<num_input_strings>
   3df8:    8d 42 ff                   lea    -0x1(%rdx),%eax
   3dfb:    48 98                      cltq
   3dfd:    48 8d 04 80                lea    (%rax,%rax,4),%rax
   3e01:    48 c1 e0 04                shl    $0x4,%rax
   3e05:    48 8d 0d b4 54 00 00       lea    0x54b4(%rip),%rcx        # 92c0
<input_strings>
   3e0c:    48 01 c8                   add    %rcx,%rax
   3e0f:    85 ff                      test   %edi,%edi
   3e11:    4c 8d 0d 83 16 00 00       lea    0x1683(%rip),%r9         # 549b
<array.3481+0x2bb>
   3e18:    48 8d 0d 84 16 00 00       lea    0x1684(%rip),%rcx        # 54a3
<array.3481+0x2c3>
   3e1f:    4c 0f 44 c9                cmove  %rcx,%r9
   3e23:    48 89 e3                   mov    %rsp,%rbx
   3e26:    50                         push   %rax
```

```
3e27:       52                          push    %rdx
3e28:       44 8b 05 15 43 00 00        mov     0x4315(%rip),%r8d      # 8144 <bomb_id>
3e2f:       48 8d 0d 76 16 00 00        lea     0x1676(%rip),%rcx      # 54ac
<array.3481+0x2cc>
3e36:       ba 00 20 00 00              mov     $0x2000,%edx
3e3b:       be 01 00 00 00              mov     $0x1,%esi
3e40:       48 89 df                    mov     %rbx,%rdi
3e43:       b8 00 00 00 00              mov     $0x0,%eax
3e48:       e8 53 f5 ff ff              callq   33a0 <__sprintf_chk@plt>
3e4d:       4c 8d 84 24 10 20 00        lea     0x2010(%rsp),%r8
3e54:       00
3e55:       b9 00 00 00 00              mov     $0x0,%ecx
3e5a:       48 89 da                    mov     %rbx,%rdx
3e5d:       48 8d 35 bc 42 00 00        lea     0x42bc(%rip),%rsi      # 8120
<user_password>
3e64:       48 8d 3d cd 42 00 00        lea     0x42cd(%rip),%rdi      # 8138 <userid>
3e6b:       e8 70 0f 00 00              callq   4de0 <driver_post>
3e70:       48 83 c4 10                 add     $0x10,%rsp
3e74:       85 c0                       test    %eax,%eax
3e76:       78 1c                       js      3e94 <send_msg+0xd7>
3e78:       48 8b 84 24 08 40 00        mov     0x4008(%rsp),%rax
3e7f:       00
3e80:       64 48 33 04 25 28 00        xor     %fs:0x28,%rax
3e87:       00 00
3e89:       75 20                       jne     3eab <send_msg+0xee>
3e8b:       48 81 c4 10 40 00 00        add     $0x4010,%rsp
3e92:       5b                          pop     %rbx
3e93:       c3                          retq
3e94:       48 8d bc 24 00 20 00        lea     0x2000(%rsp),%rdi
3e9b:       00
3e9c:       e8 af f3 ff ff              callq   3250 <puts@plt>
3ea1:       bf 00 00 00 00              mov     $0x0,%edi
3ea6:       e8 a5 f4 ff ff              callq   3350 <exit@plt>
```

```
   3eab:    e8 c0 f3 ff ff            callq  3270 <__stack_chk_fail@plt>


0000000000003eb0 <explode_bomb>:
   3eb0:    f3 0f 1e fa               endbr64
   3eb4:    50                        push   %rax
   3eb5:    58                        pop    %rax
   3eb6:    48 83 ec 08               sub    $0x8,%rsp
   3eba:    48 8d 3d f7 15 00 00      lea    0x15f7(%rip),%rdi        # 54b8
<array.3481+0x2d8>
   3ec1:    e8 8a f3 ff ff            callq  3250 <puts@plt>
   3ec6:    48 8d 3d f4 15 00 00      lea    0x15f4(%rip),%rdi        # 54c1
<array.3481+0x2e1>
   3ecd:    e8 7e f3 ff ff            callq  3250 <puts@plt>
   3ed2:    bf 00 00 00 00            mov    $0x0,%edi
   3ed7:    e8 e1 fe ff ff            callq  3dbd <send_msg>
   3edc:    48 8d 3d dd 13 00 00      lea    0x13dd(%rip),%rdi        # 52c0
<array.3481+0xe0>
   3ee3:    e8 68 f3 ff ff            callq  3250 <puts@plt>
   3ee8:    bf 08 00 00 00            mov    $0x8,%edi
   3eed:    e8 5e f4 ff ff            callq  3350 <exit@plt>


0000000000003ef2 <read_six_numbers>:
   3ef2:    f3 0f 1e fa               endbr64
   3ef6:    48 83 ec 08               sub    $0x8,%rsp
   3efa:    48 89 f2                  mov    %rsi,%rdx
   3efd:    48 8d 4e 04               lea    0x4(%rsi),%rcx
   3f01:    48 8d 46 14               lea    0x14(%rsi),%rax
   3f05:    50                        push   %rax
   3f06:    48 8d 46 10               lea    0x10(%rsi),%rax
   3f0a:    50                        push   %rax
   3f0b:    4c 8d 4e 0c               lea    0xc(%rsi),%r9
   3f0f:    4c 8d 46 08               lea    0x8(%rsi),%r8
```

```
    3f13:    48 8d 35 be 15 00 00     lea    0x15be(%rip),%rsi        # 54d8
<array.3481+0x2f8>
    3f1a:    b8 00 00 00 00           mov    $0x0,%eax
    3f1f:    e8 ec f3 ff ff           callq  3310 <__isoc99_sscanf@plt>
    3f24:    48 83 c4 10              add    $0x10,%rsp
    3f28:    83 f8 05                 cmp    $0x5,%eax
    3f2b:    7e 05                    jle    3f32 <read_six_numbers+0x40>
    3f2d:    48 83 c4 08              add    $0x8,%rsp
    3f31:    c3                       retq
    3f32:    e8 79 ff ff ff           callq  3eb0 <explode_bomb>


0000000000003f37 <read_line>:
    3f37:    f3 0f 1e fa              endbr64
    3f3b:    48 83 ec 08              sub    $0x8,%rsp
    3f3f:    b8 00 00 00 00           mov    $0x0,%eax
    3f44:    e8 22 fe ff ff           callq  3d6b <skip>
    3f49:    48 85 c0                 test   %rax,%rax
    3f4c:    74 6f                    je     3fbd <read_line+0x86>
    3f4e:    8b 35 58 53 00 00        mov    0x5358(%rip),%esi        # 92ac
<num_input_strings>
    3f54:    48 63 c6                 movslq %esi,%rax
    3f57:    48 8d 14 80              lea    (%rax,%rax,4),%rdx
    3f5b:    48 c1 e2 04              shl    $0x4,%rdx
    3f5f:    48 8d 05 5a 53 00 00     lea    0x535a(%rip),%rax        # 92c0
<input_strings>
    3f66:    48 01 c2                 add    %rax,%rdx
    3f69:    48 c7 c1 ff ff ff ff     mov    $0xffffffffffffffff,%rcx
    3f70:    b8 00 00 00 00           mov    $0x0,%eax
    3f75:    48 89 d7                 mov    %rdx,%rdi
    3f78:    f2 ae                    repnz scas %es:(%rdi),%al
    3f7a:    48 f7 d1                 not    %rcx
    3f7d:    48 83 e9 01              sub    $0x1,%rcx
    3f81:    83 f9 4e                 cmp    $0x4e,%ecx
```

```
3f84:       0f 8f ab 00 00 00         jg      4035 <read_line+0xfe>

3f8a:       83 e9 01                  sub     $0x1,%ecx

3f8d:       48 63 c9                  movslq  %ecx,%rcx

3f90:       48 63 c6                  movslq  %esi,%rax

3f93:       48 8d 04 80               lea     (%rax,%rax,4),%rax

3f97:       48 c1 e0 04               shl     $0x4,%rax

3f9b:       48 89 c7                  mov     %rax,%rdi

3f9e:       48 8d 05 1b 53 00 00      lea     0x531b(%rip),%rax       # 92c0
<input_strings>
3fa5:       48 01 f8                  add     %rdi,%rax

3fa8:       c6 04 08 00               movb    $0x0,(%rax,%rcx,1)

3fac:       83 c6 01                  add     $0x1,%esi

3faf:       89 35 f7 52 00 00         mov     %esi,0x52f7(%rip)       # 92ac
<num_input_strings>
3fb5:       48 89 d0                  mov     %rdx,%rax

3fb8:       48 83 c4 08               add     $0x8,%rsp

3fbc:       c3                        retq

3fbd:       48 8b 05 cc 52 00 00      mov     0x52cc(%rip),%rax       # 9290
<stdin@@GLIBC_2.2.5>
3fc4:       48 39 05 e5 52 00 00      cmp     %rax,0x52e5(%rip)       # 92b0 <infile>

3fcb:       74 1b                     je      3fe8 <read_line+0xb1>

3fcd:       48 8d 3d 34 15 00 00      lea     0x1534(%rip),%rdi       # 5508
<array.3481+0x328>
3fd4:       e8 27 f2 ff ff            callq   3200 <getenv@plt>

3fd9:       48 85 c0                  test    %rax,%rax

3fdc:       74 20                     je      3ffe <read_line+0xc7>

3fde:       bf 00 00 00 00            mov     $0x0,%edi

3fe3:       e8 68 f3 ff ff            callq   3350 <exit@plt>

3fe8:       48 8d 3d fb 14 00 00      lea     0x14fb(%rip),%rdi       # 54ea
<array.3481+0x30a>
3fef:       e8 5c f2 ff ff            callq   3250 <puts@plt>

3ff4:       bf 08 00 00 00            mov     $0x8,%edi

3ff9:       e8 52 f3 ff ff            callq   3350 <exit@plt>

3ffe:       48 8b 05 8b 52 00 00      mov     0x528b(%rip),%rax       # 9290
<stdin@@GLIBC_2.2.5>
```

```
    4005:     48 89 05 a4 52 00 00        mov    %rax,0x52a4(%rip)        # 92b0 <infile>

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

    4011:     e8 55 fd ff ff             callq  3d6b <skip>

    4016:     48 85 c0                   test   %rax,%rax

    4019:     0f 85 2f ff ff ff          jne    3f4e <read_line+0x17>

    401f:     48 8d 3d c4 14 00 00        lea    0x14c4(%rip),%rdi        # 54ea
<array.3481+0x30a>
    4026:     e8 25 f2 ff ff             callq  3250 <puts@plt>

    402b:     bf 00 00 00 00             mov    $0x0,%edi

    4030:     e8 1b f3 ff ff             callq  3350 <exit@plt>

    4035:     48 8d 3d d7 14 00 00        lea    0x14d7(%rip),%rdi        # 5513
<array.3481+0x333>
    403c:     e8 0f f2 ff ff             callq  3250 <puts@plt>

    4041:     8b 05 65 52 00 00          mov    0x5265(%rip),%eax        # 92ac
<num_input_strings>
    4047:     8d 50 01                   lea    0x1(%rax),%edx

    404a:     89 15 5c 52 00 00          mov    %edx,0x525c(%rip)        # 92ac
<num_input_strings>
    4050:     48 98                      cltq

    4052:     48 6b c0 50                imul   $0x50,%rax,%rax

    4056:     48 8d 15 63 52 00 00        lea    0x5263(%rip),%rdx        # 92c0
<input_strings>
    405d:     48 be 2a 2a 2a 74 72        movabs $0x636e7572742a2a2a,%rsi

    4064:     75 6e 63

    4067:     48 bf 61 74 65 64 2a        movabs $0x2a2a2a64657461,%rdi

    406e:     2a 2a 00

    4071:     48 89 34 02                mov    %rsi,(%rdx,%rax,1)

    4075:     48 89 7c 02 08             mov    %rdi,0x8(%rdx,%rax,1)

    407a:     e8 31 fe ff ff             callq  3eb0 <explode_bomb>


000000000000407f <phase_defused>:

    407f:     f3 0f 1e fa                endbr64

    4083:     48 81 ec b8 00 00 00        sub    $0xb8,%rsp

    408a:     64 48 8b 04 25 28 00        mov    %fs:0x28,%rax
```

```
4091:       00 00

4093:       48 89 84 24 a8 00 00        mov    %rax,0xa8(%rsp)

409a:       00

409b:       31 c0                       xor    %eax,%eax

409d:       bf 01 00 00 00              mov    $0x1,%edi

40a2:       e8 16 fd ff ff              callq  3dbd <send_msg>

40a7:       83 3d fe 51 00 00 06        cmpl   $0x6,0x51fe(%rip)        # 92ac
<num_input_strings>
40ae:       74 1f                       je     40cf <phase_defused+0x50>

40b0:       48 8b 84 24 a8 00 00        mov    0xa8(%rsp),%rax

40b7:       00

40b8:       64 48 33 04 25 28 00        xor    %fs:0x28,%rax

40bf:       00 00

40c1:       0f 85 58 01 00 00           jne    421f <phase_defused+0x1a0>

40c7:       48 81 c4 b8 00 00 00        add    $0xb8,%rsp

40ce:       c3                          retq

40cf:       48 8d 4c 24 30              lea    0x30(%rsp),%rcx

40d4:       48 8d 54 24 10              lea    0x10(%rsp),%rdx

40d9:       4c 8d 44 24 50              lea    0x50(%rsp),%r8

40de:       48 8d 35 49 14 00 00        lea    0x1449(%rip),%rsi        # 552e
<array.3481+0x34e>
40e5:       48 8d 3d 14 53 00 00        lea    0x5314(%rip),%rdi        # 9400
<input_strings+0x140>
40ec:       b8 00 00 00 00              mov    $0x0,%eax

40f1:       e8 1a f2 ff ff              callq  3310 <__isoc99_sscanf@plt>

40f6:       83 f8 03                    cmp    $0x3,%eax

40f9:       0f 84 e0 00 00 00           je     41df <phase_defused+0x160>

40ff:       48 8d 3d 4a 12 00 00        lea    0x124a(%rip),%rdi        # 5350
<array.3481+0x170>
4106:       e8 45 f1 ff ff              callq  3250 <puts@plt>

410b:       48 8d 3d 6e 12 00 00        lea    0x126e(%rip),%rdi        # 5380
<array.3481+0x1a0>
4112:       e8 39 f1 ff ff              callq  3250 <puts@plt>

4117:       48 8d 4c 24 0c              lea    0xc(%rsp),%rcx
```

```
411c:    48 8d 54 24 08              lea    0x8(%rsp),%rdx

4121:    4c 8d 44 24 50              lea    0x50(%rsp),%r8

4126:    48 8d 35 20 14 00 00        lea    0x1420(%rip),%rsi      # 554d
<array.3481+0x36d>
412d:    48 8d 3d 7c 52 00 00        lea    0x527c(%rip),%rdi      # 93b0
<input_strings+0xf0>
4134:    b8 00 00 00 00              mov    $0x0,%eax

4139:    e8 d2 f1 ff ff              callq  3310 <__isoc99_sscanf@plt>

413e:    83 f8 03                    cmp    $0x3,%eax

4141:    0f 85 69 ff ff ff           jne    40b0 <phase_defused+0x31>

4147:    48 8d 7c 24 50              lea    0x50(%rsp),%rdi

414c:    48 8d 35 03 14 00 00        lea    0x1403(%rip),%rsi      # 5556
<array.3481+0x376>
4153:    e8 0e fa ff ff              callq  3b66 <strings_not_equal>

4158:    85 c0                       test   %eax,%eax

415a:    0f 85 50 ff ff ff           jne    40b0 <phase_defused+0x31>

4160:    48 8d 3d 1b 14 00 00        lea    0x141b(%rip),%rdi      # 5582
<array.3481+0x3a2>
4167:    e8 e4 f0 ff ff              callq  3250 <puts@plt>

416c:    bf 02 00 00 00              mov    $0x2,%edi

4171:    e8 0a f2 ff ff              callq  3380 <sleep@plt>

4176:    48 8d 3d e0 13 00 00        lea    0x13e0(%rip),%rdi      # 555d
<array.3481+0x37d>
417d:    e8 ce f0 ff ff              callq  3250 <puts@plt>

4182:    bf 03 00 00 00              mov    $0x3,%edi

4187:    e8 f4 f1 ff ff              callq  3380 <sleep@plt>

418c:    48 8d 3d dd 13 00 00        lea    0x13dd(%rip),%rdi      # 5570
<array.3481+0x390>
4193:    e8 b8 f0 ff ff              callq  3250 <puts@plt>

4198:    bf 04 00 00 00              mov    $0x4,%edi

419d:    e8 de f1 ff ff              callq  3380 <sleep@plt>

41a2:    48 8d 3d dd 13 00 00        lea    0x13dd(%rip),%rdi      # 5586
<array.3481+0x3a6>
41a9:    e8 a2 f0 ff ff              callq  3250 <puts@plt>

41ae:    bf 05 00 00 00              mov    $0x5,%edi

41b3:    e8 c8 f1 ff ff              callq  3380 <sleep@plt>
```

```
   41b8:    48 8d 3d 09 12 00 00      lea    0x1209(%rip),%rdi        # 53c8
<array.3481+0x1e8>
   41bf:    e8 8c f0 ff ff            callq  3250 <puts@plt>

   41c4:    bf 05 00 00 00            mov    $0x5,%edi

   41c9:    e8 b2 f1 ff ff            callq  3380 <sleep@plt>

   41ce:    48 8d 3d 2b 12 00 00      lea    0x122b(%rip),%rdi        # 5400
<array.3481+0x220>
   41d5:    e8 76 f0 ff ff            callq  3250 <puts@plt>

   41da:    e9 d1 fe ff ff            jmpq   40b0 <phase_defused+0x31>

   41df:    48 8d 7c 24 50            lea    0x50(%rsp),%rdi

   41e4:    48 8d 35 4c 13 00 00      lea    0x134c(%rip),%rsi        # 5537
<array.3481+0x357>
   41eb:    e8 76 f9 ff ff            callq  3b66 <strings_not_equal>

   41f0:    85 c0                     test   %eax,%eax

   41f2:    0f 85 07 ff ff ff         jne    40ff <phase_defused+0x80>

   41f8:    48 8d 3d e9 10 00 00      lea    0x10e9(%rip),%rdi        # 52e8
<array.3481+0x108>
   41ff:    e8 4c f0 ff ff            callq  3250 <puts@plt>

   4204:    48 8d 3d 0d 11 00 00      lea    0x110d(%rip),%rdi        # 5318
<array.3481+0x138>
   420b:    e8 40 f0 ff ff            callq  3250 <puts@plt>

   4210:    b8 00 00 00 00            mov    $0x0,%eax

   4215:    e8 3f f8 ff ff            callq  3a59 <secret_phase>

   421a:    e9 e0 fe ff ff            jmpq   40ff <phase_defused+0x80>

   421f:    e8 4c f0 ff ff            callq  3270 <__stack_chk_fail@plt>


0000000000004224 <sigalrm_handler>:

   4224:    f3 0f 1e fa               endbr64

   4228:    50                        push   %rax

   4229:    58                        pop    %rax

   422a:    48 83 ec 08               sub    $0x8,%rsp

   422e:    b9 00 00 00 00            mov    $0x0,%ecx

   4233:    48 8d 15 96 20 00 00      lea    0x2096(%rip),%rdx        # 62d0
<array.3481+0x10f0>
   423a:    be 01 00 00 00            mov    $0x1,%esi
```

```
  423f:    48 8b 3d 5a 50 00 00       mov     0x505a(%rip),%rdi       # 92a0
<stderr@@GLIBC_2.2.5>
  4246:    b8 00 00 00 00             mov     $0x0,%eax
  424b:    e8 20 f1 ff ff            callq   3370 <__fprintf_chk@plt>
  4250:    bf 01 00 00 00             mov     $0x1,%edi
  4255:    e8 f6 f0 ff ff            callq   3350 <exit@plt>


000000000000425a <rio_readlineb>:
  425a:    41 56                      push    %r14
  425c:    41 55                      push    %r13
  425e:    41 54                      push    %r12
  4260:    55                         push    %rbp
  4261:    53                         push    %rbx
  4262:    48 89 f5                   mov     %rsi,%rbp
  4265:    48 83 fa 01                cmp     $0x1,%rdx
  4269:    0f 86 90 00 00 00         jbe     42ff <rio_readlineb+0xa5>
  426f:    48 89 fb                   mov     %rdi,%rbx
  4272:    4c 8d 74 16 ff            lea     -0x1(%rsi,%rdx,1),%r14
  4277:    41 bd 01 00 00 00         mov     $0x1,%r13d
  427d:    4c 8d 67 10               lea     0x10(%rdi),%r12
  4281:    eb 54                      jmp     42d7 <rio_readlineb+0x7d>
  4283:    e8 a8 ef ff ff            callq   3230 <__errno_location@plt>
  4288:    83 38 04                   cmpl    $0x4,(%rax)
  428b:    75 53                      jne     42e0 <rio_readlineb+0x86>
  428d:    ba 00 20 00 00            mov     $0x2000,%edx
  4292:    4c 89 e6                   mov     %r12,%rsi
  4295:    8b 3b                      mov     (%rbx),%edi
  4297:    e8 04 f0 ff ff            callq   32a0 <read@plt>
  429c:    89 c2                      mov     %eax,%edx
  429e:    89 43 04                   mov     %eax,0x4(%rbx)
  42a1:    85 c0                      test    %eax,%eax
  42a3:    78 de                      js      4283 <rio_readlineb+0x29>
```

```
42a5:    85 c0                      test    %eax,%eax
42a7:    74 40                      je      42e9 <rio_readlineb+0x8f>
42a9:    4c 89 63 08                mov     %r12,0x8(%rbx)
42ad:    48 8b 43 08                mov     0x8(%rbx),%rax
42b1:    0f b6 08                   movzbl  (%rax),%ecx
42b4:    48 83 c0 01                add     $0x1,%rax
42b8:    48 89 43 08                mov     %rax,0x8(%rbx)
42bc:    83 ea 01                   sub     $0x1,%edx
42bf:    89 53 04                   mov     %edx,0x4(%rbx)
42c2:    48 83 c5 01                add     $0x1,%rbp
42c6:    88 4d ff                   mov     %cl,-0x1(%rbp)
42c9:    80 f9 0a                   cmp     $0xa,%cl
42cc:    74 3c                      je      430a <rio_readlineb+0xb0>
42ce:    41 83 c5 01                add     $0x1,%r13d
42d2:    4c 39 f5                   cmp     %r14,%rbp
42d5:    74 30                      je      4307 <rio_readlineb+0xad>
42d7:    8b 53 04                   mov     0x4(%rbx),%edx
42da:    85 d2                      test    %edx,%edx
42dc:    7e af                      jle     428d <rio_readlineb+0x33>
42de:    eb cd                      jmp     42ad <rio_readlineb+0x53>
42e0:    48 c7 c0 ff ff ff ff       mov     $0xffffffffffffffff,%rax
42e7:    eb 05                      jmp     42ee <rio_readlineb+0x94>
42e9:    b8 00 00 00 00             mov     $0x0,%eax
42ee:    85 c0                      test    %eax,%eax
42f0:    75 28                      jne     431a <rio_readlineb+0xc0>
42f2:    b8 00 00 00 00             mov     $0x0,%eax
42f7:    41 83 fd 01                cmp     $0x1,%r13d
42fb:    75 0d                      jne     430a <rio_readlineb+0xb0>
42fd:    eb 12                      jmp     4311 <rio_readlineb+0xb7>
42ff:    41 bd 01 00 00 00          mov     $0x1,%r13d
4305:    eb 03                      jmp     430a <rio_readlineb+0xb0>
4307:    4c 89 f5                   mov     %r14,%rbp
```

```
430a:    c6 45 00 00               movb   $0x0,0x0(%rbp)
430e:    49 63 c5                  movslq %r13d,%rax
4311:    5b                        pop    %rbx
4312:    5d                        pop    %rbp
4313:    41 5c                     pop    %r12
4315:    41 5d                     pop    %r13
4317:    41 5e                     pop    %r14
4319:    c3                        retq
431a:    48 c7 c0 ff ff ff ff      mov    $0xffffffffffffffff,%rax
4321:    eb ee                     jmp    4311 <rio_readlineb+0xb7>


0000000000004323 <submitr>:
4323:    f3 0f 1e fa               endbr64
4327:    41 57                     push   %r15
4329:    41 56                     push   %r14
432b:    41 55                     push   %r13
432d:    41 54                     push   %r12
432f:    55                        push   %rbp
4330:    53                        push   %rbx
4331:    4c 8d 9c 24 00 60 ff      lea    -0xa000(%rsp),%r11
4338:    ff
4339:    48 81 ec 00 10 00 00      sub    $0x1000,%rsp
4340:    48 83 0c 24 00            orq    $0x0,(%rsp)
4345:    4c 39 dc                  cmp    %r11,%rsp
4348:    75 ef                     jne    4339 <submitr+0x16>
434a:    48 83 ec 68               sub    $0x68,%rsp
434e:    49 89 fd                  mov    %rdi,%r13
4351:    89 f5                     mov    %esi,%ebp
4353:    48 89 14 24               mov    %rdx,(%rsp)
4357:    48 89 4c 24 08            mov    %rcx,0x8(%rsp)
435c:    4c 89 44 24 18            mov    %r8,0x18(%rsp)
```

```
4361:    4c 89 4c 24 10              mov     %r9,0x10(%rsp)
4366:    48 8b 9c 24 a0 a0 00        mov     0xa0a0(%rsp),%rbx
436d:    00
436e:    4c 8b bc 24 a8 a0 00        mov     0xa0a8(%rsp),%r15
4375:    00
4376:    64 48 8b 04 25 28 00        mov     %fs:0x28,%rax
437d:    00 00
437f:    48 89 84 24 58 a0 00        mov     %rax,0xa058(%rsp)
4386:    00
4387:    31 c0                       xor     %eax,%eax
4389:    c7 44 24 2c 00 00 00        movl    $0x0,0x2c(%rsp)
4390:    00
4391:    ba 00 00 00 00             mov     $0x0,%edx
4396:    be 01 00 00 00             mov     $0x1,%esi
439b:    bf 02 00 00 00             mov     $0x2,%edi
43a0:    e8 0b f0 ff ff             callq   33b0 <socket@plt>
43a5:    85 c0                      test    %eax,%eax
43a7:    0f 88 17 01 00 00          js      44c4 <submitr+0x1a1>
43ad:    41 89 c4                   mov     %eax,%r12d
43b0:    4c 89 ef                   mov     %r13,%rdi
43b3:    e8 18 ef ff ff             callq   32d0 <gethostbyname@plt>
43b8:    48 85 c0                   test    %rax,%rax
43bb:    0f 84 53 01 00 00          je      4514 <submitr+0x1f1>
43c1:    4c 8d 6c 24 30             lea     0x30(%rsp),%r13
43c6:    48 c7 44 24 30 00 00       movq    $0x0,0x30(%rsp)
43cd:    00 00
43cf:    48 c7 44 24 38 00 00       movq    $0x0,0x38(%rsp)
43d6:    00 00
43d8:    66 c7 44 24 30 02 00       movw    $0x2,0x30(%rsp)
43df:    48 63 50 14                movslq  0x14(%rax),%rdx
43e3:    48 8b 40 18                mov     0x18(%rax),%rax
43e7:    48 8d 7c 24 34             lea     0x34(%rsp),%rdi
```

```
43ec:    b9 0c 00 00 00           mov    $0xc,%ecx
43f1:    48 8b 30                 mov    (%rax),%rsi
43f4:    e8 e7 ee ff ff           callq  32e0 <__memmove_chk@plt>
43f9:    66 c1 c5 08              rol    $0x8,%bp
43fd:    66 89 6c 24 32           mov    %bp,0x32(%rsp)
4402:    ba 10 00 00 00           mov    $0x10,%edx
4407:    4c 89 ee                 mov    %r13,%rsi
440a:    44 89 e7                 mov    %r12d,%edi
440d:    e8 4e ef ff ff           callq  3360 <connect@plt>
4412:    85 c0                    test   %eax,%eax
4414:    0f 88 65 01 00 00        js     457f <submitr+0x25c>
441a:    49 c7 c1 ff ff ff ff     mov    $0xffffffffffffffff,%r9
4421:    b8 00 00 00 00           mov    $0x0,%eax
4426:    4c 89 c9                 mov    %r9,%rcx
4429:    48 89 df                 mov    %rbx,%rdi
442c:    f2 ae                    repnz scas %es:(%rdi),%al
442e:    48 f7 d1                 not    %rcx
4431:    48 89 ce                 mov    %rcx,%rsi
4434:    4c 89 c9                 mov    %r9,%rcx
4437:    48 8b 3c 24              mov    (%rsp),%rdi
443b:    f2 ae                    repnz scas %es:(%rdi),%al
443d:    49 89 c8                 mov    %rcx,%r8
4440:    4c 89 c9                 mov    %r9,%rcx
4443:    48 8b 7c 24 08           mov    0x8(%rsp),%rdi
4448:    f2 ae                    repnz scas %es:(%rdi),%al
444a:    48 89 ca                 mov    %rcx,%rdx
444d:    48 f7 d2                 not    %rdx
4450:    4c 89 c9                 mov    %r9,%rcx
4453:    48 8b 7c 24 10           mov    0x10(%rsp),%rdi
4458:    f2 ae                    repnz scas %es:(%rdi),%al
445a:    4c 29 c2                 sub    %r8,%rdx
445d:    48 29 ca                 sub    %rcx,%rdx
```

```
4460:    48 8d 44 76 fd           lea    -0x3(%rsi,%rsi,2),%rax
4465:    48 8d 44 02 7b           lea    0x7b(%rdx,%rax,1),%rax
446a:    48 3d 00 20 00 00        cmp    $0x2000,%rax
4470:    0f 87 66 01 00 00        ja     45dc <submitr+0x2b9>
4476:    48 8d 94 24 50 40 00     lea    0x4050(%rsp),%rdx
447d:    00
447e:    b9 00 04 00 00           mov    $0x400,%ecx
4483:    b8 00 00 00 00           mov    $0x0,%eax
4488:    48 89 d7                 mov    %rdx,%rdi
448b:    f3 48 ab                 rep stos %rax,%es:(%rdi)
448e:    48 c7 c1 ff ff ff ff     mov    $0xffffffffffffffff,%rcx
4495:    48 89 df                 mov    %rbx,%rdi
4498:    f2 ae                    repnz scas %es:(%rdi),%al
449a:    48 f7 d1                 not    %rcx
449d:    48 8d 41 ff              lea    -0x1(%rcx),%rax
44a1:    83 f9 01                 cmp    $0x1,%ecx
44a4:    0f 84 84 06 00 00        je     4b2e <submitr+0x80b>
44aa:    8d 40 ff                 lea    -0x1(%rax),%eax
44ad:    4c 8d 74 03 01           lea    0x1(%rbx,%rax,1),%r14
44b2:    48 89 d5                 mov    %rdx,%rbp
44b5:    49 bd d9 ff 00 00 00     movabs $0x2000000000ffd9,%r13
44bc:    00 20 00
44bf:    e9 a6 01 00 00           jmpq   466a <submitr+0x347>
44c4:    48 b8 45 72 72 6f 72     movabs $0x43203a726f727245,%rax
44cb:    3a 20 43
44ce:    48 ba 6c 69 65 6e 74     movabs $0x6e7520746e65696c,%rdx
44d5:    20 75 6e
44d8:    49 89 07                 mov    %rax,(%r15)
44db:    49 89 57 08              mov    %rdx,0x8(%r15)
44df:    48 b8 61 62 6c 65 20     movabs $0x206f7420656c6261,%rax
44e6:    74 6f 20
44e9:    48 ba 63 72 65 61 74     movabs $0x7320657461657263,%rdx
```

```
44f0:      65 20 73
44f3:      49 89 47 10                  mov    %rax,0x10(%r15)
44f7:      49 89 57 18                  mov    %rdx,0x18(%r15)
44fb:      41 c7 47 20 6f 63 6b         movl   $0x656b636f,0x20(%r15)
4502:      65
4503:      66 41 c7 47 24 74 00         movw   $0x74,0x24(%r15)
450a:      b8 ff ff ff ff               mov    $0xffffffff,%eax
450f:      e9 92 04 00 00               jmpq   49a6 <submitr+0x683>
4514:      48 b8 45 72 72 6f 72         movabs $0x44203a726f727245,%rax
451b:      3a 20 44
451e:      48 ba 4e 53 20 69 73         movabs $0x6e7520736920534e,%rdx
4525:      20 75 6e
4528:      49 89 07                     mov    %rax,(%r15)
452b:      49 89 57 08                  mov    %rdx,0x8(%r15)
452f:      48 b8 61 62 6c 65 20         movabs $0x206f7420656c6261,%rax
4536:      74 6f 20
4539:      48 ba 72 65 73 6f 6c         movabs $0x2065766c6f736572,%rdx
4540:      76 65 20
4543:      49 89 47 10                  mov    %rax,0x10(%r15)
4547:      49 89 57 18                  mov    %rdx,0x18(%r15)
454b:      48 b8 73 65 72 76 65         movabs $0x6120726576726573,%rax
4552:      72 20 61
4555:      49 89 47 20                  mov    %rax,0x20(%r15)
4559:      41 c7 47 28 64 64 72         movl   $0x65726464,0x28(%r15)
4560:      65
4561:      66 41 c7 47 2c 73 73         movw   $0x7373,0x2c(%r15)
4568:      41 c6 47 2e 00               movb   $0x0,0x2e(%r15)
456d:      44 89 e7                     mov    %r12d,%edi
4570:      e8 1b ed ff ff               callq  3290 <close@plt>
4575:      b8 ff ff ff ff               mov    $0xffffffff,%eax
457a:      e9 27 04 00 00               jmpq   49a6 <submitr+0x683>
457f:      48 b8 45 72 72 6f 72         movabs $0x55203a726f727245,%rax
```

```
4586:    3a 20 55
4589:    48 ba 6e 61 62 6c 65          movabs $0x6f7420656c62616e,%rdx
4590:    20 74 6f
4593:    49 89 07                      mov    %rax,(%r15)
4596:    49 89 57 08                   mov    %rdx,0x8(%r15)
459a:    48 b8 20 63 6f 6e 6e          movabs $0x7463656e6e6f6320,%rax
45a1:    65 63 74
45a4:    48 ba 20 74 6f 20 74          movabs $0x20656874206f7420,%rdx
45ab:    68 65 20
45ae:    49 89 47 10                   mov    %rax,0x10(%r15)
45b2:    49 89 57 18                   mov    %rdx,0x18(%r15)
45b6:    41 c7 47 20 73 65 72          movl   $0x76726573,0x20(%r15)
45bd:    76
45be:    66 41 c7 47 24 65 72          movw   $0x7265,0x24(%r15)
45c5:    41 c6 47 26 00                movb   $0x0,0x26(%r15)
45ca:    44 89 e7                      mov    %r12d,%edi
45cd:    e8 be ec ff ff                callq  3290 <close@plt>
45d2:    b8 ff ff ff ff                mov    $0xffffffff,%eax
45d7:    e9 ca 03 00 00                jmpq   49a6 <submitr+0x683>
45dc:    48 b8 45 72 72 6f 72          movabs $0x52203a726f727245,%rax
45e3:    3a 20 52
45e6:    48 ba 65 73 75 6c 74          movabs $0x747320746c757365,%rdx
45ed:    20 73 74
45f0:    49 89 07                      mov    %rax,(%r15)
45f3:    49 89 57 08                   mov    %rdx,0x8(%r15)
45f7:    48 b8 72 69 6e 67 20          movabs $0x6f6f7420676e6972,%rax
45fe:    74 6f 6f
4601:    48 ba 20 6c 61 72 67          movabs $0x202e656772616c20,%rdx
4608:    65 2e 20
460b:    49 89 47 10                   mov    %rax,0x10(%r15)
460f:    49 89 57 18                   mov    %rdx,0x18(%r15)
4613:    48 b8 49 6e 63 72 65          movabs $0x6573616572636e49,%rax
```

```
461a:       61 73 65
461d:       48 ba 20 53 55 42 4d        movabs $0x5254494d42555320,%rdx
4624:       49 54 52
4627:       49 89 47 20                 mov    %rax,0x20(%r15)
462b:       49 89 57 28                 mov    %rdx,0x28(%r15)
462f:       48 b8 5f 4d 41 58 42        movabs $0x46554258414d5f,%rax
4636:       55 46 00
4639:       49 89 47 30                 mov    %rax,0x30(%r15)
463d:       44 89 e7                    mov    %r12d,%edi
4640:       e8 4b ec ff ff              callq  3290 <close@plt>
4645:       b8 ff ff ff ff              mov    $0xffffffff,%eax
464a:       e9 57 03 00 00              jmpq   49a6 <submitr+0x683>
464f:       49 0f a3 c5                 bt     %rax,%r13
4653:       73 21                       jae    4676 <submitr+0x353>
4655:       44 88 45 00                 mov    %r8b,0x0(%rbp)
4659:       48 8d 6d 01                 lea    0x1(%rbp),%rbp
465d:       48 83 c3 01                 add    $0x1,%rbx
4661:       4c 39 f3                    cmp    %r14,%rbx
4664:       0f 84 c4 04 00 00           je     4b2e <submitr+0x80b>
466a:       44 0f b6 03                 movzbl (%rbx),%r8d
466e:       41 8d 40 d6                 lea    -0x2a(%r8),%eax
4672:       3c 35                       cmp    $0x35,%al
4674:       76 d9                       jbe    464f <submitr+0x32c>
4676:       44 89 c0                    mov    %r8d,%eax
4679:       83 e0 df                    and    $0xffffffdf,%eax
467c:       83 e8 41                    sub    $0x41,%eax
467f:       3c 19                       cmp    $0x19,%al
4681:       76 d2                       jbe    4655 <submitr+0x332>
4683:       41 80 f8 20                 cmp    $0x20,%r8b
4687:       74 63                       je     46ec <submitr+0x3c9>
4689:       41 8d 40 e0                 lea    -0x20(%r8),%eax
468d:       3c 5f                       cmp    $0x5f,%al
```

```
468f:      76 0a                      jbe    469b <submitr+0x378>
4691:      41 80 f8 09                cmp    $0x9,%r8b
4695:      0f 85 06 04 00 00          jne    4aa1 <submitr+0x77e>
469b:      48 8d bc 24 50 80 00       lea    0x8050(%rsp),%rdi
46a2:      00
46a3:      45 0f b6 c0                movzbl %r8b,%r8d
46a7:      48 8d 0d f8 1c 00 00       lea    0x1cf8(%rip),%rcx        # 63a6
<array.3481+0x11c6>
46ae:      ba 08 00 00 00             mov    $0x8,%edx
46b3:      be 01 00 00 00             mov    $0x1,%esi
46b8:      b8 00 00 00 00             mov    $0x0,%eax
46bd:      e8 de ec ff ff             callq  33a0 <__sprintf_chk@plt>
46c2:      0f b6 84 24 50 80 00       movzbl 0x8050(%rsp),%eax
46c9:      00
46ca:      88 45 00                   mov    %al,0x0(%rbp)
46cd:      0f b6 84 24 51 80 00       movzbl 0x8051(%rsp),%eax
46d4:      00
46d5:      88 45 01                   mov    %al,0x1(%rbp)
46d8:      0f b6 84 24 52 80 00       movzbl 0x8052(%rsp),%eax
46df:      00
46e0:      88 45 02                   mov    %al,0x2(%rbp)
46e3:      48 8d 6d 03                lea    0x3(%rbp),%rbp
46e7:      e9 71 ff ff ff             jmpq   465d <submitr+0x33a>
46ec:      c6 45 00 2b                movb   $0x2b,0x0(%rbp)
46f0:      48 8d 6d 01                lea    0x1(%rbp),%rbp
46f4:      e9 64 ff ff ff             jmpq   465d <submitr+0x33a>
46f9:      48 b8 45 72 72 6f 72       movabs $0x47203a726f727245,%rax
4700:      3a 20 47
4703:      48 ba 45 54 20 72 65       movabs $0x6575716572205445,%rdx
470a:      71 75 65
470d:      49 89 07                   mov    %rax,(%r15)
4710:      49 89 57 08                mov    %rdx,0x8(%r15)
```

```
4714:    48 b8 73 74 20 65 78        movabs  $0x6565637865207473,%rax
471b:    63 65 65
471e:    48 ba 64 73 20 62 75        movabs  $0x6566667562207364,%rdx
4725:    66 66 65
4728:    49 89 47 10                 mov     %rax,0x10(%r15)
472c:    49 89 57 18                 mov     %rdx,0x18(%r15)
4730:    41 c7 47 20 72 20 73        movl    $0x69732072,0x20(%r15)
4737:    69
4738:    66 41 c7 47 24 7a 65        movw    $0x657a,0x24(%r15)
473f:    41 c6 47 26 00              movb    $0x0,0x26(%r15)
4744:    44 89 e7                    mov     %r12d,%edi
4747:    e8 44 eb ff ff              callq   3290 <close@plt>
474c:    b8 ff ff ff ff              mov     $0xffffffff,%eax
4751:    e9 50 02 00 00              jmpq    49a6 <submitr+0x683>
4756:    48 01 c5                    add     %rax,%rbp
4759:    48 29 c3                    sub     %rax,%rbx
475c:    74 26                       je      4784 <submitr+0x461>
475e:    48 89 da                    mov     %rbx,%rdx
4761:    48 89 ee                    mov     %rbp,%rsi
4764:    44 89 e7                    mov     %r12d,%edi
4767:    e8 f4 ea ff ff              callq   3260 <write@plt>
476c:    48 85 c0                    test    %rax,%rax
476f:    7f e5                       jg      4756 <submitr+0x433>
4771:    e8 ba ea ff ff              callq   3230 <__errno_location@plt>
4776:    83 38 04                    cmpl    $0x4,(%rax)
4779:    0f 85 c3 02 00 00           jne     4a42 <submitr+0x71f>
477f:    4c 89 e8                    mov     %r13,%rax
4782:    eb d2                       jmp     4756 <submitr+0x433>
4784:    44 89 64 24 40              mov     %r12d,0x40(%rsp)
4789:    c7 44 24 44 00 00 00        movl    $0x0,0x44(%rsp)
4790:    00
4791:    48 8d 7c 24 40              lea     0x40(%rsp),%rdi
```

```
4796:    48 8d 44 24 50         lea    0x50(%rsp),%rax

479b:    48 89 44 24 48         mov    %rax,0x48(%rsp)

47a0:    48 8d b4 24 50 20 00   lea    0x2050(%rsp),%rsi

47a7:    00

47a8:    ba 00 20 00 00         mov    $0x2000,%edx

47ad:    e8 a8 fa ff ff         callq  425a <rio_readlineb>

47b2:    48 85 c0               test   %rax,%rax

47b5:    0f 8e ec 00 00 00      jle    48a7 <submitr+0x584>

47bb:    48 8d 4c 24 2c         lea    0x2c(%rsp),%rcx

47c0:    48 8d 94 24 50 60 00   lea    0x6050(%rsp),%rdx

47c7:    00

47c8:    48 8d bc 24 50 20 00   lea    0x2050(%rsp),%rdi

47cf:    00

47d0:    4c 8d 84 24 50 80 00   lea    0x8050(%rsp),%r8

47d7:    00

47d8:    48 8d 35 ce 1b 00 00   lea    0x1bce(%rip),%rsi        # 63ad
<array.3481+0x11cd>
47df:    b8 00 00 00 00         mov    $0x0,%eax

47e4:    e8 27 eb ff ff         callq  3310 <__isoc99_sscanf@plt>

47e9:    44 8b 44 24 2c         mov    0x2c(%rsp),%r8d

47ee:    41 81 f8 c8 00 00 00   cmp    $0xc8,%r8d

47f5:    0f 85 20 01 00 00      jne    491b <submitr+0x5f8>

47fb:    48 8d 1d bc 1b 00 00   lea    0x1bbc(%rip),%rbx        # 63be
<array.3481+0x11de>
4802:    48 8d b4 24 50 20 00   lea    0x2050(%rsp),%rsi

4809:    00

480a:    b9 03 00 00 00         mov    $0x3,%ecx

480f:    48 89 df               mov    %rbx,%rdi

4812:    f3 a6                  repz cmpsb %es:(%rdi),%ds:(%rsi)

4814:    0f 97 c0               seta   %al

4817:    1c 00                  sbb    $0x0,%al

4819:    84 c0                  test   %al,%al

481b:    0f 84 31 01 00 00      je     4952 <submitr+0x62f>
```

```
4821:    48 8d b4 24 50 20 00    lea    0x2050(%rsp),%rsi
4828:    00
4829:    48 8d 7c 24 40          lea    0x40(%rsp),%rdi
482e:    ba 00 20 00 00          mov    $0x2000,%edx
4833:    e8 22 fa ff ff          callq  425a <rio_readlineb>
4838:    48 85 c0                test   %rax,%rax
483b:    7f c5                   jg     4802 <submitr+0x4df>
483d:    48 b8 45 72 72 6f 72    movabs $0x43203a726f727245,%rax
4844:    3a 20 43
4847:    48 ba 6c 69 65 6e 74    movabs $0x6e7520746e65696c,%rdx
484e:    20 75 6e
4851:    49 89 07                mov    %rax,(%r15)
4854:    49 89 57 08             mov    %rdx,0x8(%r15)
4858:    48 b8 61 62 6c 65 20    movabs $0x206f7420656c6261,%rax
485f:    74 6f 20
4862:    48 ba 72 65 61 64 20    movabs $0x6165682064616572,%rdx
4869:    68 65 61
486c:    49 89 47 10             mov    %rax,0x10(%r15)
4870:    49 89 57 18             mov    %rdx,0x18(%r15)
4874:    48 b8 64 65 72 73 20    movabs $0x6f72662073726564,%rax
487b:    66 72 6f
487e:    48 ba 6d 20 73 65 72    movabs $0x726576726573206d,%rdx
4885:    76 65 72
4888:    49 89 47 20             mov    %rax,0x20(%r15)
488c:    49 89 57 28             mov    %rdx,0x28(%r15)
4890:    41 c6 47 30 00          movb   $0x0,0x30(%r15)
4895:    44 89 e7                mov    %r12d,%edi
4898:    e8 f3 e9 ff ff          callq  3290 <close@plt>
489d:    b8 ff ff ff ff          mov    $0xffffffff,%eax
48a2:    e9 ff 00 00 00          jmpq   49a6 <submitr+0x683>
48a7:    48 b8 45 72 72 6f 72    movabs $0x43203a726f727245,%rax
48ae:    3a 20 43
```

```
48b1:	48 ba 6c 69 65 6e 74	movabs $0x6e7520746e65696c,%rdx
48b8:	20 75 6e
48bb:	49 89 07	mov    %rax,(%r15)
48be:	49 89 57 08	mov    %rdx,0x8(%r15)
48c2:	48 b8 61 62 6c 65 20	movabs $0x206f7420656c6261,%rax
48c9:	74 6f 20
48cc:	48 ba 72 65 61 64 20	movabs $0x7269662064616572,%rdx
48d3:	66 69 72
48d6:	49 89 47 10	mov    %rax,0x10(%r15)
48da:	49 89 57 18	mov    %rdx,0x18(%r15)
48de:	48 b8 73 74 20 68 65	movabs $0x6564616568207473,%rax
48e5:	61 64 65
48e8:	48 ba 72 20 66 72 6f	movabs $0x73206d6f72662072,%rdx
48ef:	6d 20 73
48f2:	49 89 47 20	mov    %rax,0x20(%r15)
48f6:	49 89 57 28	mov    %rdx,0x28(%r15)
48fa:	41 c7 47 30 65 72 76	movl   $0x65767265,0x30(%r15)
4901:	65
4902:	66 41 c7 47 34 72 00	movw   $0x72,0x34(%r15)
4909:	44 89 e7	mov    %r12d,%edi
490c:	e8 7f e9 ff ff	callq  3290 <close@plt>
4911:	b8 ff ff ff ff	mov    $0xffffffff,%eax
4916:	e9 8b 00 00 00	jmpq   49a6 <submitr+0x683>
491b:	4c 8d 8c 24 50 80 00	lea    0x8050(%rsp),%r9
4922:	00
4923:	48 8d 0d ce 19 00 00	lea    0x19ce(%rip),%rcx        # 62f8
<array.3481+0x1118>
492a:	48 c7 c2 ff ff ff ff	mov    $0xffffffffffffffff,%rdx
4931:	be 01 00 00 00	mov    $0x1,%esi
4936:	4c 89 ff	mov    %r15,%rdi
4939:	b8 00 00 00 00	mov    $0x0,%eax
493e:	e8 5d ea ff ff	callq  33a0 <__sprintf_chk@plt>
```

```
4943:       44 89 e7                    mov     %r12d,%edi
4946:       e8 45 e9 ff ff              callq   3290 <close@plt>
494b:       b8 ff ff ff ff              mov     $0xffffffff,%eax
4950:       eb 54                       jmp     49a6 <submitr+0x683>
4952:       48 8d b4 24 50 20 00        lea     0x2050(%rsp),%rsi
4959:       00
495a:       48 8d 7c 24 40              lea     0x40(%rsp),%rdi
495f:       ba 00 20 00 00              mov     $0x2000,%edx
4964:       e8 f1 f8 ff ff              callq   425a <rio_readlineb>
4969:       48 85 c0                    test    %rax,%rax
496c:       7e 61                       jle     49cf <submitr+0x6ac>
496e:       48 8d b4 24 50 20 00        lea     0x2050(%rsp),%rsi
4975:       00
4976:       4c 89 ff                    mov     %r15,%rdi
4979:       e8 c2 e8 ff ff              callq   3240 <strcpy@plt>
497e:       44 89 e7                    mov     %r12d,%edi
4981:       e8 0a e9 ff ff              callq   3290 <close@plt>
4986:       b9 03 00 00 00              mov     $0x3,%ecx
498b:       48 8d 3d 2f 1a 00 00        lea     0x1a2f(%rip),%rdi        # 63c1
<array.3481+0x11e1>
4992:       4c 89 fe                    mov     %r15,%rsi
4995:       f3 a6                       repz cmpsb %es:(%rdi),%ds:(%rsi)
4997:       0f 97 c0                    seta    %al
499a:       1c 00                       sbb     $0x0,%al
499c:       84 c0                       test    %al,%al
499e:       0f 95 c0                    setne   %al
49a1:       0f b6 c0                    movzbl  %al,%eax
49a4:       f7 d8                       neg     %eax
49a6:       48 8b 94 24 58 a0 00        mov     0xa058(%rsp),%rdx
49ad:       00
49ae:       64 48 33 14 25 28 00        xor     %fs:0x28,%rdx
49b5:       00 00
```

```
49b7:     0f 85 fb 01 00 00        jne    4bb8 <submitr+0x895>

49bd:     48 81 c4 68 a0 00 00     add    $0xa068,%rsp

49c4:     5b                       pop    %rbx

49c5:     5d                       pop    %rbp

49c6:     41 5c                    pop    %r12

49c8:     41 5d                    pop    %r13

49ca:     41 5e                    pop    %r14

49cc:     41 5f                    pop    %r15

49ce:     c3                       retq

49cf:     48 b8 45 72 72 6f 72     movabs $0x43203a726f727245,%rax

49d6:     3a 20 43

49d9:     48 ba 6c 69 65 6e 74     movabs $0x6e7520746e65696c,%rdx

49e0:     20 75 6e

49e3:     49 89 07                 mov    %rax,(%r15)

49e6:     49 89 57 08              mov    %rdx,0x8(%r15)

49ea:     48 b8 61 62 6c 65 20     movabs $0x206f7420656c6261,%rax

49f1:     74 6f 20

49f4:     48 ba 72 65 61 64 20     movabs $0x6174732064616572,%rdx

49fb:     73 74 61

49fe:     49 89 47 10              mov    %rax,0x10(%r15)

4a02:     49 89 57 18              mov    %rdx,0x18(%r15)

4a06:     48 b8 74 75 73 20 6d     movabs $0x7373656d20737574,%rax

4a0d:     65 73 73

4a10:     48 ba 61 67 65 20 66     movabs $0x6d6f726620656761,%rdx

4a17:     72 6f 6d

4a1a:     49 89 47 20              mov    %rax,0x20(%r15)

4a1e:     49 89 57 28              mov    %rdx,0x28(%r15)

4a22:     48 b8 20 73 65 72 76     movabs $0x72657672657320,%rax

4a29:     65 72 00

4a2c:     49 89 47 30              mov    %rax,0x30(%r15)

4a30:     44 89 e7                 mov    %r12d,%edi

4a33:     e8 58 e8 ff ff           callq  3290 <close@plt>
```

```
4a38:     b8 ff ff ff ff              mov     $0xffffffff,%eax
4a3d:     e9 64 ff ff ff              jmpq    49a6 <submitr+0x683>
4a42:     48 b8 45 72 72 6f 72        movabs  $0x43203a726f727245,%rax
4a49:     3a 20 43
4a4c:     48 ba 6c 69 65 6e 74        movabs  $0x6e7520746e65696c,%rdx
4a53:     20 75 6e
4a56:     49 89 07                    mov     %rax,(%r15)
4a59:     49 89 57 08                 mov     %rdx,0x8(%r15)
4a5d:     48 b8 61 62 6c 65 20        movabs  $0x206f7420656c6261,%rax
4a64:     74 6f 20
4a67:     48 ba 77 72 69 74 65        movabs  $0x6f74206574697277,%rdx
4a6e:     20 74 6f
4a71:     49 89 47 10                 mov     %rax,0x10(%r15)
4a75:     49 89 57 18                 mov     %rdx,0x18(%r15)
4a79:     48 b8 20 74 68 65 20        movabs  $0x7265732065687420,%rax
4a80:     73 65 72
4a83:     49 89 47 20                 mov     %rax,0x20(%r15)
4a87:     41 c7 47 28 76 65 72        movl    $0x726576,0x28(%r15)
4a8e:     00
4a8f:     44 89 e7                    mov     %r12d,%edi
4a92:     e8 f9 e7 ff ff              callq   3290 <close@plt>
4a97:     b8 ff ff ff ff              mov     $0xffffffff,%eax
4a9c:     e9 05 ff ff ff              jmpq    49a6 <submitr+0x683>
4aa1:     48 b8 45 72 72 6f 72        movabs  $0x52203a726f727245,%rax
4aa8:     3a 20 52
4aab:     48 ba 65 73 75 6c 74        movabs  $0x747320746c757365,%rdx
4ab2:     20 73 74
4ab5:     49 89 07                    mov     %rax,(%r15)
4ab8:     49 89 57 08                 mov     %rdx,0x8(%r15)
4abc:     48 b8 72 69 6e 67 20        movabs  $0x6e6f320676e6972,%rax
4ac3:     63 6f 6e
4ac6:     48 ba 74 61 69 6e 73        movabs  $0x6e6120736e696174,%rdx
```

```
4acd:      20 61 6e

4ad0:      49 89 47 10                  mov    %rax,0x10(%r15)

4ad4:      49 89 57 18                  mov    %rdx,0x18(%r15)

4ad8:      48 b8 20 69 6c 6c 65         movabs $0x6c6167656c6c6920,%rax

4adf:      67 61 6c

4ae2:      48 ba 20 6f 72 20 75         movabs $0x72706e7520726f20,%rdx

4ae9:      6e 70 72

4aec:      49 89 47 20                  mov    %rax,0x20(%r15)

4af0:      49 89 57 28                  mov    %rdx,0x28(%r15)

4af4:      48 b8 69 6e 74 61 62         movabs $0x20656c6261746e69,%rax

4afb:      6c 65 20

4afe:      48 ba 63 68 61 72 61         movabs $0x6574636172616863,%rdx

4b05:      63 74 65

4b08:      49 89 47 30                  mov    %rax,0x30(%r15)

4b0c:      49 89 57 38                  mov    %rdx,0x38(%r15)

4b10:      66 41 c7 47 40 72 2e         movw   $0x2e72,0x40(%r15)

4b17:      41 c6 47 42 00               movb   $0x0,0x42(%r15)

4b1c:      44 89 e7                     mov    %r12d,%edi

4b1f:      e8 6c e7 ff ff               callq  3290 <close@plt>

4b24:      b8 ff ff ff ff               mov    $0xffffffff,%eax

4b29:      e9 78 fe ff ff               jmpq   49a6 <submitr+0x683>

4b2e:      48 8d bc 24 50 20 00         lea    0x2050(%rsp),%rdi

4b35:      00

4b36:      48 8d 84 24 50 40 00         lea    0x4050(%rsp),%rax

4b3d:      00

4b3e:      50                           push   %rax

4b3f:      ff 74 24 18                  pushq  0x18(%rsp)

4b43:      ff 74 24 28                  pushq  0x28(%rsp)

4b47:      ff 74 24 20                  pushq  0x20(%rsp)

4b4b:      4c 8b 4c 24 20               mov    0x20(%rsp),%r9

4b50:      4c 8d 05 d1 17 00 00         lea    0x17d1(%rip),%r8        # 6328
<array.3481+0x1148>
```

```
    4b57:    b9 00 20 00 00              mov    $0x2000,%ecx

    4b5c:    ba 01 00 00 00              mov    $0x1,%edx

    4b61:    be 00 20 00 00              mov    $0x2000,%esi

    4b66:    b8 00 00 00 00              mov    $0x0,%eax

    4b6b:    e8 a0 e6 ff ff              callq  3210 <__snprintf_chk@plt>

    4b70:    48 83 c4 20                 add    $0x20,%rsp

    4b74:    3d ff 1f 00 00              cmp    $0x1fff,%eax

    4b79:    0f 8f 7a fb ff ff           jg     46f9 <submitr+0x3d6>

    4b7f:    48 8d bc 24 50 20 00        lea    0x2050(%rsp),%rdi

    4b86:    00

    4b87:    48 c7 c1 ff ff ff ff        mov    $0xffffffffffffffff,%rcx

    4b8e:    b8 00 00 00 00              mov    $0x0,%eax

    4b93:    f2 ae                       repnz scas %es:(%rdi),%al

    4b95:    48 f7 d1                    not    %rcx

    4b98:    48 89 cb                    mov    %rcx,%rbx

    4b9b:    48 83 eb 01                 sub    $0x1,%rbx

    4b9f:    0f 84 df fb ff ff           je     4784 <submitr+0x461>

    4ba5:    48 8d ac 24 50 20 00        lea    0x2050(%rsp),%rbp

    4bac:    00

    4bad:    41 bd 00 00 00 00           mov    $0x0,%r13d

    4bb3:    e9 a6 fb ff ff              jmpq   475e <submitr+0x43b>

    4bb8:    e8 b3 e6 ff ff              callq  3270 <__stack_chk_fail@plt>


0000000000004bbd <init_timeout>:

    4bbd:    f3 0f 1e fa                 endbr64

    4bc1:    85 ff                       test   %edi,%edi

    4bc3:    75 01                       jne    4bc6 <init_timeout+0x9>

    4bc5:    c3                          retq

    4bc6:    53                          push   %rbx

    4bc7:    89 fb                       mov    %edi,%ebx

    4bc9:    48 8d 35 54 f6 ff ff        lea    -0x9ac(%rip),%rsi       # 4224
<sigalrm_handler>
```

```
    4bd0:    bf 0e 00 00 00              mov     $0xe,%edi
    4bd5:    e8 e6 e6 ff ff             callq   32c0 <signal@plt>
    4bda:    85 db                      test    %ebx,%ebx
    4bdc:    bf 00 00 00 00             mov     $0x0,%edi
    4be1:    0f 49 fb                   cmovns  %ebx,%edi
    4be4:    e8 97 e6 ff ff             callq   3280 <alarm@plt>
    4be9:    5b                         pop     %rbx
    4bea:    c3                         retq


0000000000004beb <init_driver>:
    4beb:    f3 0f 1e fa                endbr64
    4bef:    41 54                      push    %r12
    4bf1:    55                         push    %rbp
    4bf2:    53                         push    %rbx
    4bf3:    48 83 ec 20                sub     $0x20,%rsp
    4bf7:    48 89 fd                   mov     %rdi,%rbp
    4bfa:    64 48 8b 04 25 28 00       mov     %fs:0x28,%rax
    4c01:    00 00
    4c03:    48 89 44 24 18             mov     %rax,0x18(%rsp)
    4c08:    31 c0                      xor     %eax,%eax
    4c0a:    be 01 00 00 00             mov     $0x1,%esi
    4c0f:    bf 0d 00 00 00             mov     $0xd,%edi
    4c14:    e8 a7 e6 ff ff             callq   32c0 <signal@plt>
    4c19:    be 01 00 00 00             mov     $0x1,%esi
    4c1e:    bf 1d 00 00 00             mov     $0x1d,%edi
    4c23:    e8 98 e6 ff ff             callq   32c0 <signal@plt>
    4c28:    be 01 00 00 00             mov     $0x1,%esi
    4c2d:    bf 1d 00 00 00             mov     $0x1d,%edi
    4c32:    e8 89 e6 ff ff             callq   32c0 <signal@plt>
    4c37:    ba 00 00 00 00             mov     $0x0,%edx
    4c3c:    be 01 00 00 00             mov     $0x1,%esi
```

```
4c41:      bf 02 00 00 00           mov    $0x2,%edi

4c46:      e8 65 e7 ff ff           callq  33b0 <socket@plt>

4c4b:      85 c0                    test   %eax,%eax

4c4d:      0f 88 9c 00 00 00        js     4cef <init_driver+0x104>

4c53:      89 c3                    mov    %eax,%ebx

4c55:      48 8d 3d 68 17 00 00     lea    0x1768(%rip),%rdi        # 63c4
<array.3481+0x11e4>
4c5c:      e8 6f e6 ff ff           callq  32d0 <gethostbyname@plt>

4c61:      48 85 c0                 test   %rax,%rax

4c64:      0f 84 d1 00 00 00        je     4d3b <init_driver+0x150>

4c6a:      49 89 e4                 mov    %rsp,%r12

4c6d:      48 c7 04 24 00 00 00     movq   $0x0,(%rsp)

4c74:      00

4c75:      48 c7 44 24 08 00 00     movq   $0x0,0x8(%rsp)

4c7c:      00 00

4c7e:      66 c7 04 24 02 00        movw   $0x2,(%rsp)

4c84:      48 63 50 14              movslq 0x14(%rax),%rdx

4c88:      48 8b 40 18              mov    0x18(%rax),%rax

4c8c:      48 8d 7c 24 04           lea    0x4(%rsp),%rdi

4c91:      b9 0c 00 00 00           mov    $0xc,%ecx

4c96:      48 8b 30                 mov    (%rax),%rsi

4c99:      e8 42 e6 ff ff           callq  32e0 <__memmove_chk@plt>

4c9e:      66 c7 44 24 02 3b 6e     movw   $0x6e3b,0x2(%rsp)

4ca5:      ba 10 00 00 00           mov    $0x10,%edx

4caa:      4c 89 e6                 mov    %r12,%rsi

4cad:      89 df                    mov    %ebx,%edi

4caf:      e8 ac e6 ff ff           callq  3360 <connect@plt>

4cb4:      85 c0                    test   %eax,%eax

4cb6:      0f 88 e7 00 00 00        js     4da3 <init_driver+0x1b8>

4cbc:      89 df                    mov    %ebx,%edi

4cbe:      e8 cd e5 ff ff           callq  3290 <close@plt>

4cc3:      66 c7 45 00 4f 4b        movw   $0x4b4f,0x0(%rbp)
```

```
4cc9:    c6 45 02 00            movb   $0x0,0x2(%rbp)

4ccd:    b8 00 00 00 00         mov    $0x0,%eax

4cd2:    48 8b 4c 24 18         mov    0x18(%rsp),%rcx

4cd7:    64 48 33 0c 25 28 00   xor    %fs:0x28,%rcx

4cde:    00 00

4ce0:    0f 85 f5 00 00 00      jne    4ddb <init_driver+0x1f0>

4ce6:    48 83 c4 20            add    $0x20,%rsp

4cea:    5b                     pop    %rbx

4ceb:    5d                     pop    %rbp

4cec:    41 5c                  pop    %r12

4cee:    c3                     retq

4cef:    48 b8 45 72 72 6f 72   movabs $0x43203a726f727245,%rax

4cf6:    3a 20 43

4cf9:    48 ba 6c 69 65 6e 74   movabs $0x6e7520746e65696c,%rdx

4d00:    20 75 6e

4d03:    48 89 45 00            mov    %rax,0x0(%rbp)

4d07:    48 89 55 08            mov    %rdx,0x8(%rbp)

4d0b:    48 b8 61 62 6c 65 20   movabs $0x206f7420656c6261,%rax

4d12:    74 6f 20

4d15:    48 ba 63 72 65 61 74   movabs $0x7320657461657263,%rdx

4d1c:    65 20 73

4d1f:    48 89 45 10            mov    %rax,0x10(%rbp)

4d23:    48 89 55 18            mov    %rdx,0x18(%rbp)

4d27:    c7 45 20 6f 63 6b 65   movl   $0x656b636f,0x20(%rbp)

4d2e:    66 c7 45 24 74 00      movw   $0x74,0x24(%rbp)

4d34:    b8 ff ff ff ff         mov    $0xffffffff,%eax

4d39:    eb 97                  jmp    4cd2 <init_driver+0xe7>

4d3b:    48 b8 45 72 72 6f 72   movabs $0x44203a726f727245,%rax

4d42:    3a 20 44

4d45:    48 ba 4e 53 20 69 73   movabs $0x6e7520736920534e,%rdx

4d4c:    20 75 6e

4d4f:    48 89 45 00            mov    %rax,0x0(%rbp)
```

```
4d53:      48 89 55 08               mov    %rdx,0x8(%rbp)

4d57:      48 b8 61 62 6c 65 20      movabs $0x206f7420656c6261,%rax

4d5e:      74 6f 20

4d61:      48 ba 72 65 73 6f 6c      movabs $0x2065766c6f736572,%rdx

4d68:      76 65 20

4d6b:      48 89 45 10               mov    %rax,0x10(%rbp)

4d6f:      48 89 55 18               mov    %rdx,0x18(%rbp)

4d73:      48 b8 73 65 72 76 65      movabs $0x6120726576726573,%rax

4d7a:      72 20 61

4d7d:      48 89 45 20               mov    %rax,0x20(%rbp)

4d81:      c7 45 28 64 64 72 65      movl   $0x65726464,0x28(%rbp)

4d88:      66 c7 45 2c 73 73         movw   $0x7373,0x2c(%rbp)

4d8e:      c6 45 2e 00               movb   $0x0,0x2e(%rbp)

4d92:      89 df                     mov    %ebx,%edi

4d94:      e8 f7 e4 ff ff            callq  3290 <close@plt>

4d99:      b8 ff ff ff ff            mov    $0xffffffff,%eax

4d9e:      e9 2f ff ff ff            jmpq   4cd2 <init_driver+0xe7>

4da3:      4c 8d 05 1a 16 00 00      lea    0x161a(%rip),%r8        # 63c4
<array.3481+0x11e4>
4daa:      48 8d 0d cf 15 00 00      lea    0x15cf(%rip),%rcx       # 6380
<array.3481+0x11a0>
4db1:      48 c7 c2 ff ff ff ff      mov    $0xffffffffffffffff,%rdx

4db8:      be 01 00 00 00            mov    $0x1,%esi

4dbd:      48 89 ef                  mov    %rbp,%rdi

4dc0:      b8 00 00 00 00            mov    $0x0,%eax

4dc5:      e8 d6 e5 ff ff            callq  33a0 <__sprintf_chk@plt>

4dca:      89 df                     mov    %ebx,%edi

4dcc:      e8 bf e4 ff ff            callq  3290 <close@plt>

4dd1:      b8 ff ff ff ff            mov    $0xffffffff,%eax

4dd6:      e9 f7 fe ff ff            jmpq   4cd2 <init_driver+0xe7>

4ddb:      e8 90 e4 ff ff            callq  3270 <__stack_chk_fail@plt>
```

```
0000000000004de0 <driver_post>:

    4de0:       f3 0f 1e fa                     endbr64

    4de4:       53                              push    %rbx

    4de5:       4c 89 c3                        mov     %r8,%rbx

    4de8:       85 c9                           test    %ecx,%ecx

    4dea:       75 17                           jne     4e03 <driver_post+0x23>

    4dec:       48 85 ff                        test    %rdi,%rdi

    4def:       74 05                           je      4df6 <driver_post+0x16>

    4df1:       80 3f 00                        cmpb    $0x0,(%rdi)

    4df4:       75 33                           jne     4e29 <driver_post+0x49>

    4df6:       66 c7 03 4f 4b                  movw    $0x4b4f,(%rbx)

    4dfb:       c6 43 02 00                     movb    $0x0,0x2(%rbx)

    4dff:       89 c8                           mov     %ecx,%eax

    4e01:       5b                              pop     %rbx

    4e02:       c3                              retq

    4e03:       48 8d 35 d5 15 00 00            lea     0x15d5(%rip),%rsi        # 63df
<array.3481+0x11ff>
    4e0a:       bf 01 00 00 00                  mov     $0x1,%edi

    4e0f:       b8 00 00 00 00                  mov     $0x0,%eax

    4e14:       e8 07 e5 ff ff                  callq   3320 <__printf_chk@plt>

    4e19:       66 c7 03 4f 4b                  movw    $0x4b4f,(%rbx)

    4e1e:       c6 43 02 00                     movb    $0x0,0x2(%rbx)

    4e22:       b8 00 00 00 00                  mov     $0x0,%eax

    4e27:       eb d8                           jmp     4e01 <driver_post+0x21>

    4e29:       41 50                           push    %r8

    4e2b:       52                              push    %rdx

    4e2c:       4c 8d 0d c3 15 00 00            lea     0x15c3(%rip),%r9        # 63f6
<array.3481+0x1216>
    4e33:       49 89 f0                        mov     %rsi,%r8

    4e36:       48 89 f9                        mov     %rdi,%rcx

    4e39:       48 8d 15 ba 15 00 00            lea     0x15ba(%rip),%rdx        # 63fa
<array.3481+0x121a>
    4e40:       be 6e 3b 00 00                  mov     $0x3b6e,%esi
```

```
  4e45:    48 8d 3d 78 15 00 00        lea     0x1578(%rip),%rdi        # 63c4
<array.3481+0x11e4>
  4e4c:    e8 d2 f4 ff ff              callq   4323 <submitr>
  4e51:    48 83 c4 10                 add     $0x10,%rsp
  4e55:    eb aa                       jmp     4e01 <driver_post+0x21>
  4e57:    66 0f 1f 84 00 00 00        nopw    0x0(%rax,%rax,1)
  4e5e:    00 00


0000000000004e60 <__libc_csu_init>:
  4e60:    f3 0f 1e fa                 endbr64
  4e64:    41 57                       push    %r15
  4e66:    4c 8d 3d 73 2e 00 00        lea     0x2e73(%rip),%r15        # 7ce0
<__frame_dummy_init_array_entry>
  4e6d:    41 56                       push    %r14
  4e6f:    49 89 d6                    mov     %rdx,%r14
  4e72:    41 55                       push    %r13
  4e74:    49 89 f5                    mov     %rsi,%r13
  4e77:    41 54                       push    %r12
  4e79:    41 89 fc                    mov     %edi,%r12d
  4e7c:    55                          push    %rbp
  4e7d:    48 8d 2d 64 2e 00 00        lea     0x2e64(%rip),%rbp        # 7ce8
<__do_global_dtors_aux_fini_array_entry>
  4e84:    53                          push    %rbx
  4e85:    4c 29 fd                    sub     %r15,%rbp
  4e88:    48 83 ec 08                 sub     $0x8,%rsp
  4e8c:    e8 6f e1 ff ff              callq   3000 <_init>
  4e91:    48 c1 fd 03                 sar     $0x3,%rbp
  4e95:    74 1f                       je      4eb6 <__libc_csu_init+0x56>
  4e97:    31 db                       xor     %ebx,%ebx
  4e99:    0f 1f 80 00 00 00 00        nopl    0x0(%rax)
  4ea0:    4c 89 f2                    mov     %r14,%rdx
  4ea3:    4c 89 ee                    mov     %r13,%rsi
  4ea6:    44 89 e7                    mov     %r12d,%edi
```

```
    4ea9:    41 ff 14 df               callq  *(%r15,%rbx,8)

    4ead:    48 83 c3 01               add    $0x1,%rbx

    4eb1:    48 39 dd                  cmp    %rbx,%rbp

    4eb4:    75 ea                     jne    4ea0 <__libc_csu_init+0x40>

    4eb6:    48 83 c4 08               add    $0x8,%rsp

    4eba:    5b                        pop    %rbx

    4ebb:    5d                        pop    %rbp

    4ebc:    41 5c                     pop    %r12

    4ebe:    41 5d                     pop    %r13

    4ec0:    41 5e                     pop    %r14

    4ec2:    41 5f                     pop    %r15

    4ec4:    c3                        retq

    4ec5:    66 66 2e 0f 1f 84 00      data16 nopw %cs:0x0(%rax,%rax,1)

    4ecc:    00 00 00 00


0000000000004ed0 <__libc_csu_fini>:

    4ed0:    f3 0f 1e fa               endbr64

    4ed4:    c3                        retq


Disassembly of section .fini:


0000000000004ed8 <_fini>:

    4ed8:    f3 0f 1e fa               endbr64

    4edc:    48 83 ec 08               sub    $0x8,%rsp

    4ee0:    48 83 c4 08               add    $0x8,%rsp

    4ee4:    c3                        retq
```