```
Last login: Sun Jan 24 11:47:04 on ttys000
Dhrumils-Air: ~ Dhrumil$ ssh Dpate85@23.99.192.124
Dpate85@23.99.192.124's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-43-generic x86 64)
 * Documentation: https://help.ubuntu.com/
  System information as of Sun Jan 24 17:46:53 UTC 2016
  System load: 0.0
                                  Processes:
                                                       116
                5.8% of 28.80GB
  Usage of /:
                                  Users logged in:
 Memory usage: 6%
                                  IP address for eth0: 10.2.0.4
  Swap usage:
  Graph this data and manage this system at:
    https://landscape.canonical.com/
  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud
23 packages can be updated.
21 updates are security updates.
Last login: Sun Jan 24 17:46:54 2016 from 104-1-26-208.lightspeed.cicril.sbcgloba
l.net
Dpate85@Dhrumil:~$ cd dpate85
Dpate85@Dhrumil:~/dpate85$ ls
hw1 hw2 README.md
Dpate85@Dhrumil:~/dpate85$ cd hw2
Dpate85@Dhrumil:~/dpate85/hw2$ ls
puzzles
Dpate85@Dhrumil:~/dpate85/hw2$ cd pizzles
-bash: cd: pizzles: No such file or directory
Dpate85@Dhrumil:~/dpate85/hw2$ cd puzzles
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0 1 2 3 4 howto.txt iamspecial lib361.so secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ rm lib361.so
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
  1 2 3 4 howto.txt iamspecial secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ qcc 4 -shared -o lib361.so
/usr/bin/ld: warning: Cannot create .eh_frame_hdr section, --eh-frame-hdr ignored
/usr/bin/ld: error in 4(.eh_frame); no .eh_frame_hdr table will be created.
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -a 4
ELF Header:
          7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
 Magic:
  Class:
                                     ELF64
                                     2's complement, little endian
  Data:
  Version:
                                     1 (current)
  OS/ABI:
                                     UNIX - System V
  ABI Version:
  Type:
                                     EXEC (Executable file)
```

Machine: Advanced Micro Devices X86-64

Version: 0x1

Entry point address: 0x4007e0

Start of program headers: 64 (bytes into file) Start of section headers: 8792 (bytes into file)

Flags: 0x0

Size of this header: 64 (bytes)
Size of program headers: 56 (bytes)

Number of program headers: 9

Size of section headers: 64 (bytes)

Number of section headers: 28 Section header string table index: 27

Section Headers:

ection headers.							
[]	۱r]	Name	Туре	Address	Offset		
		Size	EntSize	Flags Link Info	Align		
[0]		NULL	0000000000000000	00000000		
		00000000000000000	0000000000000000	0 0	0		
[1]	.interp	PROGBITS	0000000000400238	00000238		
		000000000000001c	0000000000000000	A 0 0	1		
[2]	.note.ABI−tag	NOTE	0000000000400254	00000254		
		00000000000000020	0000000000000000	A 0 0	4		
[3]	.note.gnu.build-i		0000000000400274	00000274		
		00000000000000024	0000000000000000	A 0 0	4		
[4]	.gnu.hash	GNU_HASH	0000000000400298	00000298		
		0000000000000038	0000000000000000	A 5 0	8		
[5]	.dynsym	DYNSYM	00000000004002d0	000002d0		
		00000000000001c8	0000000000000018	A 6 1	8		
[6]	.dynstr	STRTAB	0000000000400498	00000498		
		000000000000010e	0000000000000000	A 0 0	1		
[7]	.gnu.version	VERSYM	00000000004005a6	000005a6		
		00000000000000026	00000000000000002	A 5 0	2		
[8]	.gnu.version_r	VERNEED	00000000004005d0	000005d0		
		0000000000000030	0000000000000000	A 6 1	8		
[9]	.rela.dyn	RELA	0000000000400600	00000600		
		00000000000000018	0000000000000018	A 5 0	8		
[:	10]	.rela.plt	RELA	0000000000400618	00000618		
		00000000000000f0	0000000000000018	A 5 12	8		
[:	11]	.init	PROGBITS	0000000000400708	00000708		
		000000000000001a	0000000000000000	AX 0 0	4		
[:	12]	.plt	PROGBITS	0000000000400730	00000730		
		00000000000000b0	0000000000000010	AX 0 0	16		
[:	13]	.text	PROGBITS	00000000004007e0	000007e0		
		0000000000000532	0000000000000000	AX 0 0	16		
[:	14]	.fini	PROGBITS	0000000000400d14	00000d14		
		00000000000000009	00000000000000000	AX 0 0	4		
[:	15]	.rodata	PROGBITS	0000000000400d20	00000d20		
		00000000000000bf	00000000000000000	A 0 0	8		
[:	16]	.eh_frame_hdr	PROGBITS	0000000000400de0	00000de0		
		0000000000000044	00000000000000000	A 0 0	4		
[:	17]	.eh_frame	PROGBITS	00000000000400e28	00000e28		
		000000000000013c	0000000000000000	A 0 0	8		
[:	18]	.init_array	INIT_ARRAY	00000000000601e00	00001e00		

```
80000000000000000
                       0000000000000000
                                          WA
                                                                8
                        FINI_ARRAY
[19] .fini array
                                         0000000000601e08 00001e08
     0000000000000008
                       0000000000000000
                                                   0
                                                          0
                                                                8
[20] .jcr
                                         0000000000601e10
                                                            00001e10
                        PROGBITS
     8000000000000000
                        00000000000000000
                                         WA
                                                   0
[21] .dynamic
                        DYNAMIC
                                         0000000000601e18
                                                            00001e18
     00000000000001e0
                       00000000000000010
                                          WA
                                                   6
                                                                8
[22] .got
                                         0000000000601ff8
                        PROGBITS 1
                                                            00001ff8
     80000000000000000
                       0000000000000000
                                          WA
                                                   0
                                                          0
                                                                8
[23] .got.plt
                        PROGBITS
                                         0000000000602000
                                                            00002000
     00000000000000068
                       0000000000000000
                                                   0
                                                          0
                                                                8
[24] .data
                        PROGBITS
                                         0000000000602080
                                                            00002080
     0000000000000008c
                        00000000000000000
                                         WA
                                                   0
                                                          0
                                                                32
[25] .bss
                       NOBITS
                                         000000000060210c
                                                            0000210c
     00000000000000004
                       0000000000000000
                                         WA
                                                   0
                                                                1
[26] .comment
                        PROGBITS
                                         0000000000000000
                                                            0000210c
     0000000000000004d
                       000000000000000 MS
                                                   0
                                                          0
                                                                1
[27] shstrtab
                        STRTAB
                                         0000000000000000
                                                            00002159
     000000000000018 0000000000000000
                                                          0
W (write), A (alloc), X (execute), M (merge), S (strings), l (large)
```

Key to Flags:

I (info), L (link order), G (group), T (TLS), E (exclude), x (unknown) O (extra OS processing required) o (OS specific), p (processor specific)

There are no section groups in this file.

Program Headers:

Туре	Offset	VirtAddr	PhysAddr
	FileSiz	MemSiz	Flags Align
PHDR	0×00000000000000040	0×0000000000400040	0×0000000000400040
	0x00000000000001f8	0x00000000000001f8	RE 8
INTERP	0x00000000000000238	0x0000000000400238	0x0000000000400238
	0x000000000000001c	0x000000000000001c	R 1
[Requesting	g program interpreto	er: /lib64/ld-linux-	-x86-64.so.2]
LOAD	0×0000000000000000	0×0000000000400000	0×0000000000400000
	0x0000000000000f64	0x0000000000000164	R E 200000
LOAD	0x0000000000001e00	0x0000000000601e00	0x0000000000601e00
	0x000000000000030c	0×0000000000000310	RW 200000
DYNAMIC	0x0000000000001e18	0x0000000000601e18	0x0000000000601e18
	0x00000000000001e0	0x00000000000001e0	RW 8
NOTE	0x00000000000000254	0×0000000000400254	0×0000000000400254
	0x0000000000000044	0×0000000000000044	R 4
GNU_EH_FRAME	0x0000000000000de0	0x0000000000400de0	0x0000000000400de0
	0x00000000000000044	0×0000000000000044	R 4
GNU_STACK	0x00000000000000000	0×00000000000000000	0×00000000000000000
_	0×00000000000000000	0×0000000000000000	RW 10
GNU_RELRO	0x0000000000001e00	0x0000000000601e00	0x0000000000601e00
_	0×00000000000000200	0×00000000000000200	R 1

```
Section to Segment mapping:
```

Segment Sections...

00

01 .interp

```
02
          .interp .note.ABI-tag .note.gnu.build-id .gnu.hash .dynsym .dynstr .gnu
.version .gnu.version r .rela.dyn .rela.plt .init .plt .text .fini .rodata .eh fr
ame hdr .eh frame
          .init array .fini array .jcr .dynamic .got .got.plt .data .bss
   03
   04
          .dynamic
   05
          .note.ABI-tag .note.gnu.build-id
   06
          .eh_frame_hdr
   07
   80
          .init_array .fini_array .jcr .dynamic .got
Dynamic section at offset 0x1e18 contains 25 entries:
                                          Name/Value
  Tag
             Type
 0x0000000000000001 (NEEDED)
                                         Shared library: [lib361.so]
 0x000000000000001 (NEEDED)
                                         Shared library: [libc.so.6]
 0x0000000000000000 (INIT)
                                         0x400708
 0x000000000000000d (FINI)
                                         0x400d14
 0x0000000000000019 (INIT ARRAY)
                                         0x601e00
 0x000000000000001b (INIT ARRAYSZ)
                                         8 (bytes)
 0x000000000000001a (FINI ARRAY)
                                         0x601e08
                                         8 (bytes)
 0x000000000000001c (FINI ARRAYSZ)
 0x00000006ffffef5 (GNU HASH)
                                         0x400298
 0x0000000000000005 (STRTAB)
                                         0x400498
 0x0000000000000000 (SYMTAB)
                                         0x4002d0
                                         270 (bytes)
 0x0000000000000000 (STRSZ)
 0x000000000000000 (SYMENT)
                                         24 (bytes)
 0x0000000000000015 (DEBUG)
                                         0x0
 0x0000000000000003 (PLTGOT)
                                         0x602000
 0x0000000000000000 (PLTRELSZ)
                                         240 (bytes)
 0x000000000000014 (PLTREL)
                                         RELA
 0x0000000000000017 (JMPREL)
                                         0x400618
 0x0000000000000007 (RELA)
                                         0x400600
 0x0000000000000008 (RELASZ)
                                         24 (bytes)
 0x000000000000000 (RELAENT)
                                         24 (bytes)
 0x00000006ffffffe (VERNEED)
                                         0x4005d0
 0x00000006fffffff (VERNEEDNUM)
                                         1
 0x00000006ffffff0 (VERSYM)
                                         0x4005a6
 0x0000000000000000 (NULL)
                                         0x0
Relocation section '.rela.dyn' at offset 0x600 contains 1 entries:
                                                               Sym. Name + Addend
                                                 Sym. Value
  Offset
                                 Type
000000601ff8
              000a0000006 R X86 64 GLOB DAT 00000000000000 gmon start + 0
Relocation section '.rela.plt' at offset 0x618 contains 10 entries:
  Offset
                  Info
                                 Type
                                                 Sym. Value
                                                               Sym. Name + Addend
000000602018
              000200000007 R_X86_64_JUMP_SL0 000000000000000 puts + 0
              00030000007 R_X86_64_JUMP_SL0 000000000000000 secretoperation + 0
000000602020
000000602028
              000400000007 R X86 64 JUMP SLO 0000000000000000 strlen + 0
              000500000007 R_X86_64_JUMP_SL0 0000000000000000 __stack_chk_fail +
000000602030
0
              000600000007 R_X86_64_JUMP_SLO 0000000000000000 printf + 0
000000602038
              000700000007 R_X86_64_JUMP_SL0 000000000000000 __assert_fail + 0
000000602040
              000800000007 R_X86_64_JUMP_SL0 000000000000000 __libc_start_main +
000000602048
 0
```

```
000000602050
              00090000007 R_X86_64_JUMP_SL0 000000000000000 calloc + 0
              000a0000007 R_X86_64_JUMP_SL0 000000000000000 __gmon_start__ + 0
000000602058
              000b00000007 R_X86_64_JUMP_SL0 000000000000000 getlogin_r + 0
000000602060
The decoding of unwind sections for machine type Advanced Micro Devices X86-64 is
 not currently supported.
Symbol table '.dynsym' contains 19 entries:
   Num:
           Value
                          Size Type
                                       Bind
                                              Vis
                                                        Ndx Name
     0: 0000000000000000
                             0 NOTYPE
                                       LOCAL DEFAULT
                                                        UND
     1: 00000000000000000
                             0 NOTYPE
                                       WEAK
                                              DEFAULT
                                                       UND _ITM_deregisterTMClone
Tab
     2: 00000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND puts@GLIBC 2.2.5 (2)
     3: 0000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND secretoperation
     4: 0000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND strlen@GLIBC 2.2.5 (2)
                             0 FUNC
                                                        UND __stack_chk_fail@GLIBC
     5: 00000000000000000
                                       GLOBAL DEFAULT
_2.4 (3)
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND printf@GLIBC 2.2.5 (2)
     6: 00000000000000000
     7: 0000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND __assert_fail@GLIBC_2.
2.5 (2)
     8: 0000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND libc start main@GLIB
C_{2.2.5}(2)
     9: 0000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND calloc@GLIBC 2.2.5 (2)
    10: 0000000000000000
                             0 NOTYPE
                                                        UND __gmon_start__
                                       WEAK
                                              DEFAULT
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND getlogin_r@GLIBC_2.2.5
    11: 0000000000000000
 (2)
    12: 0000000000000000
                             0 NOTYPE
                                       WEAK
                                              DEFAULT
                                                        UND _Jv_RegisterClasses
    13: 00000000000000000
                             0 NOTYPE
                                       WEAK
                                                        UND ITM registerTMCloneTa
                                              DEFAULT
ble
    14: 000000000060210c
                             0 NOTYPE
                                       GLOBAL DEFAULT
                                                         24 _edata
    15: 0000000000602110
                             0 NOTYPE
                                       GLOBAL DEFAULT
                                                         25 _end
    16: 000000000060210c
                             0 NOTYPE
                                       GLOBAL DEFAULT
                                                         25 __bss_start
    17: 0000000000400708
                             0 FUNC
                                       GLOBAL DEFAULT
                                                         11 init
    18: 0000000000400d14
                             0 FUNC
                                       GLOBAL DEFAULT
                                                         14 fini
Histogram for `.gnu.hash' bucket list length (total of 3 buckets):
                    % of total Coverage
 Length Number
         0
                       0.0%)
      0
      1 1
                    ( 33.3%)
                                 20.0%
                    (66.7%)
                                100.0%
Version symbols section '.gnu.version' contains 19 entries:
 Addr: 0000000004005a6 Offset: 0x0005a6 Link: 5 (.dynsym)
  000:
         0 (*local*)
                           0 (*local*)
                                             2 (GLIBC_2.2.5)
                                                                0 (*local*)
  004:
         2 (GLIBC 2.2.5)
                           3 (GLIBC 2.4)
                                             2 (GLIBC 2.2.5)
                                                                2 (GLIBC 2.2.5)
         2 (GLIBC_2.2.5)
                           2 (GLIBC_2.2.5)
                                             0 (*local*)
                                                                2 (GLIBC_2.2.5)
  008:
  00c:
         0 (*local*)
                           0 (*local*)
                                             1 (*global*)
                                                                1 (*global*)
  010:
         1 (*qlobal*)
                           1 (*global*)
                                             1 (*global*)
Version needs section '.gnu.version_r' contains 1 entries:
 Addr: 0x00000000004005d0 Offset: 0x0005d0 Link: 6 (.dynstr)
  000000: Version: 1 File: libc.so.6 Cnt: 2
```

Name: GLIBC 2.4 Flags: none Version: 3

0x0010:

```
0x0020:
            Name: GLIBC_2.2.5 Flags: none Version: 2
Displaying notes found at file offset 0x00000254 with length 0x00000020:
  0wner
                        Data size
                                        Description
  GNU
                       0x00000010
                                        NT_GNU_ABI_TAG (ABI version tag)
    OS: Linux, ABI: 2.6.24
Displaying notes found at file offset 0x00000274 with length 0x00000024:
  0wner
                        Data size
                                        Description
  GNU
                       0x00000014
                                        NT_GNU_BUILD_ID (unique build ID bitstrin
a)
    Build ID: 516c99c45c7b1cd513589f91ae029c0f1528d553
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s
readelf: Warning: Nothing to do.
Usage: readelf <option(s)> elf-file(s)
 Display information about the contents of ELF format files
 Options are:
  -a --all
                         Equivalent to: -h -l -S -s -r -d -V -A -I
  -h --file-header
                         Display the ELF file header
  -l --program-headers
                         Display the program headers
     --seaments
                         An alias for --program-headers
                         Display the sections' header
  -S --section-headers
     --sections
                         An alias for --section-headers
                         Display the section groups
  -q --section-groups
                         Display the section details
  -t --section-details
                         Equivalent to: -h -l -S
  -e --headers
  -s --syms
                         Display the symbol table
     --symbols
                         An alias for --syms
  --dyn-syms
                         Display the dynamic symbol table
  -n --notes
                         Display the core notes (if present)
  -r --relocs
                         Display the relocations (if present)
                         Display the unwind info (if present)
  -u --unwind
  -d --dynamic
                         Display the dynamic section (if present)
  -V --version-info
                         Display the version sections (if present)
  -A --arch-specific
                         Display architecture specific information (if any)
  -c --archive-index
                         Display the symbol/file index in an archive
  -D --use-dynamic
                         Use the dynamic section info when displaying symbols
  -x --hex-dump=<number|name>
                         Dump the contents of section <number|name> as bytes
  -p --string-dump=<number|name>
                         Dump the contents of section <number|name> as strings
  -R --relocated-dump=<number|name>
                         Dump the contents of section <number|name> as relocated
bytes
  -w[lLiaprmfFsoRt] or
  --debug-dump[=rawline,=decodedline,=info,=abbrev,=pubnames,=aranges,=macro,=fra
mes,
               =frames-interp,=str,=loc,=Ranges,=pubtypes,
               =qdb index,=trace info,=trace abbrev,=trace aranges,
               =addr,=cu_index]
                         Display the contents of DWARF2 debug sections
  --dwarf-depth=N
                         Do not display DIEs at depth N or greater
  --dwarf-start=N
                         Display DIEs starting with N, at the same depth
```

```
or deeper
                         Display histogram of bucket list lengths
  -I --histogram
  −W −−wide
                         Allow output width to exceed 80 characters
  @<file>
                         Read options from <file>
  -H --help
                         Display this information
  -v --version
                         Display the version number of readelf
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s 4
Symbol table '.dynsym' contains 19 entries:
           Value
                          Size Type
                                               Vis
                                                        Ndx Name
   Num:
                                        Bind
     0: 0000000000000000
                             0 NOTYPE
                                        LOCAL DEFAULT
                                                        UND
     1: 00000000000000000
                             0 NOTYPE
                                        WEAK
                                               DEFAULT
                                                        UND _ITM_deregisterTMClone
Tab
     2: 00000000000000000
                             0 FUNC
                                        GLOBAL DEFAULT
                                                        UND puts@GLIBC_2.2.5 (2)
     3: 00000000000000000
                             0 FUNC
                                        GLOBAL DEFAULT
                                                        UND secretoperation
                             0 FUNC
     4: 0000000000000000
                                        GLOBAL DEFAULT
                                                        UND strlen@GLIBC_2.2.5 (2)
     5: 00000000000000000
                             0 FUNC
                                        GLOBAL DEFAULT
                                                        UND __stack_chk_fail@GLIBC
2.4 (3)
     6: 0000000000000000
                             0 FUNC
                                        GLOBAL DEFAULT
                                                        UND printf@GLIBC_2.2.5 (2)
                             0 FUNC
     7: 00000000000000000
                                        GLOBAL DEFAULT
                                                        UND __assert_fail@GLIBC_2.
2.5 (2)
     8: 0000000000000000
                             0 FUNC
                                        GLOBAL DEFAULT
                                                        UND __libc_start_main@GLIB
C 2.2.5 (2)
     9: 0000000000000000
                             0 FUNC
                                                        UND calloc@GLIBC_2.2.5 (2)
                                        GLOBAL DEFAULT
    10: 0000000000000000
                             0 NOTYPE
                                        WEAK
                                               DEFAULT
                                                        UND __gmon_start__
    11: 0000000000000000
                             0 FUNC
                                        GLOBAL DEFAULT
                                                        UND getlogin r@GLIBC 2.2.5
 (2)
    12: 00000000000000000
                             0 NOTYPE
                                        WEAK
                                               DEFAULT
                                                        UND Jv RegisterClasses
    13: 00000000000000000
                             0 NOTYPE
                                        WEAK
                                               DEFAULT
                                                        UND _ITM_registerTMCloneTa
ble
    14: 000000000060210c
                             0 NOTYPE
                                        GLOBAL DEFAULT
                                                         24 _edata
    15: 0000000000602110
                             0 NOTYPE
                                        GLOBAL DEFAULT
                                                         25 _end
    16: 000000000060210c
                             0 NOTYPE
                                        GLOBAL DEFAULT
                                                         25 __bss_start
                             0 FUNC
    17: 0000000000400708
                                        GLOBAL DEFAULT
                                                         11 init
    18: 0000000000400d14
                             0 FUNC
                                        GLOBAL DEFAULT
                                                         14 _fini
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump 4
Usage: objdump <option(s)> <file(s)>
Display information from object <file(s)>.
At least one of the following switches must be given:
  -a, --archive-headers
                           Display archive header information
  -f, --file-headers
                           Display the contents of the overall file header
                           Display object format specific file header contents
  -p, --private-headers
  -P, --private=OPT,OPT...
                           Display object format specific contents
  -h, --[section-]headers
                           Display the contents of the section headers
  -x, --all-headers
                           Display the contents of all headers
  -d, --disassemble
                           Display assembler contents of executable sections
  -D, --disassemble-all
                           Display assembler contents of all sections
  -S, --source
                           Intermix source code with disassembly
  -s, --full-contents
                           Display the full contents of all sections requested
  -g, --debugging
                           Display debug information in object file
  -e, --debugging-tags
                           Display debug information using ctags style
  -G, --stabs
                           Display (in raw form) any STABS info in the file
```

-W[lLiaprmfFsoRt] or

```
--dwarf[=rawline,=decodedline,=info,=abbrev,=pubnames,=aranges,=macro,=frames,
          =frames-interp,=str,=loc,=Ranges,=pubtypes,
          =gdb_index,=trace_info,=trace_abbrev,=trace_aranges,
          =addr,=cu index]
                           Display DWARF info in the file
  -t, --syms
                           Display the contents of the symbol table(s)
  -T, --dynamic-syms
                           Display the contents of the dynamic symbol table
  -r, --reloc
                           Display the relocation entries in the file
  -R, --dynamic-reloc
                           Display the dynamic relocation entries in the file
  0<file>
                           Read options from <file>
                           Display this program's version number
  -v, --version
  −i, --info
                           List object formats and architectures supported
  -H, --help
                           Display this information
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -S 4
       file format elf64-x86-64
4:
Disassembly of section .init:
0000000000400708 < init>:
  400708:
                48 83 ec 08
                                        sub
                                               $0x8,%rsp
  40070c:
                48 8b 05 e5 18 20 00
                                               0x2018e5(%rip),%rax
                                                                          # 601ff
                                        mov
8 < fini+0x2012e4>
  400713:
               48 85 c0
                                        test
                                               %rax,%rax
                74 05
  400716:
                                               40071d < init+0x15>
                                        jе
  400718:
                e8 a3 00 00 00
                                        callq
                                               4007c0 <__gmon_start__@plt>
                48 83 c4 08
  40071d:
                                        add
                                               $0x8,%rsp
  400721:
                с3
                                        retq
Disassembly of section .plt:
0000000000400730 <puts@plt-0x10>:
  400730:
               ff 35 d2 18 20 00
                                        pushq 0x2018d2(%rip)
                                                                     # 602008 < f
ini+0x2012f4>
               ff 25 d4 18 20 00
  400736:
                                               *0x2018d4(%rip)
                                                                      # 602010 <
                                        jmpq
fini+0x2012fc>
  40073c:
                0f 1f 40 00
                                               0x0(%rax)
                                        nopl
0000000000400740 <puts@plt>:
                                                                      # 602018 <
  400740:
               ff 25 d2 18 20 00
                                        jmpq
                                               *0x2018d2(%rip)
fini+0x201304>
  400746:
               68 00 00 00 00
                                        pushq
                                               $0x0
                e9 e0 ff ff ff
  40074b:
                                        jmpq
                                               400730 <_init+0x28>
000000000400750 <secretoperation@plt>:
                                                                      # 602020 <_
  400750:
               ff 25 ca 18 20 00
                                        jmpq
                                               *0x2018ca(%rip)
fini+0x20130c>
  400756:
                68 01 00 00 00
                                        pusha
                                               $0x1
                e9 d0 ff ff ff
  40075b:
                                        jmpq
                                               400730 <_init+0x28>
0000000000400760 <strlen@plt>:
  400760:
               ff 25 c2 18 20 00
                                        jmpq
                                               *0x2018c2(%rip)
                                                                      # 602028 <
```

```
fini+0x201314>
  400766:
                68 02 00 00 00
                                         pushq
                                                 $0x2
  40076b:
                e9 c0 ff ff ff
                                         jmpq
                                                 400730 <_init+0x28>
000000000400770 <__stack_chk_fail@plt>:
                ff 25 ba 18 20 00
  400770:
                                                 *0x2018ba(%rip)
                                                                        # 602030 <_
                                         jmpq
fini+0x20131c>
                68 03 00 00 00
  400776:
                                         pushq
                                                 $0x3
  40077b:
                e9 b0 ff ff ff
                                         jmpq
                                                 400730 <_init+0x28>
0000000000400780 <printf@plt>:
                                                                        # 602038 <_
                ff 25 b2 18 20 00
                                                 *0x2018b2(%rip)
  400780:
                                         jmpq
fini+0x201324>
  400786:
                68 04 00 00 00
                                                 $0x4
                                         pushq
  40078b:
                e9 a0 ff ff ff
                                                 400730 < init+0x28>
                                         jmpq
000000000400790 <__assert_fail@plt>:
                                                                        # 602040 <_
                ff 25 aa 18 20 00
                                                 *0x2018aa(%rip)
                                         jmpq
fini+0x20132c>
                68 05 00 00 00
  400796:
                                         pushq
                                                 $0x5
                e9 90 ff ff ff
  40079b:
                                         jmpq
                                                 400730 < init+0x28>
0000000004007a0 <__libc_start_main@plt>:
                ff 25 a2 18 20 00
  4007a0:
                                         jmpq
                                                 *0x2018a2(%rip)
                                                                        # 602048 <_
fini+0x201334>
  4007a6:
                68 06 00 00 00
                                         pushq
                                                 $0x6
  4007ab:
                e9 80 ff ff ff
                                         jmpq
                                                 400730 <_init+0x28>
00000000004007b0 <calloc@plt>:
                ff 25 9a 18 20 00
  4007b0:
                                                 *0x20189a(%rip)
                                         jmpq
                                                                        # 602050 <_
fini+0x20133c>
  4007b6:
                68 07 00 00 00
                                         pushq
                                                 $0x7
  4007bb:
                e9 70 ff ff ff
                                         jmpq
                                                 400730 <_init+0x28>
0000000004007c0 <__gmon_start__@plt>:
  4007c0:
                ff 25 92 18 20 00
                                                 *0x201892(%rip)
                                                                        # 602058 <
                                         jmpq
fini+0x201344>
  4007c6:
                68 08 00 00 00
                                         pushq
                                                 $0x8
  4007cb:
                e9 60 ff ff ff
                                                 400730 <_init+0x28>
                                         jmpq
00000000004007d0 <getlogin r@plt>:
  4007d0:
                ff 25 8a 18 20 00
                                                 *0x20188a(%rip)
                                                                        # 602060 <_
                                         jmpq
fini+0x20134c>
  4007d6:
                68 09 00 00 00
                                         pushq
                                                 $0x9
  4007db:
                e9 50 ff ff ff
                                         jmpq
                                                 400730 <_init+0x28>
Disassembly of section .text:
000000000004007e0 <.text>:
  4007e0:
                31 ed
                                         xor
                                                 %ebp,%ebp
  4007e2:
                49 89 d1
                                         mov
                                                 %rdx,%r9
                5e
                                                 %rsi
  4007e5:
                                         pop
  4007e6:
                48 89 e2
                                         mov
                                                 %rsp,%rdx
```

```
4007e9:
                 48 83 e4 f0
                                           and
                                                   $0xfffffffffffffff,%rsp
  4007ed:
                 50
                                           push
                                                  %rax
                 54
  4007ee:
                                           push
                                                  %rsp
                 49 c7 c0 10 0d 40 00
  4007ef:
                                                   $0x400d10,%r8
                                           mov
                 48 c7 c1 a0 0c 40 00
  4007f6:
                                                   $0x400ca0,%rcx
                                           mov
  4007fd:
                 48 c7 c7 cd 08 40 00
                                                   $0x4008cd,%rdi
                                           mov
  400804:
                 e8 97 ff ff ff
                                                  4007a0 <__libc_start_main@plt>
                                           callq
                 f4
  400809:
                                           hlt
  40080a:
                 66 Of 1f 44 00 00
                                           nopw
                                                  0x0(%rax,%rax,1)
                 b8 17 21 60 00
                                                   $0x602117,%eax
  400810:
                                           mov
  400815:
                 55
                                           push
                                                  %rbp
  400816:
                 48 2d 10 21 60 00
                                                   $0x602110,%rax
                                           sub
                 48 83 f8 0e
  40081c:
                                           cmp
                                                  $0xe,%rax
  400820:
                 48 89 e5
                                           mov
                                                  %rsp,%rbp
  400823:
                 77 02
                                                  400827 <getlogin_r@plt+0x57>
                                           jа
  400825:
                 5d
                                           pop
                                                  %rbp
  400826:
                 c3
                                           retq
  400827:
                 b8 00 00 00 00
                                                   $0x0,%eax
                                           mov
  40082c:
                 48 85 c0
                                           test
                                                  %rax,%rax
                 74 f4
  40082f:
                                                  400825 <getlogin_r@plt+0x55>
                                           jе
                 5d
  400831:
                                           pop
                 bf 10 21 60 00
                                                   $0x602110,%edi
  400832:
                                           mov
                 ff e0
  400837:
                                           jmpq
                                                  *%rax
  400839:
                 0f 1f 80 00 00 00 00
                                           nopl
                                                  0x0(%rax)
                 b8 10 21 60 00
  400840:
                                           mov
                                                   $0x602110,%eax
                 55
  400845:
                                           push
                                                  %rbp
  400846:
                 48 2d 10 21 60 00
                                           sub
                                                   $0x602110,%rax
                 48 c1 f8 03
  40084c:
                                           sar
                                                   $0x3,%rax
  400850:
                 48 89 e5
                                           mov
                                                  %rsp,%rbp
                 48 89 c2
  400853:
                                                  %rax,%rdx
                                           mov
  400856:
                 48 c1 ea 3f
                                                   $0x3f,%rdx
                                           shr
  40085a:
                 48 01 d0
                                           add
                                                  %rdx,%rax
  40085d:
                 48 d1 f8
                                           sar
                                                  %rax
  400860:
                 75 02
                                                  400864 <getlogin_r@plt+0x94>
                                           jne
  400862:
                 5d
                                           pop
                                                  %rbp
  400863:
                 с3
                                           retq
  400864:
                 ba 00 00 00 00
                                           mov
                                                   $0x0,%edx
                 48 85 d2
  400869:
                                           test
                                                  %rdx,%rdx
  40086c:
                 74 f4
                                                  400862 <getlogin_r@plt+0x92>
                                           jе
  40086e:
                 5d
                                                  %rbp
                                           pop
  40086f:
                 48 89 c6
                                           mov
                                                  %rax,%rsi
  400872:
                 bf 10 21 60 00
                                           mov
                                                  $0x602110,%edi
  400877:
                 ff e2
                                           jmpq
                                                  *%rdx
                 0f 1f 80 00 00 00 00
  400879:
                                           nopl
                                                  0x0(%rax)
  400880:
                 80 3d 85 18 20 00 00
                                           cmpb
                                                   $0x0,0x201885(%rip)
                                                                                # 60210
c <_edata>
  400887:
                 75 11
                                           jne
                                                  40089a <getlogin r@plt+0xca>
                 55
  400889:
                                           push
                                                  %rbp
  40088a:
                 48 89 e5
                                           mov
                                                  %rsp,%rbp
  40088d:
                 e8 7e ff ff ff
                                           callq
                                                  400810 <getlogin_r@plt+0x40>
  400892:
                 5d
                                           pop
                                                  %rbp
                 c6 05 72 18 20 00 01
                                                   $0x1,0x201872(%rip)
  400893:
                                                                                # 60210
                                           movb
c <_edata>
```

```
40089a:
                 f3 c3
                                           repz retq
                 0f 1f 40 00
  40089c:
                                           nopl
                                                  0x0(%rax)
                 48 83 3d 68 15 20 00
  4008a0:
                                           cmpq
                                                  $0x0,0x201568(%rip)
                                                                               # 601e1
0 <_fini+0x2010fc>
  4008a7:
                 00
  4008a8:
                 74 1e
                                           jе
                                                  4008c8 <getlogin_r@plt+0xf8>
  4008aa:
                 b8 00 00 00 00
                                           mov
                                                  $0x0,%eax
                 48 85 c0
                                           test
  4008af:
                                                  %rax,%rax
  4008b2:
                 74 14
                                                  4008c8 <getlogin_r@plt+0xf8>
                                           jе
                 55
  4008b4:
                                                  %rbp
                                           push
  4008b5:
                 bf 10 1e 60 00
                                           mov
                                                  $0x601e10,%edi
  4008ba:
                 48 89 e5
                                           mov
                                                  %rsp,%rbp
  4008bd:
                 ff d0
                                                  *%rax
                                           callq
  4008bf:
                 5d
                                                  %rbp
                                           pop
  4008c0:
                 e9 7b ff ff ff
                                           jmpq
                                                  400840 <getlogin r@plt+0x70>
  4008c5:
                 0f 1f 00
                                           nopl
  4008c8:
                 e9 73 ff ff ff
                                           jmpq
                                                  400840 <getlogin_r@plt+0x70>
  4008cd:
                 55
                                          push
                                                  %rbp
  4008ce:
                 48 89 e5
                                           mov
                                                  %rsp,%rbp
                 48 83 ec 10
  4008d1:
                                           sub
                                                  $0x10,%rsp
                 c7 45 f4 01 00 00 00
                                                  $0x1,-0xc(%rbp)
  4008d5:
                                           movl
                 c7 45 f8 02 00 00 00
                                                  $0x2,-0x8(%rbp)
  4008dc:
                                           movl
                 c7 45 fc 00 00 00 00
                                                  $0x0,-0x4(%rbp)
  4008e3:
                                           movl
                 bf 70 0d 40 00
                                                  $0x400d70,%edi
  4008ea:
                                           mov
                 e8 4c fe ff ff
  4008ef:
                                           callq
                                                  400740 <puts@plt>
                 be 06 00 00 00
  4008f4:
                                           mov
                                                  $0x6,%esi
  4008f9:
                 bf 03 00 00 00
                                                  $0x3,%edi
                                           mov
                 e8 4d fe ff ff
  4008fe:
                                           callq
                                                  400750 <secretoperation@plt>
  400903:
                 89 45 fc
                                                  %eax,-0x4(%rbp)
                                           mov
                 83 7d fc 0a
  400906:
                                           cmpl
                                                  $0xa,-0x4(%rbp)
  40090a:
                 74 19
                                           jе
                                                  400925 < getlogin_r@plt+0x155>
  40090c:
                 b9 da 0d 40 00
                                                  $0x400dda,%ecx
                                           mov
  400911:
                 ba 12 00 00 00
                                           mov
                                                  $0x12,%edx
  400916:
                 be b7 0d 40 00
                                                  $0x400db7,%esi
                                           mov
  40091b:
                 bf c1 0d 40 00
                                           mov
                                                  $0x400dc1,%edi
                 e8 6b fe ff ff
  400920:
                                           callq
                                                  400790 <__assert_fail@plt>
  400925:
                 8b 55 f8
                                           mov
                                                  -0x8(%rbp),%edx
                 8b 45 f4
  400928:
                                                  -0xc(%rbp),%eax
                                           mov
  40092b:
                 89 d6
                                                  %edx,%esi
                                           mov
                 89 c7
  40092d:
                                           mov
                                                  %eax,%edi
                 e8 1c fe ff ff
  40092f:
                                           callq
                                                  400750 <secretoperation@plt>
  400934:
                 89 45 fc
                                           mov
                                                  %eax,-0x4(%rbp)
                 83 7d fc 04
  400937:
                                           cmpl
                                                  $0x4,-0x4(%rbp)
                 74 19
                                                  400956 <getlogin_r@plt+0x186>
  40093b:
                                           jе
  40093d:
                 b9 da 0d 40 00
                                           mov
                                                  $0x400dda,%ecx
                 ba 14 00 00 00
                                                  $0x14,%edx
  400942:
                                           mov
  400947:
                 be b7 0d 40 00
                                           mov
                                                  $0x400db7,%esi
  40094c:
                 bf ce 0d 40 00
                                           mov
                                                  $0x400dce,%edi
  400951:
                 e8 3a fe ff ff
                                           calla
                                                  400790 < assert fail@plt>
                                                  0x201733(%rip),%rax
  400956:
                 48 8b 05 33 17 20 00
                                           mov
                                                                               # 60209
0 < fini+0x20137c>
  40095d:
                 48 89 c7
                                                  %rax,%rdi
                                           mov
                                                  40098d <getlogin_r@plt+0x1bd>
  400960:
                 e8 28 00 00 00
                                           callq
```

```
400965:
                 48 89 c2
                                                  %rax,%rdx
                                          mov
                                                  0x201731(%rip),%rcx
  400968:
                 48 8b 0d 31 17 20 00
                                                                               # 6020a
                                          mov
0 <_fini+0x20138c>
  40096f:
                 48 8b 05 22 17 20 00
                                                  0x201722(%rip),%rax
                                                                               # 60209
                                          mov
8 <_fini+0x201384>
  400976:
                 48 89 ce
                                                  %rcx,%rsi
                                          mov
  400979:
                 48 89 c7
                                                  %rax,%rdi
                                          mov
                 b8 00 00 00 00
                                                  $0x0,%eax
  40097c:
                                          mov
  400981:
                 e8 fa fd ff ff
                                          callq
                                                  400780 <printf@plt>
                 b8 00 00 00 00
  400986:
                                                  $0x0,%eax
                                          mov
  40098b:
                 c9
                                          leaveg
  40098c:
                 c3
                                          retq
  40098d:
                 55
                                          push
                                                  %rbp
  40098e:
                 48 89 e5
                                                  %rsp,%rbp
                                          mov
  400991:
                 53
                                                  %rbx
                                          push
  400992:
                 48 81 ec 38 04 00 00
                                          sub
                                                  $0x438,%rsp
  400999:
                 48 89 bd c8 fb ff ff
                                          mov
                                                  %rdi,-0x438(%rbp)
  4009a0:
                 64 48 8b 04 25 28 00
                                                  %fs:0x28,%rax
                                          mov
  4009a7:
                 00 00
                 48 89 45 e8
                                                  %rax,-0x18(%rbp)
  4009a9:
                                          mov
                 31 c0
                                                  %eax,%eax
  4009ad:
                                          xor
                 48 8d 85 e0 fb ff ff
  4009af:
                                          lea
                                                  -0x420(%rbp),%rax
                 be 00 04 00 00
                                                  $0x400,%esi
  4009b6:
                                          mov
  4009bb:
                 48 89 c7
                                          mov
                                                  %rax,%rdi
                 e8 0d fe ff ff
  4009be:
                                          callq
                                                  4007d0 <getlogin_r@plt>
                 c7 85 d4 fb ff ff 00
                                                  $0x0,-0x42c(%rbp)
  4009c3:
                                          movl
  4009ca:
                 00 00 00
  4009cd:
                 eb 3e
                                                  400a0d <getlogin r@plt+0x23d>
                                          jmp
  4009cf:
                 8b 85 d4 fb ff ff
                                          mov
                                                  -0x42c(%rbp),%eax
                 48 98
  4009d5:
                                          cltq
  4009d7:
                 0f b6 94 05 e0 fb ff
                                          movzbl -0x420(%rbp,%rax,1),%edx
  4009de:
                 ff
  4009df:
                 8b 85 d4 fb ff ff
                                          mov
                                                  -0x42c(%rbp),%eax
  4009e5:
                 48 63 c8
                                          movslq %eax,%rcx
  4009e8:
                 48 8b 85 c8 fb ff ff
                                                  -0x438(%rbp),%rax
                                          mov
  4009ef:
                 48 01 c8
                                                  %rcx,%rax
                                          add
  4009f2:
                 0f b6 00
                                          movzbl (%rax),%eax
  4009f5:
                 31 c2
                                                  %eax,%edx
                                          xor
  4009f7:
                 8b 85 d4 fb ff ff
                                                  -0x42c(%rbp),%eax
                                          mov
                 48 98
  4009fd:
                                          cltq
  4009ff:
                 88 94 05 e0 fb ff ff
                                          mov
                                                  %dl,-0x420(%rbp,%rax,1)
                 83 85 d4 fb ff ff 01
  400a06:
                                          addl
                                                  $0x1,-0x42c(%rbp)
                 8b 85 d4 fb ff ff
  400a0d:
                                          mov
                                                  -0x42c(%rbp),%eax
                 48 63 d8
  400a13:
                                          movslq %eax,%rbx
                 48 8d 85 e0 fb ff ff
  400a16:
                                          lea
                                                  -0x420(%rbp),%rax
                 48 89 c7
  400a1d:
                                          mov
                                                  %rax,%rdi
  400a20:
                 e8 3b fd ff ff
                                          callq
                                                  400760 <strlen@plt>
                 48 39 c3
                                                  %rax,%rbx
  400a25:
                                          cmp
                 72 a5
  400a28:
                                          jb
                                                  4009cf <getlogin_r@plt+0x1ff>
                 8b 85 d4 fb ff ff
  400a2a:
                                          mov
                                                  -0x42c(%rbp),%eax
  400a30:
                 48 63 c8
                                          movslq %eax,%rcx
                 48 8d 95 d8 fb ff ff
  400a33:
                                                  -0x428(%rbp),%rdx
                                          lea
                                                  -0x420(%rbp),%rax
  400a3a:
                 48 8d 85 e0 fb ff ff
                                          lea
```

```
400a41:
               48 89 ce
                                                %rcx,%rsi
                                        mov
               48 89 c7
400a44:
                                                %rax,%rdi
                                        mov
400a47:
              e8 1e 00 00 00
                                        callq
                                                400a6a <getlogin_r@plt+0x29a>
              48 8b 75 e8
                                                -0x18(%rbp), %rsi
400a4c:
                                        mov
               64 48 33 34 25 28 00
400a50:
                                                %fs:0x28,%rsi
                                        xor
               00 00
400a57:
400a59:
               74 05
                                                400a60 <getlogin r@plt+0x290>
                                        ie
               e8 10 fd ff ff
                                                400770 <__stack_chk_fail@plt>
400a5b:
                                        callq
400a60:
               48 81 c4 38 04 00 00
                                        add
                                                $0x438,%rsp
               5b
400a67:
                                        pop
                                                %rbx
400a68:
              5d
                                        pop
                                                %rbp
400a69:
               с3
                                        retq
400a6a:
              55
                                                %rbp
                                        push
400a6b:
              48 89 e5
                                                %rsp,%rbp
                                        mov
400a6e:
              48 83 ec 40
                                                $0x40,%rsp
                                        sub
400a72:
              48 89 7d d8
                                        mov
                                                %rdi,-0x28(%rbp)
400a76:
              48 89 75 d0
                                        mov
                                                %rsi,-0x30(%rbp)
              48 89 55 c8
                                                %rdx,-0x38(%rbp)
400a7a:
                                        mov
400a7e:
              48 8b 45 d0
                                        mov
                                                -0x30(%rbp),%rax
              48 83 c0 02
                                                $0x2,%rax
400a82:
                                        add
              48 ba ab aa aa aa
400a86:
                                        movabs $0xaaaaaaaaaaaaaaab,%rdx
400a8d:
              aa aa aa
              48 f7 e2
                                        mul
                                                %rdx
400a90:
400a93:
              48 89 d0
                                        mov
                                                %rdx,%rax
400a96:
              48 d1 e8
                                        shr
                                                %rax
               48 8d 14 85 00 00 00
                                                0x0(,%rax,4),%rdx
400a99:
                                        lea
400aa0:
               00
               48 8b 45 c8
400aa1:
                                                -0x38(%rbp),%rax
                                        mov
400aa5:
               48 89 10
                                                %rdx,(%rax)
                                        mov
               48 8b 45 c8
                                                -0x38(%rbp),%rax
400aa8:
                                        mov
400aac:
              48 8b 00
                                                (%rax),%rax
                                        mov
400aaf:
                                                $0x1,%esi
              be 01 00 00 00
                                        mov
400ab4:
              48 89 c7
                                        mov
                                                %rax,%rdi
              e8 f4 fc ff ff
400ab7:
                                        callq
                                                4007b0 <calloc@plt>
              48 89 45 f8
                                                %rax,-0x8(%rbp)
400abc:
                                        mov
              48 83 7d f8 00
                                                $0x0,-0x8(%rbp)
400ac0:
                                        cmpq
400ac5:
              75 0a
                                        jne
                                                400ad1 <getlogin_r@plt+0x301>
              b8 00 00 00 00
400ac7:
                                        mov
                                                $0x0,%eax
400acc:
              e9 c0 01 00 00
                                                400c91 <getlogin_r@plt+0x4c1>
                                        jmpq
               c7 45 e0 00 00 00 00
                                                $0x0,-0x20(%rbp)
400ad1:
                                        movl
400ad8:
               c7 45 e4 00 00 00 00
                                        movl
                                                $0x0,-0x1c(%rbp)
              e9 3b 01 00 00
                                                400c1f <getlogin_r@plt+0x44f>
400adf:
                                        jmpq
              8b 45 e0
400ae4:
                                        mov
                                                -0x20(%rbp),%eax
              48 98
400ae7:
                                        cltq
400ae9:
              48 3b 45 d0
                                        cmp
                                                -0x30(%rbp),%rax
              73 1b
                                                400b0a <getlogin_r@plt+0x33a>
400aed:
                                        jae
                                                -0x20(%rbp),%eax
400aef:
              8b 45 e0
                                        mov
               8d 50 01
                                                0x1(%rax),%edx
400af2:
                                        lea
400af5:
              89 55 e0
                                        mov
                                                %edx,-0x20(%rbp)
400af8:
              48 63 d0
                                        movslq %eax,%rdx
400afb:
              48 8b 45 d8
                                        mov
                                                -0x28(%rbp),%rax
400aff:
               48 01 d0
                                        add
                                                %rdx,%rax
400b02:
              0f b6 00
                                        movzbl (%rax),%eax
```

```
400b05:
               0f b6 c0
                                         movzbl %al,%eax
400b08:
               eb 05
                                                400b0f <getlogin r@plt+0x33f>
                                         jmp
              b8 00 00 00 00
400b0a:
                                         mov
                                                $0x0,%eax
                                                %eax,-0x18(%rbp)
              89 45 e8
400b0f:
                                         mov
              8b 45 e0
                                                -0x20(%rbp),%eax
400b12:
                                         mov
              48 98
400b15:
                                         cltq
400b17:
              48 3b 45 d0
                                                -0x30(%rbp),%rax
                                         cmp
              73 1b
400b1b:
                                                400b38 <getlogin_r@plt+0x368>
                                         jae
400b1d:
              8b 45 e0
                                         mov
                                                -0x20(%rbp),%eax
              8d 50 01
400b20:
                                         lea
                                                0x1(%rax),%edx
400b23:
              89 55 e0
                                         mov
                                                %edx,-0x20(%rbp)
              48 63 d0
                                         movslq %eax,%rdx
400b26:
400b29:
              48 8b 45 d8
                                                -0x28(%rbp),%rax
                                         mov
400b2d:
              48 01 d0
                                         add
                                                %rdx,%rax
400b30:
               0f b6 00
                                         movzbl (%rax),%eax
400b33:
              0f b6 c0
                                         movzbl %al,%eax
400b36:
              eb 05
                                         jmp
                                                400b3d <getlogin_r@plt+0x36d>
400b38:
              b8 00 00 00 00
                                                $0x0,%eax
                                        mov
400b3d:
              89 45 ec
                                         mov
                                                %eax,-0x14(%rbp)
              8b 45 e0
400b40:
                                         mov
                                                -0x20(%rbp),%eax
              48 98
400b43:
                                         cltq
              48 3b 45 d0
                                                -0x30(%rbp),%rax
400b45:
                                         cmp
              73 1b
                                                400b66 <getlogin r@plt+0x396>
400b49:
                                         jae
                                                -0x20(%rbp),%eax
400b4b:
              8b 45 e0
                                         mov
              8d 50 01
400b4e:
                                         lea
                                                0x1(%rax),%edx
              89 55 e0
                                                %edx,-0x20(%rbp)
400b51:
                                         mov
400b54:
              48 63 d0
                                         movslq %eax,%rdx
              48 8b 45 d8
400b57:
                                                -0x28(%rbp),%rax
                                         mov
400b5b:
              48 01 d0
                                                %rdx,%rax
                                         add
              0f b6 00
                                         movzbl (%rax),%eax
400b5e:
400b61:
              0f b6 c0
                                         movzbl %al,%eax
400b64:
              eb 05
                                                400b6b <getlogin_r@plt+0x39b>
                                         jmp
400b66:
              b8 00 00 00 00
                                                $0x0,%eax
                                         mov
400b6b:
              89 45 f0
                                                %eax,-0x10(%rbp)
                                         mov
400b6e:
              8b 45 e8
                                                -0x18(%rbp),%eax
                                         mov
400b71:
               c1 e0 10
                                         shl
                                                $0x10,%eax
400b74:
              89 c2
                                         mov
                                                %eax,%edx
              8b 45 ec
400b76:
                                                -0x14(%rbp),%eax
                                         mov
              c1 e0 08
400b79:
                                         shl
                                                $0x8,%eax
               01 c2
                                                %eax,%edx
400b7c:
                                         add
400b7e:
              8b 45 f0
                                         mov
                                                -0x10(%rbp),%eax
400b81:
               01 d0
                                         add
                                                %edx,%eax
400b83:
              89 45 f4
                                        mov
                                                %eax,-0xc(%rbp)
              8b 45 e4
400b86:
                                        mov
                                                -0x1c(%rbp),%eax
400b89:
              8d 50 01
                                         lea
                                                0x1(%rax),%edx
              89 55 e4
                                                %edx,-0x1c(%rbp)
400b8c:
                                         mov
400b8f:
              48 63 d0
                                         movslq %eax,%rdx
              48 8b 45 f8
                                                -0x8(%rbp),%rax
400b92:
                                         mov
                                                %rax,%rdx
400b96:
              48 01 c2
                                         add
              8b 45 f4
400b99:
                                         mov
                                                -0xc(%rbp),%eax
400b9c:
               c1 e8 12
                                         shr
                                                $0x12,%eax
                                                $0x3f,%eax
400b9f:
               83 e0 3f
                                         and
400ba2:
              89 c0
                                         mov
                                                %eax,%eax
```

```
400ba4:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400bab:
               88 02
                                                %al,(%rdx)
                                         mov
               8b 45 e4
400bad:
                                         mov
                                                -0x1c(%rbp),%eax
               8d 50 01
400bb0:
                                                0x1(%rax),%edx
                                         lea
400bb3:
               89 55 e4
                                                %edx,-0x1c(%rbp)
                                         mov
               48 63 d0
                                         movslq %eax,%rdx
400bb6:
               48 8b 45 f8
                                                -0x8(%rbp),%rax
400bb9:
                                         mov
400bbd:
               48 01 c2
                                                %rax,%rdx
                                         add
400bc0:
               8b 45 f4
                                                -0xc(%rbp),%eax
                                         mov
                                         shr
400bc3:
               c1 e8 0c
                                                $0xc,%eax
400bc6:
               83 e0 3f
                                         and
                                                $0x3f,%eax
               89 c0
400bc9:
                                                %eax,%eax
                                         mov
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400bcb:
               88 02
                                                %al,(%rdx)
400bd2:
                                         mov
400bd4:
               8b 45 e4
                                                -0x1c(%rbp),%eax
                                         mov
400bd7:
               8d 50 01
                                         lea
                                                0x1(%rax),%edx
400bda:
               89 55 e4
                                                %edx,-0x1c(%rbp)
                                         mov
400bdd:
               48 63 d0
                                         movslq %eax,%rdx
400be0:
               48 8b 45 f8
                                                -0x8(%rbp),%rax
                                         mov
400be4:
               48 01 c2
                                         add
                                                %rax,%rdx
               8b 45 f4
400be7:
                                         mov
                                                -0xc(%rbp),%eax
400bea:
               c1 e8 06
                                         shr
                                                $0x6,%eax
               83 e0 3f
                                                $0x3f,%eax
400bed:
                                         and
400bf0:
               89 c0
                                         mov
                                                %eax,%eax
400bf2:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
               88 02
400bf9:
                                                %al,(%rdx)
                                         mov
400bfb:
               8b 45 e4
                                                -0x1c(%rbp),%eax
                                         mov
               8d 50 01
                                                0x1(%rax),%edx
400bfe:
                                         lea
400c01:
               89 55 e4
                                                %edx,-0x1c(%rbp)
                                         mov
               48 63 d0
                                         movslq %eax,%rdx
400c04:
400c07:
               48 8b 45 f8
                                                -0x8(%rbp),%rax
                                         mov
400c0b:
               48 01 c2
                                         add
                                                %rax,%rdx
                                                -0xc(%rbp),%eax
400c0e:
               8b 45 f4
                                         mov
               83 e0 3f
400c11:
                                         and
                                                $0x3f,%eax
400c14:
               89 c0
                                         mov
                                                %eax,%eax
400c16:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400c1d:
               88 02
                                         mov
                                                %al,(%rdx)
               8b 45 e0
400c1f:
                                                -0x20(%rbp),%eax
                                         mov
400c22:
               48 98
                                         cltq
               48 3b 45 d0
400c24:
                                         cmp
                                                -0x30(%rbp),%rax
400c28:
               Of 82 b6 fe ff ff
                                         jЬ
                                                400ae4 <getlogin_r@plt+0x314>
400c2e:
               c7 45 e0 00 00 00 00
                                                $0x0,-0x20(%rbp)
                                         movl
400c35:
               eb 24
                                         jmp
                                                400c5b <getlogin_r@plt+0x48b>
400c37:
               48 8b 45 c8
                                                -0x38(%rbp),%rax
                                         mov
400c3b:
               48 8b 10
                                         mov
                                                (%rax),%rdx
               8b 45 e0
400c3e:
                                         mov
                                                -0x20(%rbp),%eax
400c41:
               48 98
                                         cltq
               48 29 c2
400c43:
                                         sub
                                                %rax,%rdx
                                                %rdx,%rax
400c46:
               48 89 d0
                                         mov
                                                -0x1(%rax),%rdx
400c49:
               48 8d 50 ff
                                         lea
400c4d:
               48 8b 45 f8
                                         mov
                                                -0x8(%rbp),%rax
               48 01 d0
                                         add
                                                %rdx,%rax
400c51:
400c54:
               c6 00 3d
                                         movb
                                                $0x3d,(%rax)
```

```
400c57:
                 83 45 e0 01
                                                  $0x1,-0x20(%rbp)
                                           addl
                 48 8b 4d d0
                                                  -0x30(%rbp), %rcx
  400c5b:
                                           mov
                 48 ba ab aa aa aa
  400c5f:
                                          movabs $0xaaaaaaaaaaaaaab,%rdx
  400c66:
                 aa aa aa
                 48 89 c8
  400c69:
                                                  %rcx,%rax
                                           mov
                 48 f7 e2
                                                  %rdx
  400c6c:
                                           mul
  400c6f:
                 48 d1 ea
                                                  %rdx
                                           shr
                 48 89 d0
  400c72:
                                                  %rdx,%rax
                                           mov
  400c75:
                 48 01 c0
                                           add
                                                  %rax,%rax
                 48 01 d0
                                                  %rdx,%rax
  400c78:
                                           add
  400c7b:
                 48 29 c1
                                           sub
                                                  %rax,%rcx
  400c7e:
                 48 89 ca
                                                  %rcx,%rdx
                                           mov
  400c81:
                 8b 04 95 00 21 60 00
                                           mov
                                                  0x602100(,%rdx,4),%eax
  400c88:
                 3b 45 e0
                                                  -0x20(%rbp),%eax
                                           cmp
  400c8b:
                 7f aa
                                                  400c37 <getlogin_r@plt+0x467>
                                           jg
  400c8d:
                 48 8b 45 f8
                                           mov
                                                  -0x8(%rbp),%rax
  400c91:
                 c9
                                           leaveq
  400c92:
                 с3
                                           retq
  400c93:
                 66 2e 0f 1f 84 00 00
                                           nopw
                                                  %cs:0x0(%rax,%rax,1)
                 00 00 00
  400c9a:
                 0f 1f 00
                                                  (%rax)
  400c9d:
                                           nopl
                41 57
                                                  %r15
  400ca0:
                                           push
                 41 89 ff
                                                  %edi,%r15d
  400ca2:
                                           mov
  400ca5:
                41 56
                                           push
                                                  %r14
  400ca7:
                49 89 f6
                                                  %rsi,%r14
                                           mov
                41 55
                                                  %r13
  400caa:
                                           push
  400cac:
                 49 89 d5
                                          mov
                                                  %rdx,%r13
                 41 54
  400caf:
                                           push
                                                  %r12
                 4c 8d 25 48 11 20 00
  400cb1:
                                           lea
                                                  0x201148(%rip),%r12
                                                                               # 601e0
0 <_fini+0x2010ec>
  400cb8:
                 55
                                           push
                                                  %rbp
  400cb9:
                 48 8d 2d 48 11 20 00
                                           lea
                                                  0x201148(%rip),%rbp
                                                                               # 601e0
8 <_fini+0x2010f4>
  400cc0:
                 53
                                                  %rbx
                                           push
                 4c 29 e5
  400cc1:
                                           sub
                                                  %r12,%rbp
  400cc4:
                31 db
                                                  %ebx,%ebx
                                           xor
  400cc6:
                48 c1 fd 03
                                           sar
                                                  $0x3,%rbp
                 48 83 ec 08
  400cca:
                                           sub
                                                  $0x8,%rsp
  400cce:
                e8 35 fa ff ff
                                           callq
                                                  400708 <_init>
                 48 85 ed
                                                  %rbp,%rbp
  400cd3:
                                           test
                                                  400cf6 <getlogin_r@plt+0x526>
  400cd6:
                 74 1e
                                           jе
                 Of 1f 84 00 00 00 00
                                                  0x0(%rax,%rax,1)
  400cd8:
                                           nopl
  400cdf:
                 00
  400ce0:
                 4c 89 ea
                                           mov
                                                  %r13,%rdx
  400ce3:
                 4c 89 f6
                                           mov
                                                  %r14,%rsi
                                                  %r15d,%edi
                 44 89 ff
  400ce6:
                                           mov
  400ce9:
                 41 ff 14 dc
                                           callq
                                                  *(%r12,%rbx,8)
                 48 83 c3 01
                                                  $0x1,%rbx
  400ced:
                                           add
                 48 39 eb
  400cf1:
                                           cmp
                                                  %rbp,%rbx
                 75 ea
  400cf4:
                                           jne
                                                  400ce0 <getlogin_r@plt+0x510>
                 48 83 c4 08
  400cf6:
                                           add
                                                  $0x8,%rsp
                 5b
  400cfa:
                                                  %rbx
                                           pop
  400cfb:
                 5d
                                           pop
                                                  %rbp
```

```
400cfc:
                41 5c
                                                %r12
                                         pop
  400cfe:
                41 5d
                                                %r13
                                         pop
                41 5e
  400d00:
                                         pop
                                                %r14
                41 5f
                                                %r15
  400d02:
                                         pop
                с3
  400d04:
                                         reta
  400d05:
                66 66 2e 0f 1f 84 00
                                         data32 nopw %cs:0x0(%rax,%rax,1)
  400d0c:
                00 00 00 00
  400d10:
                f3 c3
                                         repz retq
Disassembly of section .fini:
0000000000400d14 < fini>:
  400d14:
                48 83 ec 08
                                         sub
                                                $0x8,%rsp
  400d18:
                48 83 c4 08
                                         add
                                                $0x8,%rsp
  400d1c:
                c3
                                         reta
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s 4
Symbol table '.dynsym' contains 19 entries:
   Num:
                                                        Ndx Name
           Value
                           Size Type
                                        Bind
                                               Vis
     0: 0000000000000000
                              0 NOTYPE
                                        LOCAL
                                               DEFAULT
                                                        UND
                              0 NOTYPE
     1: 00000000000000000
                                        WEAK
                                               DEFAULT
                                                        UND _ITM_deregisterTMClone
Tab
                              0 FUNC
                                        GLOBAL DEFAULT
                                                        UND puts@GLIBC_2.2.5 (2)
     2: 0000000000000000
                              0 FUNC
                                        GLOBAL DEFAULT
     3: 0000000000000000
                                                        UND secretoperation
                                                        UND strlen@GLIBC 2.2.5 (2)
     4: 0000000000000000
                              0 FUNC
                                        GLOBAL DEFAULT
     5: 00000000000000000
                              0 FUNC
                                        GLOBAL DEFAULT
                                                        UND __stack_chk_fail@GLIBC
2.4 (3)
     6: 0000000000000000
                              0 FUNC
                                        GLOBAL DEFAULT
                                                        UND printf@GLIBC_2.2.5 (2)
     7: 00000000000000000
                              0 FUNC
                                        GLOBAL DEFAULT
                                                        UND __assert_fail@GLIBC_2.
2.5 (2)
     8: 0000000000000000
                              0 FUNC
                                        GLOBAL DEFAULT
                                                        UND __libc_start_main@GLIB
C 2.2.5 (2)
     9: 0000000000000000
                              0 FUNC
                                        GLOBAL DEFAULT
                                                        UND calloc@GLIBC 2.2.5 (2)
                              0 NOTYPE
    10: 0000000000000000
                                        WEAK
                                               DEFAULT
                                                        UND __gmon_start__
                              0 FUNC
                                                        UND getlogin r@GLIBC 2.2.5
    11: 0000000000000000
                                        GLOBAL DEFAULT
 (2)
    12: 00000000000000000
                              0 NOTYPE
                                        WEAK
                                               DEFAULT
                                                        UND Jv RegisterClasses
    13: 0000000000000000
                              0 NOTYPE
                                        WEAK
                                               DEFAULT
                                                        UND _ITM_registerTMCloneTa
ble
                              0 NOTYPE
                                        GLOBAL DEFAULT
    14: 000000000060210c
                                                         24 edata
                                                         25 _end
                              0 NOTYPE
    15: 0000000000602110
                                        GLOBAL DEFAULT
                              0 NOTYPE
                                                         25 __bss_start
    16: 000000000060210c
                                        GLOBAL DEFAULT
                              0 FUNC
                                        GLOBAL DEFAULT
                                                         11 _init
    17: 0000000000400708
    18: 0000000000400d14
                              0 FUNC
                                        GLOBAL DEFAULT
                                                         14 fini
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ qcc -c -fPIC hello.c -o hello.o
gcc: error: hello.c: No such file or directory
qcc: fatal error: no input files
compilation terminated.
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -c -fPIC lib361.c -o lib361.o
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
  1 2 3 4 howto.txt iamspecial lib361.c lib361.o lib361.so secrets.txt
```

```
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf lib361.so
Usage: readelf <option(s)> elf-file(s)
 Display information about the contents of ELF format files
 Options are:
  -a --all
                         Equivalent to: -h -l -S -s -r -d -V -A -I
  -h --file-header
                         Display the ELF file header
  -l --program-headers
                         Display the program headers
                         An alias for --program-headers
     --segments
  -S --section-headers
                         Display the sections' header
                         An alias for --section-headers
     --sections
  -g --section-groups
                         Display the section groups
  -t --section-details
                         Display the section details
  -e --headers
                         Equivalent to: -h -l -S
  -s --syms
                         Display the symbol table
                         An alias for --syms
     --symbols
                         Display the dynamic symbol table
  --dyn-syms
                         Display the core notes (if present)
  -n --notes
  -r --relocs
                         Display the relocations (if present)
                         Display the unwind info (if present)
  -u --unwind
  -d --dynamic
                         Display the dynamic section (if present)
  -V --version-info
                         Display the version sections (if present)
  -A --arch-specific
                         Display architecture specific information (if any)
  -c --archive-index
                         Display the symbol/file index in an archive
  -D --use-dynamic
                         Use the dynamic section info when displaying symbols
  -x --hex-dump=<number|name>
                         Dump the contents of section <number|name> as bytes
  -p --string-dump=<number|name>
                         Dump the contents of section <number|name> as strings
  -R --relocated-dump=<number|name>
                         Dump the contents of section <number|name> as relocated
bytes
  -w[lLiaprmfFsoRt] or
  --debug-dump[=rawline,=decodedline,=info,=abbrev,=pubnames,=aranges,=macro,=fra
mes,
               =frames-interp,=str,=loc,=Ranges,=pubtypes,
               =qdb index,=trace info,=trace abbrev,=trace aranges,
               =addr,=cu_index]
                         Display the contents of DWARF2 debug sections
  --dwarf-depth=N
                         Do not display DIEs at depth N or greater
  --dwarf-start=N
                         Display DIEs starting with N, at the same depth
                         or deeper
  -I --histogram
                         Display histogram of bucket list lengths
  −W −−wide
                         Allow output width to exceed 80 characters
  @<file>
                         Read options from <file>
  -H --help
                         Display this information
                         Display the version number of readelf
  -v --version
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s lib361.so
Symbol table '.dynsym' contains 31 entries:
   Num:
           Value
                          Size Type
                                       Bind
                                              Vis
                                                        Ndx Name
     0: 0000000000000000
                             0 NOTYPE LOCAL DEFAULT UND
                             0 SECTION LOCAL
     1: 00000000000000a10
                                              DEFAULT
                             0 NOTYPE WEAK
     2: 00000000000000000
                                              DEFAULT UND _ITM_deregisterTMClone
```

```
Tab
     3: 00000000000000000
                              0 NOTYPE
                                         WEAK
                                                DEFAULT
                                                          UND __gmon_start__
                               0 NOTYPE
     4: 0000000000000000
                                         WEAK
                                                DEFAULT
                                                          UND _Jv_RegisterClasses
                              0 NOTYPE
                                                          UND _ITM_registerTMCloneTa
     5: 00000000000000000
                                         WEAK
                                                DEFAULT
ble
                              0 FUNC
     6: 0000000000000000
                                         WEAK
                                                DEFAULT
                                                          UND __cxa_finalize@GLIBC_2
.2.5 (2)
                              0 NOTYPE
                                         GLOBAL DEFAULT
                                                           24 _edata
     7: 000000000020214c
     8: 0000000000202158
                              0 NOTYPE
                                         GLOBAL DEFAULT
                                                           25 _end
                                         GLOBAL DEFAULT
                                                           25 __bss_start
     9: 000000000020214c
                              0 NOTYPE
    10: 00000000000000a10
                              0 FUNC
                                         GLOBAL DEFAULT
                                                            9 _init
                              0 FUNC
                                                           12 _fini
    11: 0000000000001154
                                         GLOBAL DEFAULT
    12: 00000000000000000
                              0 NOTYPE
                                         LOCAL
                                                DEFAULT
                                                          UND
    13: 0000000000000000
                              0 NOTYPE
                                         WEAK
                                                          UND rt_
                                                DEFAULT
    14: 0000000000000000
                              0 FUNC
                                         GLOBAL DEFAULT
                                                          UND s start@GLIBC 2.2.5 (2
)
    15: 0000000000000000
                              0 FUNC
                                         GLOBAL DEFAULT
                                                          UND terClasses
    16: 00000000000000000
                                FUNC
                                         GLOBAL DEFAULT
                                                          UND rTMCloneTable@GLIBC_2.
2.5 (2)
                              0 FUNC
    17: 0000000000000000
                                         GLOBAL DEFAULT
                                                          UND rtreadelf: Error: bad
dynamic symbol
                              0 FUNC
                                                          UND ITM deregisterTMClone
    18: 00000000000000000
                                         GLOBAL DEFAULT
Tab@GLIBC 2.2.5 (2)
                                                          UND .5@GLIBC_2.2.5 (2)
    19: 0000000000000000
                              0 FUNC
                                         GLOBAL DEFAULT
                                         GLOBAL DEFAULT
    20: 00000000000000000
                              0 FUNC
                                                          UND on start @GLIBC 2.2.5
 (2)
    21: 00000000000000000
                              0 FUNC
                                         GLOBAL DEFAULT
                                                          UND registerTMCloneTable@G
LIBC 2.2.5 (2)
    22: 0000000000000000
                              0 NOTYPE
                                         WEAK
                                                          UND sterTMCloneTable
                                                DEFAULT
                              0 FUNC
    23: 00000000000000000
                                         GLOBAL DEFAULT
                                                          UND eTable@GLIBC_2.2.5 (2)
    24: 0000000000000000
                              0 NOTYPE
                                         WEAK
                                                DEFAULT
                                                          UND e
                                                          UND neTable
    25: 00000000000000000
                              0 NOTYPE
                                         WEAK
                                                DEFAULT
    26: 000000000060210c
                              0 NOTYPE
                                         GLOBAL DEFAULT
                                                           24 isterClasses
    27: 0000000000602110
                              0 NOTYPE
                                         GLOBAL DEFAULT
                                                           25 egisterTMCloneTable
    28: 000000000060210c
                              0 NOTYPE
                                         GLOBAL DEFAULT
                                                           25 asses
    29: 0000000000400708
                              0 FUNC
                                         GLOBAL DEFAULT
                                                           11 _RegisterClasses
    30: 0000000000400d14
                              0 FUNC
                                         GLOBAL DEFAULT
                                                           14 so.6
Symbol table '.symtab' contains 54 entries:
   Num:
           Value
                           Size Type
                                         Bind
                                                Vis
                                                          Ndx Name
     0: 00000000000000000
                              0 NOTYPE
                                         LOCAL
                                                DEFAULT
                                                          UND
     1: 00000000000000238
                               0 SECTION LOCAL
                                                DEFAULT
                                                            1
                                                            2
     2: 00000000000000280
                              0 SECTION LOCAL
                                                DEFAULT
     3: 00000000000002f0
                               0 SECTION LOCAL
                                                DEFAULT
                                                            3
                              0 SECTION LOCAL
     4: 00000000000005d8
                                                DEFAULT
                                                            4
     5: 0000000000000078a
                               0 SECTION LOCAL
                                                DEFAULT
                                                            5
                              0 SECTION LOCAL
                                                            6
     6: 00000000000007c8
                                                DEFAULT
     7: 00000000000000818
                              0 SECTION LOCAL
                                                DEFAULT
                                                            7
                              0 SECTION LOCAL
     8: 00000000000008f0
                                                DEFAULT
                                                            8
                                                            9
     9: 00000000000000a10
                              0 SECTION LOCAL
                                                DEFAULT
                              0 SECTION LOCAL
                                                           10
    10: 00000000000000a50
                                                DEFAULT
    11: 0000000000000b30
                              0 SECTION LOCAL
                                                DEFAULT
                                                           11
```

```
12: 0000000000001154
                              0 SECTION LOCAL
                                               DEFAULT
                                                          12
                              0 SECTION LOCAL
                                                          13
    13: 0000000000001168
                                               DEFAULT
                              0 SECTION LOCAL
                                                          14
    14: 0000000000001227
                                               DEFAULT
                              0 SECTION LOCAL
                                                          15
    15: 0000000000001244
                                               DEFAULT
    16: 0000000000001264
                              0 SECTION LOCAL
                                                          16
                                               DEFAULT
    17: 00000000000012a8
                              0 SECTION LOCAL
                                               DEFAULT
                                                          17
    18: 0000000000201c00
                              0 SECTION LOCAL
                                               DEFAULT
                                                          18
                              0 SECTION LOCAL
                                                          19
    19: 0000000000201c10
                                               DEFAULT
    20: 0000000000201c20
                              0 SECTION LOCAL
                                               DEFAULT
                                                          20
    21: 0000000000201c30
                              0 SECTION LOCAL
                                                          21
                                               DEFAULT
    22: 0000000000201fd0
                              0 SECTION LOCAL
                                               DEFAULT
                                                          22
    23: 0000000000202000
                              0 SECTION LOCAL
                                               DEFAULT
                                                          23
    24: 00000000002020a0
                              0 SECTION LOCAL
                                               DEFAULT
                                                          24
                                               DEFAULT
    25: 000000000020214c
                              0 SECTION LOCAL
                                                          25
    26: 0000000000000000
                              0 SECTION LOCAL
                                               DEFAULT
                                                          26
    27: 00000000000000000
                              0 FILE
                                        LOCAL
                                               DEFAULT
                                                         ABS crtstuff.c
    28: 0000000000201c20
                              0 OBJECT
                                        L0CAL
                                               DEFAULT
                                                          20 __JCR_LIST__
                              0 FUNC
                                        L0CAL
                                                          11 deregister_tm_clones
    29: 0000000000000b30
                                               DEFAULT
                                                          11 register_tm_clones
    30: 0000000000000b60
                              0 FUNC
                                        LOCAL
                                               DEFAULT
                                                          11 __do_global_dtors_aux
    31: 0000000000000ba0
                              0 FUNC
                                        L0CAL
                                               DEFAULT
    32: 000000000020214c
                              1 OBJECT
                                        LOCAL
                                               DEFAULT
                                                          25 completed.6973
    33: 0000000000201c10
                              0 OBJECT
                                        L0CAL
                                                          19 __do_global_dtors_aux_
                                               DEFAULT
fin
    34: 0000000000000be0
                              0 FUNC
                                        L0CAL
                                               DEFAULT
                                                          11 frame_dummy
    35: 0000000000201c00
                              0 OBJECT
                                        L0CAL
                                               DEFAULT
                                                          18 __frame_dummy_init_arr
ay_
    36: 00000000000000000
                              0 FILE
                                        L0CAL
                                               DEFAULT
                                                         ABS crtstuff.c
                              0 OBJECT
                                        L0CAL
                                                          17 FRAME END
    37: 0000000000001424
                                               DEFAULT
                                                          20 __JCR_END
    38: 0000000000201c28
                              0 OBJECT
                                        L0CAL
                                               DEFAULT
    39: 0000000000000000
                              0 FILE
                                        L0CAL
                                                         ABS
                                               DEFAULT
    40: 00000000002020a0
                              0 OBJECT
                                        LOCAL
                                               DEFAULT
                                                          24 __dso_handle
    41: 0000000000201c30
                              0 OBJECT
                                        L0CAL
                                               DEFAULT
                                                          21 DYNAMIC
    42: 0000000000202150
                              0 OBJECT
                                        LOCAL
                                               DEFAULT
                                                          24 TMC END
                              0 OBJECT
                                                          23 GLOBAL OFFSET TABLE
    43: 0000000000202000
                                        L0CAL
                                               DEFAULT
                                                         UND _ITM_deregisterTMClone
    44: 00000000000000000
                              0 NOTYPE
                                        WEAK
                                               DEFAULT
Tab
    45: 000000000020214c
                              0 NOTYPE
                                        GLOBAL DEFAULT
                                                          24 _edata
    46: 0000000000001154
                              0 FUNC
                                        GLOBAL DEFAULT
                                                          12 _fini
    47: 00000000000000000
                              0 NOTYPE
                                        WEAK
                                               DEFAULT
                                                         UND __gmon_start__
    48: 0000000000202158
                              0 NOTYPE
                                        GLOBAL DEFAULT
                                                          25 _end
    49: 000000000020214c
                              0 NOTYPE
                                        GLOBAL DEFAULT
                                                          25 __bss_start
                              0 NOTYPE
                                                         UND _Jv_RegisterClasses
    50: 0000000000000000
                                        WEAK
                                               DEFAULT
                                                         UND _ITM_registerTMCloneTa
    51: 0000000000000000
                              0 NOTYPE
                                        WEAK
                                               DEFAULT
ble
    52: 0000000000000000
                              0 FUNC
                                        WEAK
                                               DEFAULT
                                                         UND __cxa_finalize@@GLIBC_
2.2
    53: 00000000000000a10
                              0 FUNC
                                        GLOBAL DEFAULT
                                                           9 init
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
  1 2 3 4 howto.txt
                          iamspecial
                                       lib361.c lib361.o lib361.so
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ rm lib361.o lib361.so
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
   1 2 3 4 howto.txt iamspecial
                                      lib361.c secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o libhello.so -fPIC hello.c
```

```
gcc: fatal error: no input files
compilation terminated.
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ qcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s lib361.so
Symbol table '.dynsym' contains 13 entries:
   Num:
           Value
                           Size Type
                                                Vis
                                                          Ndx Name
     0: 0000000000000000
                              0 NOTYPE
                                         L0CAL
                                                DEFAULT
                                                          UND
     1: 0000000000000548
                              0 SECTION LOCAL
                                                DEFAULT
        00000000000000000
                              0 NOTYPE
                                         WEAK
                                                DEFAULT
                                                          UND _ITM_deregisterTMClone
Tab
     3: 00000000000000000
                              0 NOTYPE
                                         WEAK
                                                DEFAULT
                                                          UND __gmon_start__
     4: 00000000000000000
                              0 NOTYPE
                                         WEAK
                                                          UND _Jv_RegisterClasses
                                                DEFAULT
     5: 00000000000000000
                              0 NOTYPE
                                         WEAK
                                                DEFAULT
                                                          UND ITM registerTMCloneTa
ble
     6: 00000000000000000
                              0 FUNC
                                         WEAK
                                                DEFAULT
                                                          UND __cxa_finalize@GLIBC_2
.2.5(2)
     7: 0000000000201030
                              0 NOTYPE
                                         GLOBAL DEFAULT
                                                           21 _edata
     8: 0000000000201038
                              0 NOTYPE
                                         GLOBAL DEFAULT
                                                           22 _end
                                                           22 __bss_start
     9: 0000000000201030
                              0 NOTYPE
                                         GLOBAL DEFAULT
    10: 0000000000000548
                              0 FUNC
                                         GLOBAL DEFAULT
                                                            9 _init
                              6 FUNC
                                         GLOBAL DEFAULT
                                                           11 secretoperation
    11: 00000000000000685
    12: 000000000000068c
                              0 FUNC
                                         GLOBAL DEFAULT
                                                           12 _fini
Symbol table '.symtab' contains 53 entries:
   Num:
           Value
                           Size Type
                                         Bind
                                                Vis
                                                          Ndx Name
     0: 0000000000000000
                              0 NOTYPE
                                        LOCAL
                                                DEFAULT
                                                          UND
     1: 00000000000001c8
                              0 SECTION LOCAL
                                                DEFAULT
                                                            1
                                                            2
     2: 0000000000001f0
                              0 SECTION LOCAL
                                                DEFAULT
     3: 00000000000000230
                              0 SECTION LOCAL
                                                DEFAULT
                                                            3
     4: 0000000000000368
                              0 SECTION LOCAL
                                                DEFAULT
                                                            4
     5: 000000000000041c
                              0 SECTION LOCAL
                                                DEFAULT
                                                            5
     6: 0000000000000438
                              0 SECTION LOCAL
                                                DEFAULT
                                                            6
     7: 0000000000000458
                              0 SECTION LOCAL
                                                DEFAULT
                                                            7
     8: 0000000000000518
                              0 SECTION LOCAL
                                                DEFAULT
                                                            8
     9: 0000000000000548
                              0 SECTION LOCAL
                                                DEFAULT
                                                            9
    10: 000000000000570
                              0 SECTION LOCAL
                                                DEFAULT
                                                           10
    11: 00000000000005a0
                              0 SECTION LOCAL
                                                DEFAULT
                                                           11
    12: 0000000000000068c
                              0 SECTION LOCAL
                                                DEFAULT
                                                           12
    13: 0000000000000698
                              0 SECTION LOCAL
                                                DEFAULT
                                                           13
    14: 00000000000006b8
                              0 SECTION LOCAL
                                                DEFAULT
                                                           14
    15: 0000000000200e00
                              0 SECTION LOCAL
                                                DEFAULT
                                                           15
    16: 0000000000200e08
                              0 SECTION LOCAL
                                                DEFAULT
                                                           16
    17: 0000000000200e10
                              0 SECTION LOCAL
                                                DEFAULT
                                                           17
    18: 0000000000200e18
                              0 SECTION LOCAL
                                                DEFAULT
                                                           18
    19: 0000000000200fd8
                              0 SECTION LOCAL
                                                DEFAULT
                                                           19
    20: 0000000000201000
                              0 SECTION LOCAL
                                                DEFAULT
                                                           20
    21: 0000000000201028
                              0 SECTION LOCAL
                                                DEFAULT
                                                           21
    22: 0000000000201030
                              0 SECTION LOCAL
                                                DEFAULT
                                                           22
    23: 00000000000000000
                              0 SECTION LOCAL
                                                DEFAULT
                                                           23
                              0 FILE
                                         L0CAL
                                                          ABS crtstuff.c
    24: 00000000000000000
                                                DEFAULT
    25: 0000000000200e10
                              0 OBJECT
                                         L0CAL
                                                DEFAULT
                                                           17 __JCR_LIST__
```

gcc: error: hello.c: No such file or directory

```
26: 00000000000005a0
                             0 FUNC
                                       L0CAL
                                              DEFAULT
                                                         11 deregister_tm_clones
    27: 00000000000005d0
                             0 FUNC
                                       LOCAL
                                                         11 register_tm_clones
                                              DEFAULT
                             0 FUNC
                                       LOCAL
                                                         11 __do_global_dtors_aux
    28: 0000000000000610
                                              DEFAULT
    29: 000000000201030
                             1 OBJECT
                                       LOCAL
                                                         22 completed.6973
                                              DEFAULT
    30: 0000000000200e08
                             0 OBJECT
                                       LOCAL
                                              DEFAULT
                                                         16 __do_global_dtors_aux_
fin
    31: 0000000000000650
                             0 FUNC
                                       L0CAL
                                              DEFAULT
                                                         11 frame dummy
    32: 0000000000200e00
                             0 OBJECT
                                                         15 __frame_dummy_init_arr
                                       L0CAL
                                              DEFAULT
ay_
    33: 00000000000000000
                             0 FILE
                                       LOCAL
                                              DEFAULT
                                                        ABS lib361.c
    34: 0000000000000000
                             0 FILE
                                       LOCAL
                                              DEFAULT
                                                        ABS crtstuff.c
    35: 0000000000000718
                             0 OBJECT
                                       LOCAL
                                              DEFAULT
                                                         14 ___FRAME_END__
                             0 OBJECT
    36: 0000000000200e10
                                       LOCAL
                                              DEFAULT
                                                         17 __JCR_END__
    37: 00000000000000000
                             0 FILE
                                       LOCAL DEFAULT
                                                        ABS
    38: 0000000000201028
                             0 OBJECT
                                       LOCAL DEFAULT
                                                         21 __dso_handle
                                                         18 _DYNAMIC
                             0 OBJECT
    39: 0000000000200e18
                                       LOCAL DEFAULT
    40: 0000000000201030
                             0 OBJECT
                                       LOCAL
                                              DEFAULT
                                                         21 __TMC_END_
                             0 OBJECT
                                                         20 _GLOBAL_OFFSET_TABLE_
    41: 0000000000201000
                                       LOCAL
                                              DEFAULT
    42: 0000000000000000
                             0 NOTYPE
                                       WEAK
                                              DEFAULT
                                                        UND ITM deregisterTMClone
Tab
    43: 0000000000201030
                             0 NOTYPE
                                       GLOBAL DEFAULT
                                                         21 edata
    44: 0000000000000685
                             6 FUNC
                                       GLOBAL DEFAULT
                                                         11 secretoperation
    45: 000000000000068c
                             0 FUNC
                                       GLOBAL DEFAULT
                                                         12 _fini
                             0 NOTYPE
                                       WEAK
                                                        UND __gmon_start__
    46: 0000000000000000
                                              DEFAULT
                             0 NOTYPE
                                       GLOBAL DEFAULT
                                                         22 _end
    47: 0000000000201038
                                                         22 __bss_start
    48: 0000000000201030
                             0 NOTYPE
                                       GLOBAL DEFAULT
                                                        UND _Jv_RegisterClasses
    49: 0000000000000000
                             0 NOTYPE
                                       WEAK
                                              DEFAULT
                             0 NOTYPE
                                                        UND ITM registerTMCloneTa
    50: 0000000000000000
                                       WEAK
                                              DEFAULT
ble
                             0 FUNC
                                       WEAK
                                                        UND __cxa_finalize@@GLIBC_
    51: 0000000000000000
                                               DEFAULT
2.2
    52: 0000000000000548
                             0 FUNC
                                       GLOBAL DEFAULT
                                                          9 init
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
   1 2 3 4 howto.txt iamspecial lib361.c lib361.so secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ strings 4
/lib64/ld-linux-x86-64.so.2
lib361.so
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
ITM registerTMCloneTable
```

```
_{
m init}
secretoperation
_fini
libc.so.6
puts
__stack_chk_fail
__assert_fail
printf
calloc
strlen
getlogin_r
__libc_start_main
_edata
__bss_start
_end
GLIBC_2.4
GLIBC_2.2.5
dH34%(
[]A\A]A^A_
34567890123456789012
%5%5
you win! the secret is:
bangarang
this program tests the implementation of a dynamically linked library.
get_sum.c
result == 10
result == 4
main
;*3$"
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
GCC: (Ubuntu 4.8.4-2ubuntu1~14.04) 4.8.4
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
```

```
•got
.got.plt
.data
.bss
.comment
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
   1 2 3 4 howto.txt iamspecial lib361.c lib361.so secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
lib361.c: In function 'secretoperation':
lib361.c:3:35: error: expected ';' before '}' token
 int secretoperation() { return 10 }
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ strace ./4
execve("./4", ["./4"], [/* 20 vars */]) = 0
                                        = 0 \times 1897000
access("/etc/ld.so.nohwcap", F OK) = -1 ENOENT (No such file or directory)
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f76
f1a6c000
access("/etc/ld.so.preload", R OK) = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", 0_RDONLY|0_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=25058, ...}) = 0
mmap(NULL, 25058, PROT\_READ, MAP\_PRIVATE, 3, 0) = 0x7f76f1a65000
                                        = −1 ENOENT (No such file or directory)
access("/etc/ld.so.nohwcap", F_OK)
open("/lib/x86_64-linux-gnu/tls/x86_64/lib361.so", 0_{RDONLY}0_CL0EXEC) = -1 ENOEN
T (No such file or directory)
stat("/lib/x86~64-linux-qnu/tls/x86~64", 0x7fffd5ddb150) = -1 EN0ENT (No such fil
e or directory)
open("/lib/x86~64-linux-qnu/tls/lib361.so", O RDONLY|O CLOEXEC) = -1 ENOENT (No s
uch file or directory)
stat("/lib/x86 64-linux-qnu/tls", 0x7fffd5ddb150) = -1 EN0ENT (No such file or di
```

```
rectory)
open("/lib/x86~64-linux-qnu/x86~64/lib361.so", O RDONLY|O CLOEXEC) = -1 ENOENT (N
o such file or directory)
stat("/lib/x86~64-linux-qnu/x86~64", 0x7fffd5ddb150) = -1~ENOENT~(No~such~file~or~
 directory)
open("/lib/x86_64-linux-gnu/lib361.so", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\5\0\0\0\0\0\0\0"..., 83
2) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=7868, ...}) = 0
mmap(NULL, 2101304, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f7
6f164a000
mprotect(0x7f76f164b000, 2093056, PROT NONE) = 0
mmap(0x7f76f184a000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWR
ITE, 3, 0) = 0x7f76f184a000
close(3)
                                         = 0
access("/etc/ld.so.nohwcap", F_OK)
                                        = −1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\1\0\0\0\320\37\2\0\0\0\0\0\"..., 8
32) = 832
fstat(3, {st mode=S IFREG|0755, st size=1840928, ...}) = 0
mmap(NULL, 3949248, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f7
6f1285000
mprotect(0x7f76f1440000, 2093056, PROT NONE) = 0
mmap(0x7f76f163f000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYW
RITE, 3, 0x1ba000) = 0x7f76f163f000
mmap(0x7f76f1645000, 17088, PROT READ|PROT WRITE, MAP PRIVATE|MAP FIXED|MAP ANONY
MOUS, -1, 0) = 0 \times 7 f 7 6 f 1 6 4 5 0 0 0
close(3)
                                         = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f76
f1a64000
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f76
f1a62000
arch_prctl(ARCH_SET_FS, 0x7f76f1a62740) = 0
mprotect(0x7f76f163f000, 16384, PROT_READ) = 0
mprotect(0x7f76f184a000, 4096, PROT_READ) = 0
mprotect(0x601000, 4096, PROT_READ)
mprotect(0x7f76f1a6e000, 4096, PROT_READ) = 0
munmap(0x7f76f1a65000, 25058)
fstat(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f76
f1a6b000
write(1, "this program tests the implement"..., 71this program tests the implemen
tation of a dynamically linked library.
) = 71
brk(0)
                                         = 0 \times 1897000
                                         = 0 \times 18b8000
brk(0x18b8000)
write(2, "4: get sum.c:20: main: Assertion"..., 554: get sum.c:20: main: Assertio
n `result == 4' failed.
) = 55
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f76
rt_sigprocmask(SIG_UNBLOCK, [ABRT], NULL, 8) = 0
gettid()
                                         = 22989
```

```
tgkill(22989, 22989, SIGABRT)
                                        = 0
--- SIGABRT {si signo=SIGABRT, si code=SI TKILL, si pid=22989, si uid=1000} ---
+++ killed by SIGABRT (core dumped) +++
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
lib361.c:5:1: error: expected identifier or '(' before 'return'
 return 4:
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
lib361.c:5:1: error: expected ',' or ';' before 'int'
 int secretoperation() { return num; }
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
lib361.c: In function 'secretoperation':
lib361.c:5:25: warning: return makes integer from pointer without a cast [enabled
 bv default]
 int secretoperation() { return num; }
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -d 4
```

4: file format elf64-x86-64

Disassembly of section .init:

```
0000000000400708 < init>:
  400708:
                48 83 ec 08
                                          sub
                                                 $0x8,%rsp
                48 8b 05 e5 18 20 00
  40070c:
                                                 0x2018e5(%rip),%rax
                                                                             # 601ff
                                          mov
8 <_fini+0x2012e4>
  400713:
                48 85 c0
                                          test
                                                 %rax,%rax
  400716:
                74 05
                                                 40071d <_init+0x15>
                                          iе
  400718:
                e8 a3 00 00 00
                                          callq
                                                 4007c0 <__gmon_start__@plt>
  40071d:
                48 83 c4 08
                                          add
                                                 $0x8,%rsp
  400721:
                с3
                                          retq
Disassembly of section .plt:
0000000000400730 <puts@plt-0x10>:
                ff 35 d2 18 20 00
                                                0x2018d2(%rip)
                                                                        # 602008 < f
  400730:
                                         pushq
ini+0x2012f4>
  400736:
                ff 25 d4 18 20 00
                                          jmpq
                                                 *0x2018d4(%rip)
                                                                         # 602010 <_
fini+0x2012fc>
  40073c:
                0f 1f 40 00
                                          nopl
                                                 0x0(%rax)
0000000000400740 <puts@plt>:
                ff 25 d2 18 20 00
  400740:
                                          jmpq
                                                 *0x2018d2(%rip)
                                                                        # 602018 <_
fini+0x201304>
                68 00 00 00 00
  400746:
                                          pushq
                                                 $0x0
  40074b:
                e9 e0 ff ff ff
                                          jmpq
                                                 400730 <_init+0x28>
000000000400750 <secretoperation@plt>:
                ff 25 ca 18 20 00
                                                 *0x2018ca(%rip)
                                                                        # 602020 <
  400750:
                                          jmpq
fini+0x20130c>
  400756:
                68 01 00 00 00
                                         pushq
                                                 $0x1
  40075b:
                e9 d0 ff ff ff
                                                 400730 <_init+0x28>
                                          jmpq
0000000000400760 <strlen@plt>:
  400760:
                ff 25 c2 18 20 00
                                          jmpq
                                                 *0x2018c2(%rip)
                                                                         # 602028 <
fini+0x201314>
  400766:
                68 02 00 00 00
                                          pushq
                                                 $0x2
  40076b:
                e9 c0 ff ff ff
                                          jmpq
                                                 400730 <_init+0x28>
0000000000400770 <__stack_chk_fail@plt>:
                ff 25 ba 18 20 00
  400770:
                                                 *0x2018ba(%rip)
                                                                         # 602030 <
                                          jmpq
fini+0x20131c>
  400776:
                68 03 00 00 00
                                          pushq
                                                 $0x3
  40077b:
                e9 b0 ff ff ff
                                          jmpq
                                                 400730 <_init+0x28>
0000000000400780 <printf@plt>:
                ff 25 b2 18 20 00
  400780:
                                          jmpq
                                                 *0x2018b2(%rip)
                                                                         # 602038 <_
fini+0x201324>
  400786:
                68 04 00 00 00
                                          pushq
                                                 $0x4
  40078b:
                e9 a0 ff ff ff
                                          jmpq
                                                 400730 < init+0x28>
000000000400790 <__assert_fail@plt>:
                ff 25 aa 18 20 00
                                                                        # 602040 <_
  400790:
                                          jmpq
                                                 *0x2018aa(%rip)
fini+0x20132c>
```

```
400796:
                 68 05 00 00 00
                                          pushq
                                                  $0x5
                 e9 90 ff ff ff
  40079b:
                                                 400730 <_init+0x28>
                                          jmpq
0000000004007a0 <__libc_start_main@plt>:
                ff 25 a2 18 20 00
  4007a0:
                                                 *0x2018a2(%rip)
                                                                          # 602048 <_
                                          jmpq
fini+0x201334>
  4007a6:
                 68 06 00 00 00
                                          pushq
                                                  $0x6
  4007ab:
                 e9 80 ff ff ff
                                                 400730 <_init+0x28>
                                          jmpq
00000000004007b0 <calloc@plt>:
  4007b0:
                 ff 25 9a 18 20 00
                                                 *0x20189a(%rip)
                                                                          # 602050 <
                                          jmpq
fini+0x20133c>
  4007b6:
                 68 07 00 00 00
                                          pushq
                                                 $0x7
  4007bb:
                e9 70 ff ff ff
                                          jmpq
                                                 400730 <_init+0x28>
0000000004007c0 <__gmon_start__@plt>:
  4007c0:
                 ff 25 92 18 20 00
                                                 *0x201892(%rip)
                                                                          # 602058 <_
                                          jmpq
fini+0x201344>
  4007c6:
                 68 08 00 00 00
                                          pushq
                                                 $0x8
                 e9 60 ff ff ff
  4007cb:
                                          jmpq
                                                 400730 <_init+0x28>
0000000004007d0 <getlogin_r@plt>:
                 ff 25 8a 18 20 00
  4007d0:
                                          jmpq
                                                 *0x20188a(%rip)
                                                                          # 602060 <
fini+0x20134c>
  4007d6:
                 68 09 00 00 00
                                          pushq
                                                 $0x9
  4007db:
                e9 50 ff ff ff
                                                 400730 < init+0x28>
                                          jmpq
Disassembly of section .text:
00000000004007e0 <.text>:
  4007e0:
                 31 ed
                                                 %ebp,%ebp
                                          xor
  4007e2:
                 49 89 d1
                                                 %rdx,%r9
                                          mov
  4007e5:
                 5e
                                                 %rsi
                                          qoq
                 48 89 e2
  4007e6:
                                                 %rsp,%rdx
                                          mov
                 48 83 e4 f0
  4007e9:
                                          and
                                                  $0xffffffffffffff,%rsp
  4007ed:
                 50
                                                 %rax
                                          push
  4007ee:
                 54
                                          push
                                                 %rsp
  4007ef:
                 49 c7 c0 10 0d 40 00
                                                  $0x400d10,%r8
                                          mov
  4007f6:
                 48 c7 c1 a0 0c 40 00
                                                  $0x400ca0,%rcx
                                          mov
                 48 c7 c7 cd 08 40 00
  4007fd:
                                          mov
                                                  $0x4008cd,%rdi
  400804:
                 e8 97 ff ff ff
                                          callq
                                                 4007a0 < libc start main@plt>
  400809:
                 f4
                                          hlt
  40080a:
                 66 0f 1f 44 00 00
                                          nopw
                                                 0x0(%rax,%rax,1)
  400810:
                 b8 17 21 60 00
                                                  $0x602117,%eax
                                          mov
  400815:
                 55
                                          push
                                                 %rbp
                 48 2d 10 21 60 00
  400816:
                                          sub
                                                  $0x602110,%rax
  40081c:
                 48 83 f8 0e
                                                  $0xe,%rax
                                          cmp
                 48 89 e5
  400820:
                                          mov
                                                 %rsp,%rbp
  400823:
                 77 02
                                                 400827 <getlogin_r@plt+0x57>
                                          jа
  400825:
                 5d
                                                 %rbp
                                          pop
  400826:
                 с3
                                          retq
  400827:
                 b8 00 00 00 00
                                                  $0x0,%eax
                                          mov
  40082c:
                 48 85 c0
                                          test
                                                 %rax,%rax
```

```
40082f:
                 74 f4
                                                   400825 <getlogin_r@plt+0x55>
                                           jе
  400831:
                 5d
                                                   %rbp
                                           pop
                 bf 10 21 60 00
                                                   $0x602110,%edi
  400832:
                                           mov
                 ff e0
  400837:
                                                   *%rax
                                           jmpq
                 0f 1f 80 00 00 00 00
                                                   0x0(%rax)
  400839:
                                           nopl
                 b8 10 21 60 00
  400840:
                                           mov
                                                   $0x602110,%eax
  400845:
                 55
                                           push
                                                   %rbp
                 48 2d 10 21 60 00
  400846:
                                           sub
                                                   $0x602110,%rax
  40084c:
                 48 c1 f8 03
                                                   $0x3,%rax
                                           sar
                 48 89 e5
  400850:
                                                   %rsp,%rbp
                                           mov
  400853:
                 48 89 c2
                                           mov
                                                   %rax,%rdx
  400856:
                 48 c1 ea 3f
                                                   $0x3f,%rdx
                                           shr
                 48 01 d0
                                                   %rdx,%rax
  40085a:
                                           add
  40085d:
                 48 d1 f8
                                           sar
                                                   %rax
  400860:
                 75 02
                                           ine
                                                   400864 < getlogin r@plt+0x94>
  400862:
                 5d
                                           pop
                                                   %rbp
  400863:
                 с3
                                           retq
  400864:
                 ba 00 00 00 00
                                                   $0x0,%edx
                                           mov
  400869:
                 48 85 d2
                                           test
                                                   %rdx,%rdx
                                                   400862 < getlogin_r@plt+0x92>
                 74 f4
  40086c:
                                           ie
                 5d
  40086e:
                                           pop
                                                   %rbp
                 48 89 c6
                                                   %rax,%rsi
  40086f:
                                           mov
                 bf 10 21 60 00
  400872:
                                           mov
                                                   $0x602110,%edi
                 ff e2
  400877:
                                           jmpq
                                                   *%rdx
                 Of 1f 80 00 00 00 00
  400879:
                                           nopl
                                                   0x0(%rax)
                 80 3d 85 18 20 00 00
                                                   $0x0,0x201885(%rip)
                                                                                # 60210
  400880:
                                           cmpb
c <_edata>
                 75 11
  400887:
                                                   40089a <getlogin r@plt+0xca>
                                           jne
  400889:
                 55
                                           push
                                                   %rbp
                 48 89 e5
                                                   %rsp,%rbp
  40088a:
                                           mov
  40088d:
                 e8 7e ff ff ff
                                           callq
                                                   400810 <getlogin_r@plt+0x40>
  400892:
                 5d
                                           pop
  400893:
                 c6 05 72 18 20 00 01
                                           movb
                                                   $0x1,0x201872(%rip)
                                                                                # 60210
c < edata>
  40089a:
                 f3 c3
                                           repz retq
  40089c:
                 0f 1f 40 00
                                           nopl
                                                   0x0(%rax)
                 48 83 3d 68 15 20 00
  4008a0:
                                           cmpq
                                                   $0x0,0x201568(%rip)
                                                                                # 601e1
0 < fini+0x2010fc>
  4008a7:
                 00
  4008a8:
                 74 1e
                                                   4008c8 <getlogin_r@plt+0xf8>
                                           jе
  4008aa:
                 b8 00 00 00 00
                                           mov
                                                   $0x0,%eax
  4008af:
                 48 85 c0
                                           test
                                                   %rax,%rax
  4008b2:
                 74 14
                                           jе
                                                   4008c8 <getlogin_r@plt+0xf8>
                 55
  4008b4:
                                           push
                                                   %rbp
  4008b5:
                 bf 10 1e 60 00
                                           mov
                                                   $0x601e10,%edi
                 48 89 e5
  4008ba:
                                           mov
                                                   %rsp,%rbp
  4008bd:
                 ff d0
                                           callq
                                                  *%rax
                 5d
  4008bf:
                                           pop
                                                   %rbp
  4008c0:
                 e9 7b ff ff ff
                                           jmpq
                                                   400840 < \text{getlogin r@plt+0x70}
                 0f 1f 00
  4008c5:
                                           nopl
                 e9 73 ff ff ff
  4008c8:
                                           jmpq
                                                   400840 <getlogin_r@plt+0x70>
                 55
                                                   %rbp
  4008cd:
                                           push
  4008ce:
                 48 89 e5
                                           mov
                                                   %rsp,%rbp
```

```
4008d1:
                 48 83 ec 10
                                          sub
                                                  $0x10,%rsp
                 c7 45 f4 01 00 00 00
                                                  $0x1,-0xc(%rbp)
  4008d5:
                                          movl
                                                  $0x2,-0x8(%rbp)
  4008dc:
                 c7 45 f8 02 00 00 00
                                          movl
                 c7 45 fc 00 00 00 00
                                                  $0x0,-0x4(%rbp)
  4008e3:
                                          movl
                 bf 70 0d 40 00
                                                  $0x400d70,%edi
  4008ea:
                                          mov
                 e8 4c fe ff ff
                                                  400740 <puts@plt>
  4008ef:
                                          callq
  4008f4:
                 be 06 00 00 00
                                                  $0x6,%esi
                                          mov
                 bf 03 00 00 00
  4008f9:
                                          mov
                                                  $0x3,%edi
  4008fe:
                 e8 4d fe ff ff
                                          callq
                                                  400750 <secretoperation@plt>
                 89 45 fc
                                                  %eax,-0x4(%rbp)
  400903:
                                          mov
  400906:
                 83 7d fc 0a
                                          cmpl
                                                  $0xa,-0x4(%rbp)
  40090a:
                 74 19
                                                  400925 <getlogin_r@plt+0x155>
                                          jе
  40090c:
                 b9 da 0d 40 00
                                                  $0x400dda,%ecx
                                          mov
  400911:
                 ba 12 00 00 00
                                                  $0x12,%edx
                                          mov
  400916:
                 be b7 0d 40 00
                                                  $0x400db7,%esi
                                          mov
  40091b:
                 bf c1 0d 40 00
                                          mov
                                                  $0x400dc1,%edi
  400920:
                 e8 6b fe ff ff
                                          callq
                                                  400790 <__assert_fail@plt>
                 8b 55 f8
  400925:
                                                  -0x8(%rbp),%edx
                                          mov
  400928:
                 8b 45 f4
                                          mov
                                                  -0xc(%rbp),%eax
                 89 d6
  40092b:
                                                  %edx,%esi
                                          mov
                 89 c7
  40092d:
                                          mov
                                                  %eax,%edi
                 e8 1c fe ff ff
                                                  400750 <secretoperation@plt>
  40092f:
                                          callq
                                                  %eax,-0x4(%rbp)
                 89 45 fc
  400934:
                                          mov
                 83 7d fc 04
  400937:
                                          cmpl
                                                  $0x4,-0x4(%rbp)
                 74 19
  40093b:
                                                  400956 <getlogin_r@plt+0x186>
                                          jе
                 b9 da 0d 40 00
                                                  $0x400dda,%ecx
  40093d:
                                          mov
  400942:
                 ba 14 00 00 00
                                                  $0x14,%edx
                                          mov
                 be b7 0d 40 00
  400947:
                                                  $0x400db7,%esi
                                          mov
  40094c:
                 bf ce 0d 40 00
                                                  $0x400dce,%edi
                                          mov
                 e8 3a fe ff ff
                                                  400790 <__assert_fail@plt>
  400951:
                                          callq
  400956:
                 48 8b 05 33 17 20 00
                                                  0x201733(%rip),%rax
                                                                               # 60209
                                          mov
0 < fini+0x20137c>
  40095d:
                 48 89 c7
                                          mov
                                                  %rax,%rdi
  400960:
                 e8 28 00 00 00
                                          callq
                                                  40098d <getlogin_r@plt+0x1bd>
  400965:
                 48 89 c2
                                          mov
                                                  %rax,%rdx
                 48 8b 0d 31 17 20 00
  400968:
                                                  0x201731(%rip),%rcx
                                                                               # 6020a
                                          mov
0 <_fini+0x20138c>
                 48 8b 05 22 17 20 00
                                                  0x201722(%rip),%rax
  40096f:
                                          mov
                                                                               # 60209
8 <_fini+0x201384>
                 48 89 ce
                                                  %rcx,%rsi
  400976:
                                          mov
  400979:
                 48 89 c7
                                          mov
                                                  %rax,%rdi
  40097c:
                 b8 00 00 00 00
                                          mov
                                                  $0x0,%eax
                                                  400780 <printf@plt>
  400981:
                 e8 fa fd ff ff
                                          callq
  400986:
                 b8 00 00 00 00
                                          mov
                                                  $0x0,%eax
                                          leaveq
  40098b:
                 c9
                 с3
  40098c:
                                          retq
  40098d:
                 55
                                          push
                                                  %rbp
                 48 89 e5
  40098e:
                                          mov
                                                  %rsp,%rbp
  400991:
                 53
                                          push
                                                  %rbx
  400992:
                 48 81 ec 38 04 00 00
                                          sub
                                                  $0x438,%rsp
  400999:
                 48 89 bd c8 fb ff ff
                                          mov
                                                  %rdi,-0x438(%rbp)
                 64 48 8b 04 25 28 00
                                                  %fs:0x28,%rax
  4009a0:
                                          mov
  4009a7:
                 00 00
```

```
4009a9:
               48 89 45 e8
                                                %rax,-0x18(%rbp)
                                        mov
4009ad:
               31 c0
                                                %eax,%eax
                                        xor
               48 8d 85 e0 fb ff ff
4009af:
                                        lea
                                                -0x420(%rbp),%rax
              be 00 04 00 00
                                                $0x400,%esi
4009b6:
                                        mov
4009bb:
              48 89 c7
                                        mov
                                                %rax,%rdi
              e8 0d fe ff ff
4009be:
                                               4007d0 <getlogin_r@plt>
                                        callq
4009c3:
               c7 85 d4 fb ff ff 00
                                                $0x0.-0x42c(%rbp)
                                        movl
               00 00 00
4009ca:
4009cd:
               eb 3e
                                        jmp
                                                400a0d <getlogin_r@plt+0x23d>
              8b 85 d4 fb ff ff
                                                -0x42c(%rbp),%eax
4009cf:
                                        mov
4009d5:
               48 98
                                        cltq
4009d7:
               0f b6 94 05 e0 fb ff
                                        movzbl -0x420(%rbp,%rax,1),%edx
4009de:
               ff
4009df:
              8b 85 d4 fb ff ff
                                        mov
                                                -0x42c(%rbp),%eax
4009e5:
               48 63 c8
                                        movslq %eax,%rcx
4009e8:
              48 8b 85 c8 fb ff ff
                                        mov
                                                -0x438(%rbp),%rax
4009ef:
              48 01 c8
                                        add
                                                %rcx,%rax
              0f b6 00
4009f2:
                                        movzbl (%rax),%eax
4009f5:
               31 c2
                                        xor
                                                %eax,%edx
              8b 85 d4 fb ff ff
4009f7:
                                        mov
                                                -0x42c(%rbp),%eax
              48 98
4009fd:
                                        cltq
              88 94 05 e0 fb ff ff
                                                %dl,-0x420(%rbp,%rax,1)
4009ff:
                                        mov
              83 85 d4 fb ff ff 01
                                                $0x1,-0x42c(%rbp)
400a06:
                                        addl
              8b 85 d4 fb ff ff
400a0d:
                                        mov
                                                -0x42c(%rbp),%eax
              48 63 d8
400a13:
                                        movslq %eax,%rbx
              48 8d 85 e0 fb ff ff
                                        lea
                                                -0x420(%rbp),%rax
400a16:
400a1d:
              48 89 c7
                                        mov
                                                %rax,%rdi
              e8 3b fd ff ff
400a20:
                                        callq
                                                400760 <strlen@plt>
400a25:
              48 39 c3
                                        cmp
                                                %rax,%rbx
              72 a5
                                                4009cf <getlogin_r@plt+0x1ff>
400a28:
                                        jЬ
400a2a:
              8b 85 d4 fb ff ff
                                        mov
                                                -0x42c(%rbp),%eax
400a30:
               48 63 c8
                                        movslq %eax,%rcx
              48 8d 95 d8 fb ff ff
400a33:
                                        lea
                                                -0x428(%rbp),%rdx
              48 8d 85 e0 fb ff ff
400a3a:
                                        lea
                                                -0x420(%rbp),%rax
              48 89 ce
400a41:
                                        mov
                                                %rcx,%rsi
              48 89 c7
400a44:
                                        mov
                                                %rax,%rdi
400a47:
              e8 1e 00 00 00
                                        callq
                                                400a6a <getlogin_r@plt+0x29a>
              48 8b 75 e8
                                                -0x18(%rbp), %rsi
400a4c:
                                        mov
400a50:
              64 48 33 34 25 28 00
                                                %fs:0x28,%rsi
                                        xor
               00 00
400a57:
400a59:
               74 05
                                        jе
                                                400a60 <getlogin r@plt+0x290>
400a5b:
               e8 10 fd ff ff
                                        callq
                                                400770 <__stack_chk_fail@plt>
               48 81 c4 38 04 00 00
400a60:
                                        add
                                                $0x438,%rsp
               5b
400a67:
                                        pop
                                                %rbx
400a68:
               5d
                                        pop
                                                %rbp
400a69:
               с3
                                        retq
400a6a:
               55
                                        push
                                                %rbp
              48 89 e5
                                                %rsp,%rbp
400a6b:
                                        mov
400a6e:
               48 83 ec 40
                                        sub
                                                $0x40,%rsp
                                                %rdi,-0x28(%rbp)
400a72:
              48 89 7d d8
                                        mov
400a76:
               48 89 75 d0
                                        mov
                                                %rsi,-0x30(%rbp)
                                                rdx_{-0}x38(rbp)
               48 89 55 c8
400a7a:
                                        mov
                                                -0x30(%rbp),%rax
400a7e:
               48 8b 45 d0
                                        mov
```

```
400a82:
               48 83 c0 02
                                        add
                                                $0x2,%rax
               48 ba ab aa aa aa
400a86:
                                        movabs $0xaaaaaaaaaaaaaaab,%rdx
400a8d:
               aa aa aa
              48 f7 e2
400a90:
                                        mul
                                                %rdx
               48 89 d0
400a93:
                                        mov
                                                %rdx,%rax
               48 d1 e8
                                                %rax
400a96:
                                        shr
400a99:
               48 8d 14 85 00 00 00
                                                0x0(,%rax,4),%rdx
                                        lea
400aa0:
               00
400aa1:
              48 8b 45 c8
                                        mov
                                                -0x38(%rbp),%rax
              48 89 10
                                                %rdx,(%rax)
400aa5:
                                        mov
400aa8:
              48 8b 45 c8
                                        mov
                                                -0x38(%rbp),%rax
400aac:
              48 8b 00
                                                (%rax),%rax
                                        mov
400aaf:
              be 01 00 00 00
                                                $0x1,%esi
                                        mov
400ab4:
              48 89 c7
                                                %rax,%rdi
                                        mov
400ab7:
              e8 f4 fc ff ff
                                        callq
                                                4007b0 <calloc@plt>
400abc:
              48 89 45 f8
                                        mov
                                                %rax,-0x8(%rbp)
                                                $0x0,-0x8(%rbp)
400ac0:
              48 83 7d f8 00
                                        cmpq
400ac5:
              75 0a
                                        jne
                                                400ad1 <getlogin_r@plt+0x301>
400ac7:
              b8 00 00 00 00
                                        moν
                                                $0x0,%eax
                                                400c91 <getlogin_r@plt+0x4c1>
400acc:
              e9 c0 01 00 00
                                        jmpq
               c7 45 e0 00 00 00 00
                                                $0x0,-0x20(%rbp)
400ad1:
                                        movl
               c7 45 e4 00 00 00 00
                                                $0x0,-0x1c(%rbp)
400ad8:
                                        movl
               e9 3b 01 00 00
                                                400c1f <getlogin_r@plt+0x44f>
400adf:
                                        jmpq
              8b 45 e0
                                                -0x20(%rbp),%eax
400ae4:
                                        mov
              48 98
400ae7:
                                        cltq
              48 3b 45 d0
                                                -0x30(%rbp),%rax
400ae9:
                                        cmp
400aed:
              73 1b
                                        jae
                                                400b0a <getlogin_r@plt+0x33a>
                                                -0x20(%rbp),%eax
400aef:
              8b 45 e0
                                        mov
400af2:
              8d 50 01
                                                0x1(%rax),%edx
                                        lea
              89 55 e0
                                                %edx,-0x20(%rbp)
400af5:
                                        mov
400af8:
              48 63 d0
                                        movslq %eax,%rdx
400afb:
              48 8b 45 d8
                                        mov
                                                -0x28(%rbp),%rax
400aff:
              48 01 d0
                                        add
                                                %rdx,%rax
400b02:
              0f b6 00
                                        movzbl (%rax),%eax
400b05:
              0f b6 c0
                                        movzbl %al,%eax
400b08:
              eb 05
                                                400b0f <getlogin_r@plt+0x33f>
                                        jmp
400b0a:
              b8 00 00 00 00
                                        mov
                                                $0x0,%eax
              89 45 e8
400b0f:
                                                %eax,-0x18(%rbp)
                                        mov
400b12:
              8b 45 e0
                                                -0x20(%rbp),%eax
                                        mov
              48 98
400b15:
                                        cltq
400b17:
              48 3b 45 d0
                                        cmp
                                                -0x30(%rbp),%rax
              73 1b
400b1b:
                                                400b38 <getlogin_r@plt+0x368>
                                        jae
400b1d:
              8b 45 e0
                                        mov
                                                -0x20(%rbp),%eax
               8d 50 01
400b20:
                                        lea
                                                0x1(%rax),%edx
400b23:
              89 55 e0
                                        mov
                                                %edx,-0x20(%rbp)
              48 63 d0
                                        movslq %eax,%rdx
400b26:
400b29:
              48 8b 45 d8
                                        mov
                                                -0x28(%rbp),%rax
              48 01 d0
                                                %rdx,%rax
400b2d:
                                        add
                                        movzbl (%rax),%eax
400b30:
               0f b6 00
400b33:
              0f b6 c0
                                        movzbl %al,%eax
400b36:
              eb 05
                                        jmp
                                                400b3d <getlogin r@plt+0x36d>
400b38:
               b8 00 00 00 00
                                                $0x0,%eax
                                        mov
400b3d:
              89 45 ec
                                        mov
                                                %eax,-0x14(%rbp)
```

```
400b40:
               8b 45 e0
                                                -0x20(%rbp),%eax
                                         mov
               48 98
400b43:
                                         cltq
               48 3b 45 d0
400b45:
                                         cmp
                                                -0x30(%rbp),%rax
               73 1b
400b49:
                                                400b66 <getlogin r@plt+0x396>
                                         jae
400b4b:
               8b 45 e0
                                                -0x20(%rbp),%eax
                                         mov
               8d 50 01
                                                0x1(%rax),%edx
400b4e:
                                         lea
               89 55 e0
                                                %edx,-0x20(%rbp)
400b51:
                                         mov
               48 63 d0
400b54:
                                         movslq %eax,%rdx
400b57:
               48 8b 45 d8
                                                -0x28(%rbp),%rax
                                         mov
               48 01 d0
400b5b:
                                         add
                                                %rdx,%rax
400b5e:
               0f b6 00
                                         movzbl (%rax),%eax
               0f b6 c0
                                         movzbl %al,%eax
400b61:
               eb 05
                                                400b6b <getlogin_r@plt+0x39b>
400b64:
                                         jmp
               b8 00 00 00 00
                                                $0x0,%eax
400b66:
                                         mov
400b6b:
               89 45 f0
                                                %eax,-0x10(%rbp)
                                         mov
400b6e:
               8b 45 e8
                                         mov
                                                -0x18(%rbp),%eax
400b71:
               c1 e0 10
                                         shl
                                                $0x10,%eax
400b74:
               89 c2
                                                %eax,%edx
                                         mov
400b76:
               8b 45 ec
                                         mov
                                                -0x14(%rbp),%eax
400b79:
               c1 e0 08
                                         shl
                                                $0x8,%eax
400b7c:
               01 c2
                                         add
                                                %eax,%edx
               8b 45 f0
400b7e:
                                         mov
                                                -0x10(%rbp),%eax
               01 d0
                                                %edx,%eax
400b81:
                                         add
400b83:
               89 45 f4
                                         mov
                                                %eax,-0xc(%rbp)
                                                -0x1c(%rbp),%eax
400b86:
               8b 45 e4
                                         mov
               8d 50 01
                                                0x1(%rax),%edx
400b89:
                                         lea
400b8c:
               89 55 e4
                                         mov
                                                %edx,-0x1c(%rbp)
               48 63 d0
                                         movslq %eax,%rdx
400b8f:
400b92:
               48 8b 45 f8
                                                -0x8(%rbp),%rax
                                         mov
               48 01 c2
400b96:
                                                %rax,%rdx
                                         add
                                                -0xc(%rbp),%eax
400b99:
               8b 45 f4
                                         mov
               c1 e8 12
400b9c:
                                         shr
                                                $0x12,%eax
                                                $0x3f,%eax
400b9f:
               83 e0 3f
                                         and
               89 c0
                                         mov
400ba2:
                                                %eax,%eax
400ba4:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400bab:
               88 02
                                                %al,(%rdx)
                                         mov
400bad:
               8b 45 e4
                                         mov
                                                -0x1c(%rbp),%eax
400bb0:
               8d 50 01
                                         lea
                                                0x1(%rax),%edx
400bb3:
               89 55 e4
                                                %edx,-0x1c(%rbp)
                                         mov
               48 63 d0
400bb6:
                                         movslq %eax,%rdx
400bb9:
               48 8b 45 f8
                                         mov
                                                -0x8(%rbp),%rax
400bbd:
               48 01 c2
                                                %rax,%rdx
                                         add
400bc0:
               8b 45 f4
                                         mov
                                                -0xc(%rbp),%eax
400bc3:
               c1 e8 0c
                                         shr
                                                $0xc, %eax
400bc6:
               83 e0 3f
                                         and
                                                $0x3f,%eax
               89 c0
400bc9:
                                         mov
                                                %eax,%eax
400bcb:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
                                                %al,(%rdx)
400bd2:
               88 02
                                         mov
400bd4:
               8b 45 e4
                                         mov
                                                -0x1c(%rbp),%eax
                                                0x1(%rax),%edx
400bd7:
               8d 50 01
                                         lea
400bda:
               89 55 e4
                                         mov
                                                %edx,-0x1c(%rbp)
               48 63 d0
                                         movslq %eax,%rdx
400bdd:
400be0:
               48 8b 45 f8
                                         mov
                                                -0x8(%rbp),%rax
```

```
400be4:
               48 01 c2
                                         add
                                                %rax,%rdx
               8b 45 f4
400be7:
                                                -0xc(%rbp),%eax
                                         mov
400bea:
               c1 e8 06
                                         shr
                                                $0x6,%eax
               83 e0 3f
400bed:
                                                $0x3f,%eax
                                         and
               89 c0
400bf0:
                                                %eax,%eax
                                         mov
               0f b6 80 c0 20 60 00
400bf2:
                                         movzbl 0x6020c0(%rax),%eax
400bf9:
               88 02
                                                %al,(%rdx)
                                         mov
               8b 45 e4
400bfb:
                                                -0x1c(%rbp),%eax
                                         mov
400bfe:
               8d 50 01
                                         lea
                                                0x1(%rax),%edx
               89 55 e4
400c01:
                                                %edx,-0x1c(%rbp)
                                         mov
400c04:
               48 63 d0
                                         movslq %eax,%rdx
               48 8b 45 f8
                                                -0x8(%rbp),%rax
400c07:
                                         mov
               48 01 c2
400c0b:
                                         add
                                                %rax,%rdx
400c0e:
               8b 45 f4
                                                -0xc(%rbp),%eax
                                         mov
400c11:
               83 e0 3f
                                                $0x3f,%eax
                                         and
400c14:
               89 c0
                                         mov
                                                %eax,%eax
400c16:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400c1d:
               88 02
                                                %al,(%rdx)
                                         mov
400c1f:
               8b 45 e0
                                         mov
                                                -0x20(%rbp),%eax
               48 98
400c22:
                                         clta
               48 3b 45 d0
                                                -0x30(%rbp),%rax
400c24:
                                         cmp
               0f 82 b6 fe ff ff
                                                400ae4 <getlogin_r@plt+0x314>
400c28:
                                         jЬ
               c7 45 e0 00 00 00 00
                                                $0x0,-0x20(%rbp)
400c2e:
                                         movl
400c35:
               eb 24
                                         jmp
                                                400c5b <getlogin_r@plt+0x48b>
400c37:
               48 8b 45 c8
                                                -0x38(%rbp),%rax
                                         mov
               48 8b 10
400c3b:
                                                (%rax),%rdx
                                         mov
400c3e:
               8b 45 e0
                                                -0x20(%rbp),%eax
                                         mov
               48 98
400c41:
                                         cltq
400c43:
               48 29 c2
                                         sub
                                                %rax,%rdx
               48 89 d0
400c46:
                                                %rdx,%rax
                                         mov
400c49:
               48 8d 50 ff
                                                -0x1(%rax),%rdx
                                         lea
400c4d:
               48 8b 45 f8
                                         mov
                                                -0x8(%rbp),%rax
400c51:
               48 01 d0
                                         add
                                                %rdx,%rax
400c54:
               c6 00 3d
                                                $0x3d,(%rax)
                                         movb
400c57:
               83 45 e0 01
                                         addl
                                                $0x1,-0x20(%rbp)
400c5b:
               48 8b 4d d0
                                                -0x30(%rbp),%rcx
                                         mov
               48 ba ab aa aa aa
400c5f:
                                        movabs $0xaaaaaaaaaaaaaab,%rdx
400c66:
               aa aa aa
400c69:
               48 89 c8
                                                %rcx,%rax
                                         mov
               48 f7 e2
                                                %rdx
400c6c:
                                         mul
400c6f:
               48 d1 ea
                                         shr
                                                %rdx
400c72:
               48 89 d0
                                                %rdx,%rax
                                         mov
400c75:
               48 01 c0
                                         add
                                                %rax,%rax
400c78:
               48 01 d0
                                         add
                                                %rdx,%rax
400c7b:
               48 29 c1
                                         sub
                                                %rax,%rcx
               48 89 ca
400c7e:
                                         mov
                                                %rcx,%rdx
400c81:
               8b 04 95 00 21 60 00
                                         mov
                                                0x602100(,%rdx,4),%eax
               3b 45 e0
400c88:
                                         cmp
                                                -0x20(%rbp),%eax
                                                400c37 <getlogin_r@plt+0x467>
400c8b:
               7f aa
                                         jg
               48 8b 45 f8
400c8d:
                                         mov
                                                -0x8(%rbp),%rax
400c91:
               c9
                                         leaveq
               с3
400c92:
                                         retq
400c93:
               66 2e 0f 1f 84 00 00
                                         nopw
                                                %cs:0x0(%rax,%rax,1)
```

```
400c9a:
                00 00 00
                0f 1f 00
                                                 (%rax)
  400c9d:
                                          nopl
                41 57
  400ca0:
                                          push
                                                 %r15
                41 89 ff
                                                 %edi,%r15d
  400ca2:
                                          mov
                41 56
                                                 %r14
  400ca5:
                                          push
                49 89 f6
                                                 %rsi,%r14
  400ca7:
                                          mov
  400caa:
                41 55
                                                 %r13
                                          push
                49 89 d5
  400cac:
                                          mov
                                                 %rdx,%r13
  400caf:
                41 54
                                          push
                                                 %r12
  400cb1:
                4c 8d 25 48 11 20 00
                                                 0x201148(%rip),%r12
                                                                              # 601e0
                                          lea
0 <_fini+0x2010ec>
  400cb8:
                                          push
                55
                                                 %rbp
  400cb9:
                48 8d 2d 48 11 20 00
                                          lea
                                                 0x201148(%rip),%rbp
                                                                              # 601e0
8 <_fini+0x2010f4>
  400cc0:
                53
                                          push
                                                 %rbx
                4c 29 e5
  400cc1:
                                          sub
                                                 %r12,%rbp
  400cc4:
                31 db
                                          xor
                                                 %ebx,%ebx
  400cc6:
                48 c1 fd 03
                                                 $0x3,%rbp
                                          sar
  400cca:
                48 83 ec 08
                                          sub
                                                 $0x8,%rsp
                e8 35 fa ff ff
                                                 400708 <_init>
  400cce:
                                          callq
                48 85 ed
                                          test
                                                 %rbp,%rbp
  400cd3:
                                                 400cf6 <getlogin_r@plt+0x526>
                74 1e
  400cd6:
                                          jе
                0f 1f 84 00 00 00 00
                                                 0x0(%rax,%rax,1)
  400cd8:
                                          nopl
  400cdf:
                00
  400ce0:
                4c 89 ea
                                          mov
                                                 %r13,%rdx
                4c 89 f6
                                                 %r14,%rsi
  400ce3:
                                          mov
  400ce6:
                44 89 ff
                                          mov
                                                 %r15d,%edi
                41 ff 14 dc
  400ce9:
                                          callq
                                                 *(%r12,%rbx,8)
  400ced:
                48 83 c3 01
                                          add
                                                 $0x1,%rbx
                48 39 eb
  400cf1:
                                                 %rbp,%rbx
                                          cmp
  400cf4:
                75 ea
                                          jne
                                                 400ce0 <getlogin_r@plt+0x510>
  400cf6:
                48 83 c4 08
                                          add
                                                 $0x8,%rsp
  400cfa:
                5b
                                                 %rbx
                                          pop
  400cfb:
                5d
                                                 %rbp
                                          pop
  400cfc:
                41 5c
                                          pop
                                                 %r12
  400cfe:
                41 5d
                                                 %r13
                                          pop
  400d00:
                41 5e
                                          pop
                                                 %r14
                41 5f
                                                 %r15
  400d02:
                                          pop
  400d04:
                с3
                                          retq
                66 66 2e 0f 1f 84 00
                                          data32 nopw %cs:0x0(%rax,%rax,1)
  400d05:
  400d0c:
                00 00 00 00
  400d10:
                f3 c3
                                          repz retq
Disassembly of section .fini:
0000000000400d14 <_fini>:
  400d14:
                48 83 ec 08
                                          sub
                                                  $0x8,%rsp
  400d18:
                48 83 c4 08
                                          add
                                                 $0x8,%rsp
  400d1c:
                с3
                                          retq
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ scanelf result 4
        FILE
TYPE
ET EXEC 4
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ scanelf --name result 4
```

```
scanelf: Unknown option '' or argument missing
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ scanelf -name result 4
               PERM ENDIAN STK/REL/PTL TEXTREL RPATH NEEDED BIND FILE
TYPE
ET EXEC PeMRxS 0775 LE RW- R-- RW-
                                                  lib361.so,libc.so.6 LAZY 4
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ clear
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ strings 4
/lib64/ld-linux-x86-64.so.2
lib361.so
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
_{
m init}
secretoperation
_fini
libc.so.6
puts
__stack_chk_fail
__assert_fail
printf
calloc
strlen
getlogin r
__libc_start_main
_edata
__bss_start
end
GLIBC 2.4
GLIBC 2.2.5
dH34%(
[]A\A]A^A
34567890123456789012
%5%5
you win! the secret is:
bangarang
this program tests the implementation of a dynamically linked library.
qet sum.c
result == 10
result == 4
main
;*3$"
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
GCC: (Ubuntu 4.8.4-2ubuntu1~14.04) 4.8.4
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
```

```
.gnu.hash
.dynsym
.dynstr
.qnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.text
.fini
.rodata
.eh_frame_hdr
.eh frame
.init_array
.fini array
.jcr
.dynamic
.got
.got.plt
.data
.bss
.comment
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 4
GNU qdb (Ubuntu 7.7.1-0ubuntu5~14.04.2) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from 4...(no debugging symbols found)...done.
(qdb) disas
No frame selected.
(qdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/4
this program tests the implementation of a dynamically linked library.
4: get sum.c:20: main: Assertion `result == 4' failed.
```

Program received signal SIGABRT, Aborted.

```
0x00007fffff7849cc9 in __GI_raise (sig=sig@entry=6)
    at ../nptl/sysdeps/unix/sysv/linux/raise.c:56
        ../nptl/sysdeps/unix/sysv/linux/raise.c: No such file or directory.
56
(qdb) b main
Function "main" not defined.
Make breakpoint pending on future shared library load? (y or [n]) n
(qdb) quit
A debugging session is active.
        Inferior 1 [process 23157] will be killed.
Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ clear
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ strings 4
/lib64/ld-linux-x86-64.so.2
lib361.so
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
_{
m init}
secretoperation
fini
libc.so.6
puts
__stack_chk_fail
__assert_fail
printf
calloc
strlen
getlogin r
__libc_start_main
_edata
__bss_start
end
GLIBC<sub>2.4</sub>
GLIBC 2.2.5
dH34%(
[]A\A]A^A_
34567890123456789012
%5%5
you win! the secret is:
bangarang
this program tests the implementation of a dynamically linked library.
get_sum.c
result == 10
result == 4
main
;*3$"
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
GCC: (Ubuntu 4.8.4-2ubuntu1~14.04) 4.8.4
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
```

```
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
.got
.got.plt
.data
.bss
.comment
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -a 4
ELF Header:
 Magic:
          7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
 Class:
                                     ELF64
 Data:
                                     2's complement, little endian
 Version:
                                     1 (current)
 OS/ABI:
                                     UNIX - System V
 ABI Version:
                                     EXEC (Executable file)
 Type:
                                     Advanced Micro Devices X86-64
 Machine:
 Version:
                                     0x1
 Entry point address:
                                     0x4007e0
  Start of program headers:
                                     64 (bytes into file)
 Start of section headers:
                                     8792 (bytes into file)
 Flags:
                                     0x0
                                     64 (bytes)
 Size of this header:
 Size of program headers:
                                     56 (bytes)
 Number of program headers:
 Size of section headers:
                                     64 (bytes)
 Number of section headers:
 Section header string table index: 27
Section Headers:
  [Nr] Name
                         Type
                                          Address
                                                             0ffset
       Size
                         EntSize
                                          Flags Link Info Align
  [ 0 ]
                                          000000000000000 0000000
                         NULL
       0
                                                          0
                                                                 0
```

Г 1	1	intorn	DDOCDITC	000000000000000000000000000000000000000	00000220
ГТ	L]	<pre>.interp 000000000000001c</pre>	PROGBITS	0000000000400238 A 0 0	00000238 1
Γ⊃	2]	.note.ABI-tag	00000000000000000 NOTE	A 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	00000254
LZ	- 1	00000000000000020	00000000000000000	A 0 0	4
Г २	3]	<pre>.note.gnu.build-i</pre>		0000000000400274	00000274
	, ,	00000000000000024	00000000000000000	A 0 0	4
「 4	1]	.gnu.hash	GNU HASH	0000000000400298	00000298
-	•	00000000000000038	000000000000000000	A 5 0	8
[5	5]	.dynsym	DYNSYM	00000000004002d0	000002d0
		00000000000001c8	0000000000000018	A 6 1	8
[6	5]	.dynstr	STRTAB	0000000000400498	00000498
		000000000000010e	000000000000000000	A 0 0	1
[7	7]	<pre>.gnu.version</pre>	VERSYM	00000000004005a6	000005a6
		00000000000000026	000000000000000002	A 5 0	2
[8	3]	.gnu.version_r	VERNEED	00000000004005d0	000005d0
_		0000000000000030	0000000000000000	A 6 1	8
[9]	.rela.dyn	RELA	0000000000400600	00000600
		0000000000000018	0000000000000018	A 5 0	8
[10)]	.rela.plt	RELA	0000000000400618	00000618
Г а а	. 1	00000000000000f0	0000000000000018	A 5 12	8
[11	LJ	init	PROGBITS 000000000000000000000000000000000000	0000000000400708	00000708
[12	1	0000000000000001a .plt	PROGBITS	AX 0 0 00000000000400730	4 00000730
LIZ	- 1	000000000000000000000	000000000000000000000000000000000000000	AX 0 0	16
[13	1 1	.text	PROGBITS	00000000004007e0	000007e0
	, ,	00000000000000532	00000000000000000	AX 0 0	16
[14	11	.fini	PROGBITS	00000000000400d14	00000d14
-	•	000000000000000009	000000000000000000	AX 0 0	4
[15	5]	.rodata	PROGBITS	0000000000400d20	00000d20
		000000000000000bf	00000000000000000	A 0 0	8
[16	5]	<pre>.eh_frame_hdr</pre>	PROGBITS	0000000000400de0	00000de0
		00000000000000044	00000000000000000	A 0 0	4
[17	7]	.eh_frame	PROGBITS	00000000000400e28	00000e28
_		000000000000013c	00000000000000000	A 0 0	8
[18	3]			0000000000601e00	
r		0000000000000008			
[19)]	.fini_array			
ר ז מ	. T	0000000000000008	0000000000000000		
[20)]	.jcr	PROGBITS 000000000000000000000000000000000000	00000000000601e10	
[21	1	00000000000000008 .dynamic	DYNAMIC	WA 0 0 00000000000601e18	
[L J	00000000000001e0	000000000000000000000000000000000000000		
[22	1	.got	PROGBITS	0000000000601ff8	
		00000000000000008	00000000000000008		
[23	31		PROGBITS	0000000000602000	_
	•	00000000000000068	00000000000000008		
[24	ļ]	.data	PROGBITS	0000000000602080	00002080
		0000000000000008c	00000000000000000		
[25	5]	.bss	NOBITS	000000000060210c	0000210c
		00000000000000004	00000000000000000	WA 0 0	1
[26	5]	<pre>.comment</pre>	PROGBITS	0000000000000000	0000210c
			000000000000000001		1
[27	']	.shstrtab	STRTAB	0000000000000000	00002159

```
00000000000000f8 0000000000000000
                                                           1
Key to Flags:
 W (write), A (alloc), X (execute), M (merge), S (strings), l (large)
  I (info), L (link order), G (group), T (TLS), E (exclude), x (unknown)
  O (extra OS processing required) o (OS specific), p (processor specific)
There are no section groups in this file.
Program Headers:
               Offset
                                 VirtAddr
                                                   PhysAddr
 Type
               FileSiz
                                 MemSiz
                                                   Flags Align
 PHDR
               0x0000000000001f8 0x0000000000001f8
                                                   R E
  INTERP
               0x000000000000238 0x000000000400238 0x0000000000400238
               0x000000000000001c 0x00000000000001c
      [Requesting program interpreter: /lib64/ld-linux-x86-64.so.2]
  L<sub>OAD</sub>
               0x0000000000000f64 0x0000000000000f64
                                                   R E
 LOAD
               0x000000000001e00 0x000000000601e00 0x000000000601e00
               0x000000000000030c 0x000000000000310
                                                   RW
                                                          200000
  DYNAMIC
               0x00000000001e18 0x0000000000601e18 0x0000000000601e18
               0x00000000000001e0 0x0000000000001e0
                                                   RW
                                                          8
 NOTE.
               0 \times 0000000000000254 0 \times 000000000400254 0 \times 0000000000400254
               0x0000000000000044 0x0000000000000044
               0x000000000000de0 0x000000000400de0 0x000000000400de0
  GNU_EH_FRAME
               0 \times 00000000000000044 0 \times 00000000000000044
  GNU_STACK
               RW
                                                          10
  GNU_RELRO
               0x00000000001e00 0x0000000000601e00 0x0000000000601e00
               R
                                                          1
 Section to Segment mapping:
  Segment Sections...
  00
  01
         .interp
         .interp .note.ABI-tag .note.qnu.build-id .qnu.hash .dynsym .dynstr .qnu
  02
.version .gnu.version_r .rela.dyn .rela.plt .init .plt .text .fini .rodata .eh_fr
ame hdr .eh frame
  03
         .init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
  04
         .dynamic
         .note.ABI-tag .note.gnu.build-id
  05
         .eh_frame_hdr
  06
  07
         .init_array .fini_array .jcr .dynamic .got
  08
Dynamic section at offset 0x1e18 contains 25 entries:
 Tag
            Type
                                      Name/Value
 0x000000000000001 (NEEDED)
                                      Shared library: [lib361.so]
                                      Shared library: [libc.so.6]
 0x0000000000000001 (NEEDED)
 0x000000000000000 (INIT)
                                      0x400708
 0x000000000000000 (FINI)
                                      0x400d14
 0x0000000000000019 (INIT_ARRAY)
                                      0x601e00
 0x000000000000001b (INIT ARRAYSZ)
                                      8 (bytes)
```

```
0x000000000000001c (FINI ARRAYSZ)
                                         8 (bytes)
 0x000000006ffffef5 (GNU_HASH)
                                         0x400298
 0x0000000000000005 (STRTAB)
                                         0x400498
 0x0000000000000000 (SYMTAB)
                                         0x4002d0
 0x0000000000000000 (STRSZ)
                                         270 (bytes)
 0x0000000000000000 (SYMENT)
                                         24 (bytes)
 0x0000000000000015 (DEBUG)
                                         0x0
 0x0000000000000003 (PLTGOT)
                                         0x602000
 0x0000000000000000 (PLTRELSZ)
                                         240 (bytes)
 0x0000000000000014 (PLTREL)
                                         RELA
 0x0000000000000017 (JMPREL)
                                         0x400618
 0x0000000000000007 (RELA)
                                         0×400600
 0x0000000000000008 (RELASZ)
                                         24 (bytes)
 0x0000000000000000 (RELAENT)
                                         24 (bytes)
 0x000000006ffffffe (VERNEED)
                                         0x4005d0
 0x00000006fffffff (VERNEEDNUM)
                                         1
 0x000000006ffffff0 (VERSYM)
                                         0x4005a6
 0x000000000000000 (NULL)
                                         0x0
Relocation section '.rela.dyn' at offset 0x600 contains 1 entries:
 Offset
                  Info
                                 Type
                                                 Sym. Value
                                                               Sym. Name + Addend
000000601ff8
              000a00000006 R_X86_64_GLOB_DAT 000000000000000 __gmon_start__ + 0
Relocation section '.rela.plt' at offset 0x618 contains 10 entries:
 Offset
                                                 Sym. Value
                                                               Sym. Name + Addend
                  Info
                                 Type
000000602018
              000200000007 R_X86_64_JUMP_SL0 000000000000000 puts + 0
              00030000007 R X86 64 JUMP SL0 000000000000000 secretoperation + 0
000000602020
000000602028
              00040000007 R_X86_64_JUMP_SLO 0000000000000000 strlen + 0
              000500000007 R_X86_64_JUMP_SL0 000000000000000 __stack_chk_fail +
000000602030
000000602038
              00060000007 R X86 64 JUMP SLO 000000000000000 printf + 0
              000700000007 R_X86_64_JUMP_SL0 000000000000000 __assert_fail + 0
000000602040
              000800000007 R X86 64 JUMP SL0 000000000000000 libc start main +
000000602048
0
              00090000007 R X86 64 JUMP SLO 000000000000000 calloc + 0
000000602050
000000602058
              000a0000007 R_X86_64_JUMP_SL0 000000000000000 __gmon_start__ + 0
              000b00000007 R X86 64 JUMP SL0 000000000000000 getlogin r + 0
000000602060
The decoding of unwind sections for machine type Advanced Micro Devices X86-64 is
 not currently supported.
Symbol table '.dynsym' contains 19 entries:
                                                        Ndx Name
   Num:
           Value
                          Size Type
                                       Bind
                                               Vis
     0: 0000000000000000
                             0 NOTYPE
                                       LOCAL
                                              DEFAULT
                                                        UND
     1: 00000000000000000
                             0 NOTYPE
                                       WEAK
                                                        UND _ITM_deregisterTMClone
                                               DEFAULT
Tab
     2: 00000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND puts@GLIBC_2.2.5 (2)
     3: 00000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND secretoperation
                                                        UND strlen@GLIBC 2.2.5 (2)
     4: 0000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
     5: 00000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND __stack_chk_fail@GLIBC
2.4 (3)
     6: 0000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        UND printf@GLIBC 2.2.5 (2)
```

0x601e08

0x000000000000001a (FINI_ARRAY)

```
7: 00000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                       UND __assert_fail@GLIBC_2.
2.5 (2)
                             0 FUNC
                                       GLOBAL DEFAULT
     8: 0000000000000000
                                                       UND __libc_start_main@GLIB
C 2.2.5 (2)
     9: 0000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                       UND calloc@GLIBC_2.2.5 (2)
    10: 00000000000000000
                             0 NOTYPE
                                       WEAK
                                              DEFAULT
                                                       UND __gmon_start__
    11: 0000000000000000
                             0 FUNC
                                       GLOBAL DEFAULT
                                                       UND getlogin_r@GLIBC_2.2.5
 (2)
    12: 00000000000000000
                             0 NOTYPE
                                       WEAK
                                              DEFAULT
                                                        UND _Jv_RegisterClasses
    13: 00000000000000000
                             0 NOTYPE
                                       WEAK
                                              DEFAULT
                                                       UND ITM registerTMCloneTa
ble
                             0 NOTYPE
    14: 000000000060210c
                                       GLOBAL DEFAULT
                                                        24 _edata
    15: 00000000000602110
                             0 NOTYPE
                                       GLOBAL DEFAULT
                                                        25 _end
                                                        25 <u>__</u>bss_start
    16: 000000000060210c
                             0 NOTYPE
                                       GLOBAL DEFAULT
                                                        11 _init
    17: 0000000000400708
                             0 FUNC
                                       GLOBAL DEFAULT
                                                        14 _fini
    18: 0000000000400d14
                             0 FUNC
                                       GLOBAL DEFAULT
Histogram for `.gnu.hash' bucket list length (total of 3 buckets):
 Lenath Number
                    % of total Coverage
      0 0
                    ( 0.0%)
                    (33.3%)
      1 1
                                 20.0%
      2 2
                    ( 66.7%)
                                100.0%
Version symbols section '.gnu.version' contains 19 entries:
 Addr: 0000000004005a6 Offset: 0x0005a6 Link: 5 (.dynsym)
         0 (*local*)
                           0 (*local*)
                                             2 (GLIBC 2.2.5)
  000:
                                                                0 (*local*)
                                                                2 (GLIBC_2.2.5)
  004:
         2 (GLIBC_2.2.5)
                           3 (GLIBC_2.4)
                                             2 (GLIBC_2.2.5)
  008: 2 (GLIBC 2.2.5)
                           2 (GLIBC 2.2.5)
                                                                2 (GLIBC 2.2.5)
                                             0 (*local*)
  00c:
         0 (*local*)
                           0 (*local*)
                                             1 (*qlobal*)
                                                                1 (*global*)
  010:
         1 (*global*)
                           1 (*global*)
                                             1 (*global*)
Version needs section '.gnu.version_r' contains 1 entries:
 Addr: 0x0000000004005d0 Offset: 0x0005d0 Link: 6 (.dynstr)
  000000: Version: 1 File: libc.so.6 Cnt: 2
            Name: GLIBC_2.4 Flags: none Version: 3
  0x0010:
            Name: GLIBC_2.2.5 Flags: none Version: 2
  0x0020:
Displaying notes found at file offset 0x00000254 with length 0x00000020:
  0wner
                        Data size
                                        Description
  GNU
                       0x00000010
                                        NT_GNU_ABI_TAG (ABI version tag)
    OS: Linux, ABI: 2.6.24
Displaying notes found at file offset 0x00000274 with length 0x00000024:
  0wner
                        Data size
                                        Description
  GNU
                       0x00000014
                                        NT_GNU_BUILD_ID (unique build ID bitstrin
q)
    Build ID: 516c99c45c7b1cd513589f91ae029c0f1528d553
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get sum.c:18: main: Assertion `result == 10' failed.
```

```
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ strace ./4
execve("./4", ["./4"], [/* 20 vars */]) = 0
brk(0)
                                        = 0x20aa000
access("/etc/ld.so.nohwcap", F OK)
                                       = -1 ENOENT (No such file or directory)
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e
4977d000
access("/etc/ld.so.preload", R_OK)
                                       = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", 0_RDONLY|0_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=25058, ...}) = 0
mmap(NULL, 25058, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f4e49776000
close(3)
                                        = 0
access("/etc/ld.so.nohwcap", F OK)
                                        = −1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/tls/x86_64/lib361.so", 0_{RDONLY}0_CL0EXEC) = -1 EN0EN
T (No such file or directory)
stat("/lib/x86_64-linux-gnu/tls/x86_64", 0x7ffd788daf10) = -1 EN0ENT (No such fil
e or directory)
open("/lib/x86_64-linux-gnu/tls/lib361.so", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No s
uch file or directory)
stat("/lib/x86~64-linux-qnu/tls", 0x7ffd788daf10) = -1 ENOENT (No such file or di
open("/lib/x86_64-linux-gnu/x86_64/lib361.so", 0_{RDONLY}]0_CL0EXEC) = -1 EN0ENT (N
o such file or directory)
stat("/lib/x86~64-linux-qnu/x86~64", 0x7ffd788daf10) = -1 ENOENT (No such file or
 directory)
open("/lib/x86~64-linux-qnu/lib361.so", 0 RDONLY|0 CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\5\0\0\0\0\0\0\0\0"..., 83
2) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=7868, ...}) = 0
mmap(NULL, 2101304, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f4
e4935b000
mprotect(0x7f4e4935c000, 2093056, PROT NONE) = 0
mmap(0x7f4e4955b000, 8192, PROT READ|PROT WRITE, MAP PRIVATE|MAP FIXED|MAP DENYWR
ITE, 3, 0) = 0x7f4e4955b000
close(3)
                                        = 0
access("/etc/ld.so.nohwcap", F OK)
                                        = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\320\37\2\0\0\0\0\0\"..., 8
32) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=1840928, ...}) = 0
mmap(NULL, 3949248, PROT READ|PROT EXEC, MAP PRIVATE|MAP DENYWRITE, 3, 0) = 0x7f4
e48f96000
mprotect(0x7f4e49151000, 2093056, PROT_NONE) = 0
mmap(0x7f4e49350000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYW
RITE, 3, 0x1ba000) = 0x7f4e49350000
mmap(0x7f4e49356000, 17088, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONY
MOUS, -1, 0) = 0 \times 7f4e49356000
close(3)
                                        = 0
mmap(NULL, 4096, PROT READ|PROT WRITE, MAP PRIVATE|MAP ANONYMOUS, -1, 0) = 0x7f4e
49775000
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e
49773000
arch prctl(ARCH SET FS, 0x7f4e49773740) = 0
```

```
mprotect(0x7f4e49350000, 16384, PROT_READ) = 0
mprotect(0x7f4e4955b000, 4096, PROT READ) = 0
mprotect(0x601000, 4096, PROT_READ)
mprotect(0x7f4e4977f000, 4096, PROT READ) = 0
munmap(0x7f4e49776000, 25058)
fstat(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e
4977c000
write(1, "this program tests the implement"..., 71this program tests the implemen
tation of a dynamically linked library.
) = 71
brk(0)
                                        = 0x20aa000
brk(0x20cb000)
                                        = 0x20cb000
write(2, "4: get_sum.c:18: main: Assertion"..., 564: get_sum.c:18: main: Assertio
n `result == 10' failed.
) = 56
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e
rt sigprocmask(SIG UNBLOCK, [ABRT], NULL, 8) = 0
                                        = 23254
qettid()
tgkill(23254, 23254, SIGABRT)
                                        = 0
--- SIGABRT {si_signo=SIGABRT, si_code=SI_TKILL, si_pid=23254, si_uid=1000} ---
+++ killed by SIGABRT (core dumped) +++
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -d 4
4:
       file format elf64-x86-64
Disassembly of section .init:
0000000000400708 < init>:
  400708:
                48 83 ec 08
                                        sub
                                               $0x8,%rsp
  40070c:
                48 8b 05 e5 18 20 00
                                               0x2018e5(%rip),%rax
                                                                          # 601ff
                                        mov
8 < fini+0x2012e4 >
               48 85 c0
  400713:
                                        test
                                               %rax,%rax
  400716:
                74 05
                                               40071d <_init+0x15>
                                        jе
                                               4007c0 <__gmon_start__@plt>
  400718:
                e8 a3 00 00 00
                                        callq
                48 83 c4 08
  40071d:
                                        add
                                               $0x8,%rsp
  400721:
                c3
                                        retq
Disassembly of section .plt:
0000000000400730 <puts@plt-0x10>:
  400730:
                ff 35 d2 18 20 00
                                        pushq 0x2018d2(%rip)
                                                                      # 602008 < f
ini+0x2012f4>
  400736:
               ff 25 d4 18 20 00
                                        jmpq
                                               *0x2018d4(%rip)
                                                                      # 602010 <
fini+0x2012fc>
  40073c:
                0f 1f 40 00
                                        laon
                                               0x0(%rax)
0000000000400740 <puts@plt>:
               ff 25 d2 18 20 00
                                                                      # 602018 <_
  400740:
                                        jmpq
                                               *0x2018d2(%rip)
fini+0x201304>
```

400746:	68 0					pushq	\$0×0	
40074b:	e9 e	0 ff	ff	ff		jmpq	400730 <_init+0x28>	
000000000040075			•				. 0 2010 (0)	# C02020 .
400750:	ff 2	5 ca	18	20	00	jmpq	*0x2018ca(%rip)	# 602020 <_
fini+0x20130c> 400756:	68 0	1 00	aa	aa		pushq	\$0×1	
40075b:	e9 d					jmpq	400730 <_init+0x28>	
1007301	cs u	•	• •	• •		Jiiipq	100750 <u>111111</u>	
000000000040076	0 <st< td=""><td>rlen</td><td>@pl</td><td>t>:</td><td></td><td></td><td></td><td></td></st<>	rlen	@pl	t>:				
400760:	ff 2		-		00	jmpq	*0x2018c2(%rip)	# 602028 <_
fini+0x201314>								
400766:	68 0					pushq	\$0×2	
40076b:	e9 c	0 ff	ff	ff		jmpq	400730 <_init+0x28>	
	_							
000000000040077		-	_				. 0. 20101 (0. 1.)	" 602020
400770:	ff 2	5 ba	18	20	00	jmpq	*0x2018ba(%rip)	# 602030 <_
fini+0x20131c> 400776:	68 0	2 00	aa	aa		nucha	\$0x3	
400776: 40077b:	e9 b					pushq jmpq	400730 <_init+0x28>	
400775.	C9 D	0 11				Jiiibd	400730 _1111(+0\20>	
000000000040078	0 <pr< td=""><td>intf</td><td>an l</td><td>t>:</td><td></td><td></td><td></td><td></td></pr<>	intf	an l	t>:				
	ff 2				00	jmpq	*0x2018b2(%rip)	# 602038 <_
fini+0x201324>						5		_
400786:	68 0	4 00	00	00		pushq	\$0×4	
40078b:	e9 a	0 ff	ff	ff		jmpq	400730 <_init+0x28>	
	_							
000000000040079		-	_					
400790:	ff 2	5 aa	18	20	00	jmpq	*0x2018aa(%rip)	# 602040 <_
fini+0x20132c> 400796:	68 0	E 00	00	00		nucha	# Ove	
400790: 40079b:	e9 9					pushq jmpq	<pre>\$0x5 400730 <_init+0x28></pre>	
400790.	69 9	0 11		11		Jiiibd	400/30 _11111+0\20>	
00000000004007a	0 <	libo	st	art	main@plt:	>:		
4007a0:	ff 2				-	jmpq	*0x2018a2(%rip)	# 602048 <_
fini+0x201334>						5		_
4007a6:	68 0	6 00	00	00		pushq	\$0×6	
4007ab:	e9 8	0 ff	ff	ff		jmpq	400730 <_init+0x28>	
00000000004007b								
4007b0:	ff 2	5 9a	18	20	00	jmpq	*0x20189a(%rip)	# 602050 <_
fini+0x20133c> 4007b6:	60 0	7 00	00	00		nucha	¢0×7	
4007bb:	68 0					pushq jmpq	<pre>\$0x7 400730 <_init+0x28></pre>	
400700.	E9 /	וו ש	11	11		Jiiibd	400/30 <_11111+00028>	
0000000004007c0 <gmon_start@plt>:</gmon_start@plt>								
4007c0:	ff 2					jmpq	*0x201892(%rip)	# 602058 <_
fini+0x201344>				- •		J 15 41		_
4007c6:	68 0	8 00	00	00		pushq	\$0×8	
4007cb:	e9 6	0 ff	ff	ff		jmpq .	400730 <_init+0x28>	
000000000040070	_	_	_			_		
4007d0:	ff 2	5 8a	18	20	00	jmpq	*0x20188a(%rip)	# 602060 <_
.00,401								

```
fini+0x20134c>
  4007d6:
                 68 09 00 00 00
                                           pushq
                                                   $0x9
  4007db:
                 e9 50 ff ff ff
                                           jmpq
                                                   400730 <_init+0x28>
Disassembly of section .text:
00000000004007e0 <.text>:
  4007e0:
                 31 ed
                                                   %ebp,%ebp
                                           xor
  4007e2:
                 49 89 d1
                                                   %rdx,%r9
                                           mov
                 5e
  4007e5:
                                                   %rsi
                                           pop
  4007e6:
                 48 89 e2
                                           mov
                                                   %rsp,%rdx
  4007e9:
                 48 83 e4 f0
                                           and
                                                   $0xffffffffffffff,%rsp
  4007ed:
                 50
                                           push
                                                   %rax
  4007ee:
                 54
                                                   %rsp
                                           push
  4007ef:
                 49 c7 c0 10 0d 40 00
                                                   $0x400d10,%r8
                                           mov
  4007f6:
                 48 c7 c1 a0 0c 40 00
                                           mov
                                                   $0x400ca0,%rcx
  4007fd:
                 48 c7 c7 cd 08 40 00
                                           mov
                                                   $0x4008cd,%rdi
                 e8 97 ff ff ff
  400804:
                                           callq
                                                   4007a0 <__libc_start_main@plt>
  400809:
                 f4
                                           hlt
                 66 0f 1f 44 00 00
  40080a:
                                           nopw
                                                   0x0(%rax,%rax,1)
                 b8 17 21 60 00
  400810:
                                           mov
                                                   $0x602117,%eax
                 55
  400815:
                                           push
                                                   %rbp
                 48 2d 10 21 60 00
  400816:
                                           sub
                                                   $0x602110,%rax
  40081c:
                 48 83 f8 0e
                                           cmp
                                                   $0xe,%rax
                 48 89 e5
  400820:
                                           mov
                                                   %rsp,%rbp
                 77 02
                                                   400827 <getlogin r@plt+0x57>
  400823:
                                           jа
  400825:
                 5d
                                                   %rbp
                                           pop
  400826:
                 с3
                                           retq
  400827:
                 b8 00 00 00 00
                                                   $0x0,%eax
                                           mov
                 48 85 c0
  40082c:
                                           test
                                                   %rax,%rax
  40082f:
                 74 f4
                                                   400825 <getlogin_r@plt+0x55>
                                           jе
  400831:
                 5d
                                           pop
                                                   %rbp
                                                   $0x602110,%edi
  400832:
                 bf 10 21 60 00
                                           mov
                                                   *%rax
  400837:
                 ff e0
                                           jmpq
  400839:
                 0f 1f 80 00 00 00 00
                                           nopl
                                                   0x0(%rax)
  400840:
                 b8 10 21 60 00
                                                   $0x602110,%eax
                                           mov
  400845:
                 55
                                           push
                                                   %rbp
                 48 2d 10 21 60 00
  400846:
                                                   $0x602110,%rax
                                           sub
  40084c:
                 48 c1 f8 03
                                                   $0x3,%rax
                                           sar
                 48 89 e5
  400850:
                                                   %rsp,%rbp
                                           mov
  400853:
                 48 89 c2
                                           mov
                                                   %rax,%rdx
                 48 c1 ea 3f
  400856:
                                                   $0x3f,%rdx
                                           shr
  40085a:
                 48 01 d0
                                           add
                                                   %rdx,%rax
```

sar

ine

pop

mov

jе

pop

mov

mov

retq

test

%rax

%rbp

%rbp

\$0x0,%edx

%rdx,%rdx

%rax,%rsi

\$0x602110,%edi

400864 <getlogin_r@plt+0x94>

400862 <getlogin_r@plt+0x92>

40085d:

400860:

400862:

400863:

400864:

400869:

40086c:

40086e:

40086f:

400872:

48 d1 f8

48 85 d2

48 89 c6

74 f4

ba 00 00 00 00

bf 10 21 60 00

75 02

5d

с3

5d

```
400877:
                 ff e2
                                                  *%rdx
                                           jmpq
                 0f 1f 80 00 00 00 00
  400879:
                                           nopl
                                                  0x0(%rax)
                 80 3d 85 18 20 00 00
  400880:
                                           cmpb
                                                  $0x0,0x201885(%rip)
                                                                               # 60210
c < edata>
  400887:
                 75 11
                                                  40089a <getlogin_r@plt+0xca>
                                           jne
  400889:
                 55
                                                  %rbp
                                           push
  40088a:
                 48 89 e5
                                                  %rsp,%rbp
                                           mov
                 e8 7e ff ff ff
  40088d:
                                           callq
                                                  400810 <getlogin_r@plt+0x40>
  400892:
                 5d
                                                  %rbp
                                           pop
  400893:
                 c6 05 72 18 20 00 01
                                                  $0x1,0x201872(%rip)
                                           movb
                                                                               # 60210
c <_edata>
  40089a:
                 f3 c3
                                           repz retq
  40089c:
                 0f 1f 40 00
                                           nopl
                                                  0x0(%rax)
  4008a0:
                 48 83 3d 68 15 20 00
                                                  $0x0,0x201568(%rip)
                                                                               # 601e1
                                           cmpq
0 < fini+0x2010fc>
  4008a7:
                 00
  4008a8:
                 74 1e
                                           jе
                                                  4008c8 <getlogin_r@plt+0xf8>
  4008aa:
                 b8 00 00 00 00
                                           mov
                                                  $0x0,%eax
  4008af:
                 48 85 c0
                                           test
                                                  %rax,%rax
                                                  4008c8 <getlogin_r@plt+0xf8>
                 74 14
  4008b2:
                                           iе
                 55
  4008b4:
                                           push
                 bf 10 1e 60 00
                                                  $0x601e10,%edi
  4008b5:
                                           mov
                 48 89 e5
  4008ba:
                                           mov
                                                  %rsp,%rbp
                 ff d0
  4008bd:
                                           callq
                                                  *%rax
                 5d
  4008bf:
                                           pop
                                                  %rbp
                 e9 7b ff ff ff
                                                  400840 <getlogin r@plt+0x70>
  4008c0:
                                           jmpq
  4008c5:
                 0f 1f 00
                                           nopl
                                                  (%rax)
                 e9 73 ff ff ff
  4008c8:
                                                  400840 < \text{getlogin r@plt+0x70}
                                           jmpq
  4008cd:
                 55
                                                  %rbp
                                           push
                 48 89 e5
                                                  %rsp,%rbp
  4008ce:
                                           mov
  4008d1:
                 48 83 ec 10
                                           sub
                                                  $0x10,%rsp
  4008d5:
                 c7 45 f4 01 00 00 00
                                           movl
                                                  $0x1,-0xc(%rbp)
                                                  $0x2.-0x8(%rbp)
  4008dc:
                 c7 45 f8 02 00 00 00
                                           movl
  4008e3:
                 c7 45 fc 00 00 00 00
                                           movl
                                                  $0x0,-0x4(%rbp)
                 bf 70 0d 40 00
  4008ea:
                                           mov
                                                  $0x400d70,%edi
                 e8 4c fe ff ff
  4008ef:
                                           callq
                                                  400740 <puts@plt>
  4008f4:
                 be 06 00 00 00
                                           mov
                                                  $0x6,%esi
                 bf 03 00 00 00
  4008f9:
                                           mov
                                                  $0x3,%edi
  4008fe:
                 e8 4d fe ff ff
                                           callq
                                                  400750 <secretoperation@plt>
                 89 45 fc
                                                  %eax,-0x4(%rbp)
  400903:
                                           mov
                 83 7d fc 0a
  400906:
                                           cmpl
                                                  $0xa,-0x4(%rbp)
                 74 19
  40090a:
                                                  400925 <getlogin_r@plt+0x155>
                                           jе
                 b9 da 0d 40 00
  40090c:
                                           mov
                                                  $0x400dda,%ecx
  400911:
                 ba 12 00 00 00
                                           mov
                                                  $0x12,%edx
  400916:
                 be b7 0d 40 00
                                           mov
                                                  $0x400db7,%esi
                 bf c1 0d 40 00
                                                  $0x400dc1,%edi
  40091b:
                                           mov
                                                  400790 <__assert_fail@plt>
  400920:
                 e8 6b fe ff ff
                                           callq
                                                  -0x8(%rbp),%edx
                 8b 55 f8
  400925:
                                           mov
  400928:
                 8b 45 f4
                                           mov
                                                  -0xc(%rbp),%eax
                 89 d6
  40092b:
                                           mov
                                                  %edx,%esi
  40092d:
                 89 c7
                                           mov
                                                  %eax,%edi
  40092f:
                 e8 1c fe ff ff
                                                  400750 <secretoperation@plt>
                                           callq
                 89 45 fc
  400934:
                                           mov
                                                  %eax,-0x4(%rbp)
```

```
400937:
                 83 7d fc 04
                                                  $0x4,-0x4(%rbp)
                                          cmpl
                 74 19
  40093b:
                                                  400956 < qetlogin r@plt+0x186>
                                          jе
                 b9 da 0d 40 00
  40093d:
                                          mov
                                                  $0x400dda,%ecx
                 ba 14 00 00 00
                                                  $0x14,%edx
  400942:
                                          mov
                 be b7 0d 40 00
                                                  $0x400db7,%esi
  400947:
                                          mov
                 bf ce 0d 40 00
                                                  $0x400dce,%edi
  40094c:
                                          mov
  400951:
                 e8 3a fe ff ff
                                                  400790 <__assert_fail@plt>
                                          callq
                 48 8b 05 33 17 20 00
                                                  0x201733(%rip),%rax
  400956:
                                                                               # 60209
                                          mov
0 <_fini+0x20137c>
                 48 89 c7
  40095d:
                                                  %rax,%rdi
                                          mov
  400960:
                 e8 28 00 00 00
                                          callq
                                                  40098d <getlogin_r@plt+0x1bd>
  400965:
                 48 89 c2
                                                  %rax,%rdx
                                          mov
  400968:
                 48 8b 0d 31 17 20 00
                                                  0x201731(%rip),%rcx
                                          mov
                                                                               # 6020a
0 <_fini+0x20138c>
  40096f:
                48 8b 05 22 17 20 00
                                                  0x201722(%rip),%rax
                                                                               # 60209
                                          mov
8 <_fini+0x201384>
  400976:
                 48 89 ce
                                                  %rcx,%rsi
                                          mov
                                                  %rax,%rdi
  400979:
                 48 89 c7
                                          mov
  40097c:
                 b8 00 00 00 00
                                          mov
                                                  $0x0,%eax
                 e8 fa fd ff ff
                                                  400780 <printf@plt>
  400981:
                                          callq
                 b8 00 00 00 00
  400986:
                                          mov
                                                  $0x0,%eax
  40098b:
                 c9
                                          leaveq
                 с3
  40098c:
                                          retq
  40098d:
                 55
                                          push
                                                  %rbp
  40098e:
                 48 89 e5
                                                  %rsp,%rbp
                                          mov
                 53
  400991:
                                          push
                                                  %rbx
  400992:
                 48 81 ec 38 04 00 00
                                          sub
                                                  $0x438,%rsp
                 48 89 bd c8 fb ff ff
                                                  %rdi,-0x438(%rbp)
  400999:
                                          mov
  4009a0:
                 64 48 8b 04 25 28 00
                                                  %fs:0x28,%rax
                                          mov
                 00 00
  4009a7:
  4009a9:
                 48 89 45 e8
                                                  %rax,-0x18(%rbp)
                                          mov
  4009ad:
                 31 c0
                                          xor
                                                  %eax,%eax
                                                  -0x420(%rbp),%rax
  4009af:
                 48 8d 85 e0 fb ff ff
                                          lea
  4009b6:
                 be 00 04 00 00
                                                  $0x400,%esi
                                          mov
  4009bb:
                 48 89 c7
                                          mov
                                                  %rax,%rdi
                 e8 0d fe ff ff
  4009be:
                                          callq
                                                  4007d0 <getlogin_r@plt>
  4009c3:
                 c7 85 d4 fb ff ff 00
                                          movl
                                                  $0x0,-0x42c(%rbp)
                 00 00 00
  4009ca:
  4009cd:
                 eb 3e
                                                  400a0d <getlogin_r@plt+0x23d>
                                          jmp
                 8b 85 d4 fb ff ff
                                                  -0x42c(%rbp),%eax
  4009cf:
                                          mov
  4009d5:
                 48 98
                                          cltq
  4009d7:
                 0f b6 94 05 e0 fb ff
                                          movzbl -0x420(%rbp,%rax,1),%edx
  4009de:
                 ff
                 8b 85 d4 fb ff ff
  4009df:
                                          mov
                                                  -0x42c(%rbp),%eax
  4009e5:
                 48 63 c8
                                          movslq %eax,%rcx
                 48 8b 85 c8 fb ff ff
  4009e8:
                                          mov
                                                  -0x438(%rbp),%rax
  4009ef:
                 48 01 c8
                                          add
                                                  %rcx,%rax
                 0f b6 00
                                          movzbl (%rax),%eax
  4009f2:
  4009f5:
                 31 c2
                                          xor
                                                  %eax,%edx
                 8b 85 d4 fb ff ff
  4009f7:
                                          mov
                                                  -0x42c(%rbp),%eax
  4009fd:
                 48 98
                                          cltq
                 88 94 05 e0 fb ff ff
  4009ff:
                                                  %dl,-0x420(%rbp,%rax,1)
                                          mov
  400a06:
                 83 85 d4 fb ff ff 01
                                          addl
                                                  $0x1,-0x42c(%rbp)
```

```
400a0d:
               8b 85 d4 fb ff ff
                                                -0x42c(%rbp),%eax
                                        mov
               48 63 d8
400a13:
                                        movslq %eax,%rbx
               48 8d 85 e0 fb ff ff
400a16:
                                        lea
                                                -0x420(%rbp),%rax
               48 89 c7
400a1d:
                                        mov
                                                %rax,%rdi
               e8 3b fd ff ff
                                        callq
                                                400760 <strlen@plt>
400a20:
               48 39 c3
                                                %rax,%rbx
400a25:
                                        cmp
400a28:
               72 a5
                                        jb
                                                4009cf <getlogin_r@plt+0x1ff>
               8b 85 d4 fb ff ff
400a2a:
                                        mov
                                                -0x42c(%rbp),%eax
400a30:
               48 63 c8
                                        movslq %eax,%rcx
               48 8d 95 d8 fb ff ff
400a33:
                                        lea
                                                -0x428(%rbp),%rdx
400a3a:
               48 8d 85 e0 fb ff ff
                                        lea
                                                -0x420(%rbp),%rax
400a41:
               48 89 ce
                                                %rcx,%rsi
                                        mov
400a44:
              48 89 c7
                                                %rax,%rdi
                                        mov
400a47:
              e8 1e 00 00 00
                                               400a6a <getlogin_r@plt+0x29a>
                                        callq
400a4c:
              48 8b 75 e8
                                        mov
                                                -0x18(%rbp),%rsi
               64 48 33 34 25 28 00
400a50:
                                        xor
                                                %fs:0x28,%rsi
400a57:
               00 00
               74 05
400a59:
                                                400a60 <getlogin_r@plt+0x290>
                                        jе
400a5b:
               e8 10 fd ff ff
                                        callq
                                                400770 <__stack_chk_fail@plt>
               48 81 c4 38 04 00 00
400a60:
                                        add
                                                $0x438,%rsp
               5b
                                                %rbx
400a67:
                                        pop
              5d
                                                %rbp
400a68:
                                        pop
               с3
400a69:
                                        retq
400a6a:
               55
                                        push
                                                %rbp
400a6b:
               48 89 e5
                                                %rsp,%rbp
                                        mov
               48 83 ec 40
                                                $0x40,%rsp
400a6e:
                                        sub
400a72:
               48 89 7d d8
                                                %rdi,-0x28(%rbp)
                                        mov
               48 89 75 d0
                                                %rsi,-0x30(%rbp)
400a76:
                                        mov
400a7a:
              48 89 55 c8
                                                %rdx,-0x38(%rbp)
                                        mov
               48 8b 45 d0
                                                -0x30(%rbp),%rax
400a7e:
                                        mov
400a82:
              48 83 c0 02
                                        add
                                                $0x2,%rax
400a86:
               48 ba ab aa aa aa
                                        movabs $0xaaaaaaaaaaaaaab,%rdx
400a8d:
               aa aa aa
400a90:
               48 f7 e2
                                        mul
                                                %rdx
400a93:
               48 89 d0
                                        mov
                                                %rdx,%rax
400a96:
               48 d1 e8
                                        shr
                                                %rax
400a99:
               48 8d 14 85 00 00 00
                                        lea
                                                0x0(,%rax,4),%rdx
               00
400aa0:
400aa1:
              48 8b 45 c8
                                                -0x38(%rbp),%rax
                                        mov
               48 89 10
                                                %rdx,(%rax)
400aa5:
                                        mov
400aa8:
              48 8b 45 c8
                                        mov
                                                -0x38(%rbp),%rax
400aac:
              48 8b 00
                                                (%rax),%rax
                                        mov
              be 01 00 00 00
400aaf:
                                        mov
                                                $0x1,%esi
              48 89 c7
                                        mov
                                                %rax,%rdi
400ab4:
                                                4007b0 <calloc@plt>
400ab7:
               e8 f4 fc ff ff
                                        callq
                                                %rax,-0x8(%rbp)
              48 89 45 f8
400abc:
                                        mov
400ac0:
              48 83 7d f8 00
                                        cmpq
                                                $0x0,-0x8(%rbp)
                                                400ad1 <getlogin_r@plt+0x301>
               75 0a
400ac5:
                                        jne
400ac7:
              b8 00 00 00 00
                                        mov
                                                $0x0.%eax
400acc:
               e9 c0 01 00 00
                                        jmpq
                                                400c91 <getlogin_r@plt+0x4c1>
400ad1:
               c7 45 e0 00 00 00 00
                                        movl
                                                $0x0,-0x20(%rbp)
                                                $0x0,-0x1c(%rbp)
400ad8:
               c7 45 e4 00 00 00 00
                                        movl
                                                400c1f <getlogin_r@plt+0x44f>
400adf:
               e9 3b 01 00 00
                                        jmpq
```

```
400ae4:
               8b 45 e0
                                                -0x20(%rbp),%eax
                                        mov
               48 98
400ae7:
                                        cltq
              48 3b 45 d0
400ae9:
                                        cmp
                                                -0x30(%rbp),%rax
              73 1b
400aed:
                                        jae
                                                400b0a <getlogin r@plt+0x33a>
              8b 45 e0
                                                -0x20(%rbp),%eax
400aef:
                                        mov
              8d 50 01
                                                0x1(%rax),%edx
400af2:
                                        lea
400af5:
              89 55 e0
                                                %edx,-0x20(%rbp)
                                        mov
              48 63 d0
400af8:
                                        movslq %eax,%rdx
400afb:
              48 8b 45 d8
                                        mov
                                                -0x28(%rbp),%rax
              48 01 d0
400aff:
                                        add
                                                %rdx,%rax
400b02:
              0f b6 00
                                        movzbl (%rax),%eax
400b05:
              0f b6 c0
                                        movzbl %al,%eax
400b08:
              eb 05
                                                400b0f <getlogin_r@plt+0x33f>
                                        jmp
400b0a:
              b8 00 00 00 00
                                                $0x0,%eax
                                        mov
400b0f:
              89 45 e8
                                                %eax,-0x18(%rbp)
                                        mov
400b12:
              8b 45 e0
                                        mov
                                                -0x20(%rbp),%eax
400b15:
              48 98
                                        cltq
              48 3b 45 d0
400b17:
                                                -0x30(%rbp),%rax
                                        cmp
400b1b:
              73 1b
                                        jae
                                                400b38 <getlogin_r@plt+0x368>
                                                -0x20(%rbp),%eax
400b1d:
              8b 45 e0
                                        mov
              8d 50 01
                                                0x1(%rax),%edx
400b20:
                                        lea
              89 55 e0
                                                %edx,-0x20(%rbp)
400b23:
                                        mov
              48 63 d0
                                        movslq %eax,%rdx
400b26:
400b29:
              48 8b 45 d8
                                        mov
                                                -0x28(%rbp),%rax
400b2d:
              48 01 d0
                                        add
                                                %rdx,%rax
              0f b6 00
                                        movzbl (%rax),%eax
400b30:
400b33:
              0f b6 c0
                                        movzbl %al,%eax
400b36:
              eb 05
                                                400b3d <getlogin r@plt+0x36d>
                                        jmp
400b38:
              b8 00 00 00 00
                                                $0x0,%eax
                                        mov
              89 45 ec
                                                %eax,-0x14(%rbp)
400b3d:
                                        mov
400b40:
              8b 45 e0
                                                -0x20(%rbp),%eax
                                        mov
400b43:
              48 98
                                        cltq
              48 3b 45 d0
400b45:
                                        cmp
                                                -0x30(%rbp),%rax
400b49:
              73 1b
                                                400b66 <getlogin_r@plt+0x396>
                                        jae
400b4b:
              8b 45 e0
                                        mov
                                                -0x20(%rbp),%eax
              8d 50 01
400b4e:
                                        lea
                                                0x1(%rax),%edx
400b51:
              89 55 e0
                                        mov
                                                %edx,-0x20(%rbp)
              48 63 d0
400b54:
                                        movslq %eax,%rdx
400b57:
              48 8b 45 d8
                                                -0x28(%rbp),%rax
                                        mov
              48 01 d0
                                                %rdx,%rax
400b5b:
                                        add
400b5e:
              0f b6 00
                                        movzbl (%rax),%eax
400b61:
              0f b6 c0
                                        movzbl %al,%eax
400b64:
              eb 05
                                        jmp
                                                400b6b <getlogin_r@plt+0x39b>
400b66:
              b8 00 00 00 00
                                                $0x0,%eax
                                        mov
400b6b:
              89 45 f0
                                        mov
                                                %eax,-0x10(%rbp)
              8b 45 e8
400b6e:
                                        mov
                                                -0x18(%rbp),%eax
400b71:
              c1 e0 10
                                        shl
                                                $0x10,%eax
               89 c2
                                                %eax,%edx
400b74:
                                        mov
400b76:
              8b 45 ec
                                        mov
                                                -0x14(%rbp),%eax
400b79:
               c1 e0 08
                                        shl
                                                $0x8,%eax
400b7c:
               01 c2
                                        add
                                                %eax,%edx
                                                -0x10(%rbp),%eax
400b7e:
               8b 45 f0
                                        mov
400b81:
               01 d0
                                        add
                                                %edx,%eax
```

```
400b83:
               89 45 f4
                                                 %eax,-0xc(%rbp)
                                         mov
                                                 -0x1c(%rbp),%eax
               8b 45 e4
400b86:
                                         mov
400b89:
               8d 50 01
                                         lea
                                                 0x1(%rax),%edx
               89 55 e4
                                                 %edx,-0x1c(%rbp)
400b8c:
                                         mov
               48 63 d0
                                         movslq %eax,%rdx
400b8f:
               48 8b 45 f8
400b92:
                                                 -0x8(%rbp),%rax
                                         mov
               48 01 c2
400b96:
                                                 %rax,%rdx
                                         add
400b99:
               8b 45 f4
                                                 -0xc(%rbp),%eax
                                         mov
400b9c:
               c1 e8 12
                                         shr
                                                 $0x12,%eax
               83 e0 3f
400b9f:
                                                 $0x3f,%eax
                                         and
400ba2:
               89 c0
                                         mov
                                                 %eax,%eax
               0f b6 80 c0 20 60 00
400ba4:
                                         movzbl 0x6020c0(%rax),%eax
               88 02
                                                 %al,(%rdx)
400bab:
                                         mov
               8b 45 e4
                                                 -0x1c(%rbp),%eax
400bad:
                                         mov
400bb0:
               8d 50 01
                                                 0x1(%rax),%edx
                                         lea
                                                 %edx,-0x1c(%rbp)
400bb3:
               89 55 e4
                                         mov
400bb6:
               48 63 d0
                                         movslq %eax,%rdx
400bb9:
               48 8b 45 f8
                                                 -0x8(%rbp),%rax
                                         mov
400bbd:
               48 01 c2
                                         add
                                                 %rax,%rdx
400bc0:
               8b 45 f4
                                                 -0xc(%rbp),%eax
                                         mov
400bc3:
               c1 e8 0c
                                         shr
                                                 $0xc,%eax
400bc6:
               83 e0 3f
                                         and
                                                 $0x3f,%eax
               89 c0
400bc9:
                                         mov
                                                 %eax,%eax
400bcb:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400bd2:
               88 02
                                                 %al,(%rdx)
                                         mov
               8b 45 e4
                                                 -0x1c(%rbp),%eax
400bd4:
                                         mov
400bd7:
               8d 50 01
                                                 0x1(%rax),%edx
                                         lea
               89 55 e4
                                                 %edx_{\bullet}-0x1c(%rbp)
400bda:
                                         mov
400bdd:
               48 63 d0
                                         movslq %eax,%rdx
               48 8b 45 f8
                                                 -0x8(%rbp),%rax
400be0:
                                         mov
400be4:
               48 01 c2
                                                 %rax,%rdx
                                         add
400be7:
               8b 45 f4
                                                 -0xc(%rbp),%eax
                                         mov
400bea:
               c1 e8 06
                                         shr
                                                 $0x6,%eax
               83 e0 3f
400bed:
                                                 $0x3f,%eax
                                         and
400bf0:
               89 c0
                                                 %eax,%eax
                                         mov
                                         movzbl 0x6020c0(%rax),%eax
400bf2:
               0f b6 80 c0 20 60 00
400bf9:
               88 02
                                         mov
                                                 %al,(%rdx)
               8b 45 e4
400bfb:
                                                 -0x1c(%rbp),%eax
                                         mov
400bfe:
               8d 50 01
                                         lea
                                                 0x1(%rax),%edx
               89 55 e4
                                                 %edx,-0x1c(%rbp)
400c01:
                                         mov
400c04:
               48 63 d0
                                         movslq %eax,%rdx
               48 8b 45 f8
                                                 -0x8(%rbp),%rax
400c07:
                                         mov
400c0b:
               48 01 c2
                                         add
                                                 %rax,%rdx
400c0e:
               8b 45 f4
                                                 -0xc(%rbp),%eax
                                         mov
400c11:
               83 e0 3f
                                         and
                                                 $0x3f,%eax
               89 c0
400c14:
                                         mov
                                                 %eax,%eax
400c16:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400c1d:
               88 02
                                         mov
                                                 %al,(%rdx)
400c1f:
               8b 45 e0
                                         mov
                                                 -0x20(%rbp),%eax
400c22:
               48 98
                                         cltq
400c24:
               48 3b 45 d0
                                         cmp
                                                 -0x30(%rbp),%rax
               0f 82 b6 fe ff ff
                                                 400ae4 <getlogin_r@plt+0x314>
400c28:
                                         ib
400c2e:
               c7 45 e0 00 00 00 00
                                         movl
                                                 $0x0,-0x20(%rbp)
```

```
400c35:
                 eb 24
                                                  400c5b <getlogin_r@plt+0x48b>
                                          jmp
                 48 8b 45 c8
  400c37:
                                                  -0x38(%rbp),%rax
                                          mov
  400c3b:
                 48 8b 10
                                          mov
                                                  (%rax),%rdx
                8b 45 e0
  400c3e:
                                                  -0x20(%rbp),%eax
                                          mov
                 48 98
                                          cltq
  400c41:
                 48 29 c2
  400c43:
                                          sub
                                                  %rax,%rdx
  400c46:
                 48 89 d0
                                                  %rdx,%rax
                                          mov
                 48 8d 50 ff
                                                  -0x1(%rax),%rdx
  400c49:
                                          lea
  400c4d:
                48 8b 45 f8
                                          mov
                                                  -0x8(%rbp),%rax
                48 01 d0
  400c51:
                                          add
                                                  %rdx,%rax
  400c54:
                 c6 00 3d
                                          movb
                                                  $0x3d,(%rax)
  400c57:
                83 45 e0 01
                                          addl
                                                  $0x1,-0x20(%rbp)
  400c5b:
                48 8b 4d d0
                                                  -0x30(%rbp),%rcx
                                          mov
  400c5f:
                48 ba ab aa aa aa
                                          movabs $0xaaaaaaaaaaaaaab,%rdx
  400c66:
                 aa aa aa
  400c69:
                 48 89 c8
                                          mov
                                                  %rcx,%rax
  400c6c:
                 48 f7 e2
                                          mul
                                                  %rdx
  400c6f:
                48 d1 ea
                                          shr
                                                  %rdx
  400c72:
                 48 89 d0
                                          mov
                                                  %rdx,%rax
                48 01 c0
  400c75:
                                          add
                                                  %rax,%rax
                48 01 d0
  400c78:
                                          add
                                                  %rdx,%rax
                                                  %rax,%rcx
                48 29 c1
  400c7b:
                                          sub
                 48 89 ca
                                                  %rcx,%rdx
  400c7e:
                                          mov
  400c81:
                 8b 04 95 00 21 60 00
                                                  0x602100(,%rdx,4),%eax
                                          mov
                 3b 45 e0
  400c88:
                                          cmp
                                                  -0x20(%rbp),%eax
                 7f aa
                                                  400c37 <getlogin r@plt+0x467>
  400c8b:
                                          jg
  400c8d:
                 48 8b 45 f8
                                          mov
                                                  -0x8(%rbp),%rax
                 с9
  400c91:
                                          leaveg
  400c92:
                 с3
                                          retq
                 66 2e 0f 1f 84 00 00
  400c93:
                                          nopw
                                                  %cs:0x0(%rax,%rax,1)
  400c9a:
                 00 00 00
  400c9d:
                 0f 1f 00
                                          nopl
                                                  (%rax)
  400ca0:
                 41 57
                                          push
                                                  %r15
  400ca2:
                41 89 ff
                                                  %edi,%r15d
                                          mov
  400ca5:
                 41 56
                                          push
                                                  %r14
                 49 89 f6
  400ca7:
                                                  %rsi,%r14
                                          mov
  400caa:
                 41 55
                                          push
                                                  %r13
                49 89 d5
                                                  %rdx,%r13
  400cac:
                                          mov
  400caf:
                 41 54
                                          push
                                                  %r12
                 4c 8d 25 48 11 20 00
  400cb1:
                                          lea
                                                  0x201148(%rip),%r12
                                                                               # 601e0
0 < fini+0x2010ec>
  400cb8:
                                          push
                 48 8d 2d 48 11 20 00
  400cb9:
                                          lea
                                                  0x201148(%rip),%rbp
                                                                               # 601e0
8 <_fini+0x2010f4>
  400cc0:
                                          push
                                                  %rbx
                 4c 29 e5
                                                  %r12,%rbp
  400cc1:
                                          sub
  400cc4:
                31 db
                                          xor
                                                  %ebx,%ebx
                48 c1 fd 03
                                                  $0x3,%rbp
  400cc6:
                                          sar
  400cca:
                 48 83 ec 08
                                          sub
                                                  $0x8,%rsp
                 e8 35 fa ff ff
  400cce:
                                          callq
                                                  400708 <_init>
  400cd3:
                 48 85 ed
                                          test
                                                  %rbp,%rbp
                 74 1e
                                                  400cf6 <getlogin_r@plt+0x526>
  400cd6:
                                          iе
                 0f 1f 84 00 00 00 00
  400cd8:
                                          nopl
                                                  0x0(%rax,%rax,1)
```

```
400cdf:
                4c 89 ea
  400ce0:
                                               %r13,%rdx
                                        mov
                4c 89 f6
                                               %r14,%rsi
  400ce3:
                                        mov
                44 89 ff
                                               %r15d,%edi
  400ce6:
                                        mov
                41 ff 14 dc
                                               *(%r12,%rbx,8)
  400ce9:
                                        calla
                48 83 c3 01
                                                $0x1,%rbx
  400ced:
                                        add
  400cf1:
                48 39 eb
                                               %rbp,%rbx
                                        cmp
                75 ea
  400cf4:
                                        jne
                                               400ce0 <getlogin_r@plt+0x510>
  400cf6:
                48 83 c4 08
                                        add
                                                $0x8,%rsp
                5b
  400cfa:
                                               %rbx
                                        pop
  400cfb:
                5d
                                        pop
                                               %rbp
  400cfc:
                41 5c
                                               %r12
                                        pop
  400cfe:
                41 5d
                                               %r13
                                        pop
  400d00:
                41 5e
                                               %r14
                                        pop
  400d02:
                41 5f
                                               %r15
                                        pop
  400d04:
                с3
                                        retq
  400d05:
                66 66 2e 0f 1f 84 00
                                        data32 nopw %cs:0x0(%rax,%rax,1)
                00 00 00 00
  400d0c:
  400d10:
                f3 c3
                                        repz retq
Disassembly of section .fini:
0000000000400d14 < fini>:
  400d14:
                48 83 ec 08
                                        sub
                                                $0x8,%rsp
                48 83 c4 08
  400d18:
                                        add
                                                $0x8,%rsp
  400d1c:
                с3
                                        reta
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -a 4
4:
       file format elf64-x86-64
4
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -s 4
       file format elf64-x86-64
4:
Contents of section .interp:
 400238 2f6c6962 36342f6c 642d6c69 6e75782d /lib64/ld-linux-
 400248 7838362d 36342e73 6f2e3200
                                             x86-64.so.2.
Contents of section .note.ABI-tag:
 400254 04000000 10000000 01000000 474e5500
                                              400264 00000000 02000000 06000000 18000000
                                              . . . . . . . . . . . . . . . .
Contents of section .note.gnu.build-id:
 400274 04000000 14000000 03000000 474e5500
                                              400284 516c99c4 5c7b1cd5 13589f91 ae029c0f
                                             01..\{...X.....
 400294 1528d553
                                              .(.S
Contents of section .gnu.hash:
 400298 03000000 0e0000000 01000000 06000000
                                              . . . . . . . . . . . . . . . .
 4002a8 88c02001 00044009 0e000000 10000000
                                              .. ...@......
 4002b8 12000000 4245d5ec bbe3927c d871581c
                                             ....BE.....|.qX.
 4002c8 b98df10e ebd3ef0e
                                              . . . . . . . .
Contents of section .dynsym:
 4002e0 00000000 00000000 0b000000 20000000
```

00

4002f0	00000000	00000000	00000000	00000000	
400300	8a000000	12000000	00000000	00000000	
400310	00000000	00000000	6a000000	12000000	j
400320	00000000	00000000	00000000	00000000	
400330	bc000000	12000000	00000000	00000000	
400340	00000000	00000000	8f000000	12000000	
400350	00000000	00000000	00000000	00000000	
400360	ae000000	12000000	00000000	00000000	
400370	00000000	00000000	a0000000	12000000	
400380	00000000	00000000	00000000	00000000	
400390	ce000000	12000000	00000000	00000000	
4003a0	00000000	00000000	b5000000	12000000	
4003b0	00000000	00000000	00000000	00000000	
4003c0	27000000	20000000	00000000	00000000	1
4003d0	00000000	00000000	c3000000	12000000	
4003e0	00000000	00000000	00000000	00000000	
4003f0	36000000	20000000	00000000	00000000	6
400400	00000000	00000000	4a000000	20000000	J
400410	00000000	00000000	00000000	00000000	
400420	e0000000	10001800	0c216000	00000000	!`!
400430	00000000	00000000	f3000000	10001900	
400440	10216000	00000000	00000000	00000000	.!`
400450	e7000000	10001900	0c216000	00000000	!`!
400460	00000000	00000000	64000000	12000b00	d
400470	08074000	00000000	00000000	00000000	@
400480	7a000000	12000e00	140d4000	00000000	Z
400490	00000000	00000000			
400490 Contents	00000000 s of secti	00000000 ion .dynst	tr:		
Contents				49544d5f	
Contents	s of secti	ion .dynst	736f005f	49544d5f 436c6f6e	
Contents 400498	s of secti 006c6962	ion .dyns† 3336312e	736f005f		.lib361.soITM_
Contents 400498 4004a8	s of secti 006c6962 64657265	ion .dynst 3336312e 67697374	736f005f 6572544d	436c6f6e	.lib361.soITM_ deregisterTMClon
Contents 400498 4004a8 4004b8	s of secti 006c6962 64657265 65546162 6172745f	ion .dynst 3336312e 67697374 6c65005f	736f005f 6572544d 5f676d6f	436c6f6e 6e5f7374	.lib361.soITM_ deregisterTMClon eTablegmon_st
Contents 400498 4004a8 4004b8 4004c8 4004d8	s of secti 006c6962 64657265 65546162 6172745f	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365	736f005f 6572544d 5f676d6f 765f5265 73005f49	436c6f6e 6e5f7374 67697374 544d5f72	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist
Contents 400498 4004a8 4004b8 4004c8 4004d8 4004e8	s of secti 006c6962 64657265 65546162 6172745f 6572436c	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f	436c6f6e 6e5f7374 67697374 544d5f72 6e655461	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r
Contents 400498 4004a8 4004b8 4004c8 4004d8 4004e8 4004f8	s of secti 006c6962 64657265 65546162 6172745f 6572436c 65676973	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa
Contents 400498 4004a8 4004b8 4004c8 4004d8 4004e8 4004f8 400508	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret
Contents 400498 4004a8 4004b8 4004c8 4004d8 4004f8 400508 400518	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini.
Contents 400498 4004a8 4004b8 4004c8 4004e8 4004e8 400518 400518 400528	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.puts
Contents 400498 4004a8 4004b8 4004c8 4004e8 4004e8 400508 400518 400528 400538	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_fail.
Contents 400498 4004a8 4004b8 4004c8 4004e8 4004f8 400508 400518 400528 400538 400548	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr
Contents 400498 4004a8 4004c8 4004c8 4004e8 4004f8 400508 400518 400528 400538 400548 400558	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl
Contents 400498 4004a8 4004b8 4004c8 4004e8 4004f8 400518 400528 400538 400558 400568	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r libc_start_main.
Contents 400498 4004a8 4004b8 4004c8 4004e8 4004f8 400518 400528 400538 400548 400568 400578	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461 7461005f	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d 5f627373	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00 5f737461	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r
Contents 400498 4004a8 4004b8 4004c8 4004f8 400508 400518 400538 400538 400558 400568 400578 400588	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461 7461005f 656e6400	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d 5f627373 474c4942	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00 5f737461 435f322e	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r libc_start_mainedatabss_sta
Contents 400498 4004a8 4004c8 4004c8 4004e8 4004f8 400508 400518 400528 400538 400548 400558 400578 400588 400598	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461 7461005f 656e6400 4942435f	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d 5f627373 474c4942 322e322e	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00 5f737461 435f322e	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r libc_start_mainedatabss_sta rtend.GLIBC_2.
Contents 400498 4004a8 4004b8 4004c8 4004d8 4004e8 400518 400528 400528 400538 400558 400568 400578 400598 Contents	s of sects 006c6962 64657265 65546162 6172745f 6572436c 65676973 626c6500 6f706572 6c696263 5f737461 5f5f6173 696e7466 656e0067 6c696263 5f656461 7274005f 3400474c	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461 7461005f 656e6400 4942435f ion .gnu.	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d 5f627373 474c4942 322e322e version:	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00 5f737461 435f322e	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r libc_start_mainedatabss_sta rtend.GLIBC_2.
Contents 400498 4004a8 4004b8 4004c8 4004d8 4004f8 400508 400518 400528 400538 400568 400568 400578 400588 400598 Contents 4005a6	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461 7461005f 656e6400 4942435f ion .gnu.v	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d 5f627373 474c4942 322e322e version: 02000300	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00 5f737461 435f322e 3500	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r libc_start_mainedatabss_sta rtend.GLIBC_2. 4.GLIBC_2.2.5.
Contents 400498 4004a8 4004b8 4004c8 4004f8 400508 400518 400538 400538 400558 400578 400588 400598 Contents 4005a6 4005b6	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461 7461005f 656e6400 4942435f ion .gnu.v	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d 5f627373 474c4942 322e322e version: 02000300	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00 5f737461 435f322e 3500	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r libc_start_mainedatabss_sta rtend.GLIBC_2. 4.GLIBC_2.2.5.
Contents 400498 4004a8 4004b8 4004c8 4004d8 400468 400508 400518 400528 400538 400548 400558 400578 400588 400598 Contents 4005b6 4005c6	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461 7461005f 656e6400 4942435f ion .gnu.v 02000000 0100	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d 5f627373 474c4942 322e322e version: 02000300 00000000	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00 5f737461 435f322e 3500 02000200 01000100	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r libc_start_mainedatabss_sta rtend.GLIBC_2. 4.GLIBC_2.2.5.
Contents 400498 4004a8 4004b8 4004c8 4004d8 4004f8 400518 400528 400538 400558 400568 400568 400598 Contents 4005c6 Contents	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461 7461005f 656e6400 4942435f ion .gnu.v 02000000 0100 ion .gnu.v	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d 5f627373 474c4942 322e322e version: 02000300 00000000	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00 5f737461 435f322e 3500 02000200 01000100	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r libc_start_mainedatabss_sta rtend.GLIBC_2. 4.GLIBC_2.2.5.
Contents 400498 4004a8 4004b8 4004c8 4004f8 400508 400518 400538 400538 400558 400568 400578 400588 400598 Contents 4005c6 Contents 4005d0	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461 7461005f 656e6400 4942435f ion .gnu.v 02000000 0100 ion .gnu.v 80000000	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d 5f627373 474c4942 322e322e version: 02000300 00000000	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00 5f737461 435f322e 3500 02000200 01000100	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r libc_start_mainedatabss_sta rtend.GLIBC_2. 4.GLIBC_2.2.5.
Contents 400498 4004a8 4004b8 4004c8 4004f8 400508 400518 400538 400538 400558 400578 400588 400598 Contents 4005d6 4005d0 4005d0 4005e0	s of section of sectio	ion .dynst 3336312e 67697374 6c65005f 5f005f4a 61737365 74657254 5f696e69 6174696f 2e736f2e 636b5f63 73657274 0063616c 65746c6f 5f737461 7461005f 656e6400 4942435f ion .gnu.v 02000000 0100 ion .gnu.v 80000000 00000300	736f005f 6572544d 5f676d6f 765f5265 73005f49 4d436c6f 74007365 6e005f66 36007075 686b5f66 5f666169 6c6f6300 67696e5f 72745f6d 5f627373 474c4942 322e322e version: 02000300 00000000 version_r: 100000000	436c6f6e 6e5f7374 67697374 544d5f72 6e655461 63726574 696e6900 7473005f 61696c00 6c007072 7374726c 72005f5f 61696e00 5f737461 435f322e 3500 02000200 01000100	.lib361.soITM_ deregisterTMClon eTablegmon_st artJv_Regist erClassesITM_r egisterTMCloneTa bleinit.secret operationfini. libc.so.6.putsstack_chk_failassert_fail.pr intf.calloc.strl en.getlogin_r libc_start_mainedatabss_sta rtend.GLIBC_2. 4.GLIBC_2.2.5.

```
Contents of section .rela.dyn:
 400600 f81f6000 00000000 06000000 0a000000
 400610 00000000 00000000
Contents of section .rela.plt:
 400618 18206000 00000000 07000000 02000000
 400628 00000000 00000000 20206000 00000000
                                              . . . . . . . . ` . . . . .
 400638 07000000 03000000 00000000 00000000
 400648 28206000 00000000 07000000 04000000
                                                 . . . . . . . . . . . . .
 400658 00000000 00000000 30206000 00000000
                                              ...... 0 `.....
 400668 07000000 05000000 00000000 00000000
                                              . . . . . . . . . . . . . . . .
 400678 38206000 00000000 07000000 06000000
                                              8 `..........
 400688 00000000 00000000 40206000 00000000
                                              400698 07000000 07000000 00000000 00000000
                                              H `.....
 4006a8 48206000 00000000 07000000 08000000
                                              .....P `.....
 4006b8 00000000 00000000 50206000 00000000
 4006c8 07000000 09000000 00000000 00000000
                                              . . . . . . . . . . . . . . . .
 4006d8 58206000 00000000 07000000 0a000000
                                              Χ `.....
                                              . . . . . . . . . ` `
 4006e8 00000000 00000000 60206000 00000000
 4006f8 07000000 0b000000 00000000 00000000
Contents of section .init:
 400708 4883ec08 488b05e5 18200048 85c07405
                                              H...H... .H..t.
 400718 e8a30000 004883c4 08c3
                                              . . . . . H. . . .
Contents of section .plt:
                                              .5.. ..%.. ...@.
 400730 ff35d218 2000ff25 d4182000 0f1f4000
 400740 ff25d218 20006800 000000e9 e0ffffff
                                              .%.. .h......
 400750 ff25ca18 20006801 000000e9 d0ffffff
                                              .%.. .h.......
 400760 ff25c218 20006802 000000e9 c0ffffff
                                              .%.. .h......
 400770 ff25ba18 20006803 000000e9 b0ffffff
                                              .%.. .h.......
 400780 ff25b218 20006804 000000e9 a0ffffff
                                              .%.. .h......
 400790 ff25aa18 20006805 000000e9 90ffffff
                                              .%.. .h......
 4007a0 ff25a218 20006806 000000e9 80ffffff
                                              .%.. .h......
 4007b0 ff259a18 20006807 000000e9 70ffffff
                                              .%.. .h....p...
 4007c0 ff259218 20006808 000000e9 60ffffff
                                              .%.. .h....`...
 4007d0 ff258a18 20006809 000000e9 50ffffff
                                              .%.. .h....P...
Contents of section .text:
 4007e0 31ed4989 d15e4889 e24883e4 f0505449
                                              1.I..^H..H...PTI
 4007f0 c7c0100d 400048c7 c1a00c40 0048c7c7
                                              ....@.H....@.H..
 400800 cd084000 e897ffff fff4660f 1f440000
                                              ..@....f..D..
 400810 b8172160 0055482d 10216000 4883f80e
                                              ..!`.UH-.!`.H...
 400820 4889e577 025dc3b8 00000000 4885c074
                                              H..w.].....H..t
 400830 f45dbf10 216000ff e00f1f80 00000000
                                              .]..!`......
                                              ..!`.UH-.!`.H...
 400840 b8102160 0055482d 10216000 48c1f803
 400850 4889e548 89c248c1 ea3f4801 d048d1f8
                                              H..H..H..?H..H..
 400860 75025dc3 ba000000 004885d2 74f45d48
                                              u.l.....H..t.lH
                                              . . . . !` . . . . . . . . . .
 400870 89c6bf10 216000ff e20f1f80 00000000
 400880 803d8518 20000075 11554889 e5e87eff
                                              .=.. ..u.UH...~.
 400890 ffff5dc6 05721820 0001f3c3 0f1f4000
                                              ..l..r. ......a.
 4008a0 48833d68 15200000 741eb800 00000048
                                              H.=h. ..t.....H
                                              ..t.U...`.H....l
 4008b0 85c07414 55bf101e 60004889 e5ffd05d
 4008c0 e97bffff ff0f1f00 e973ffff ff554889
                                              .{.....s...UH.
 4008d0 e54883ec 10c745f4 01000000 c745f802
                                              .H....E.....E..
 4008e0 000000c7 45fc0000 0000bf70 0d4000e8
                                              ....E.....p.@..
 4008f0 4cfeffff be060000 00bf0300 0000e84d
```

```
400900 feffff89 45fc837d fc0a7419 b9da0d40
                                             ....E...}..t....@
400910 00ba1200 0000beb7 0d4000bf c10d4000
                                            400920 e86bfeff ff8b55f8 8b45f489 d689c7e8
                                            .k....U..E.....
400930 1cfeffff 8945fc83 7dfc0474 19b9da0d
                                            .....E...}..t....
400940 4000ba14 000000be b70d4000 bfce0d40
                                            @....@...@
400950 00e83afe ffff488b 05331720 004889c7
                                            ..:...H..3. .H..
400960 e8280000 004889c2 488b0d31 17200048
                                            .(...H..H..1. .H
400970 8b052217 20004889 ce4889c7 b8000000
                                            ..". .H..H.....
                                            .....UH.
400980 00e8fafd ffffb800 000000c9 c3554889
400990 e5534881 ec380400 004889bd c8fbffff
                                            .SH..8...H.....
4009a0 64488b04 25280000 00488945 e831c048
                                            dH..%(...H.E.1.H
4009b0 8d85e0fb ffffbe00 04000048 89c7e80d
                                            . . . . . . . . . . . H . . . .
4009c0 feffffc7 85d4fbff ff000000 00eb3e8b
                                            4009d0 85d4fbff ff48980f b69405e0 fbffff8b
                                            . . . . . H . . . . . . . . . .
4009e0 85d4fbff ff4863c8 488b85c8 fbffff48
                                            ....Hc.H.....H
4009f0 01c80fb6 0031c28b 85d4fbff ff489888
                                            ......H...
400a00 9405e0fb ffff8385 d4fbffff 018b85d4
                                             . . . . . . . . . . . . . . . . .
400a10 fbffff48 63d8488d 85e0fbff ff4889c7
                                             ...Hc.H.....H..
400a20 e83bfdff ff4839c3 72a58b85 d4fbffff
                                            .;...H9.r.....
400a30 4863c848 8d95d8fb ffff488d 85e0fbff
                                            Hc.H....H....
400a40 ff4889ce 4889c7e8 1e000000 488b75e8
                                            .H..H......H.u.
400a50 64483334 25280000 007405e8 10fdffff
                                            dH34%(...t....
400a60 4881c438 0400005b 5dc35548 89e54883
                                            H..8...[].UH..H.
400a70 ec404889 7dd84889 75d04889 55c8488b
                                            .@H.}.H.u.H.U.H.
400a80 45d04883 c00248ba abaaaaaa aaaaaaaa
                                            E.H...H......
400a90 48f7e248 89d048d1 e8488d14 85000000
                                            H..H..H..H.....
400aa0 00488b45 c8488910 488b45c8 488b00be
                                            .H.E.H..H.E.H...
400ab0 01000000 4889c7e8 f4fcffff 488945f8
                                            ....H.......H.E.
400ac0 48837df8 00750ab8 00000000 e9c00100
                                            H.}..u......
400ad0 00c745e0 00000000 c745e400 000000e9
                                            ..E.....E....
400ae0 3b010000 8b45e048 98483b45 d0731b8b
                                            ;....E.H.H;E.s..
400af0 45e08d50 018955e0 4863d048 8b45d848
                                            E..P..U.Hc.H.E.H
400b00 01d00fb6 000fb6c0 eb05b800 00000089
                                            . . . . . . . . . . . . . . . .
400b10 45e88b45 e0489848 3b45d073 1b8b45e0
                                            E..E.H.H; E.s..E.
400b20 8d500189 55e04863 d0488b45 d84801d0
                                            .P..U.Hc.H.E.H..
400b30 0fb6000f b6c0eb05 b8000000 008945ec
                                            . . . . . . . . . . . . . E .
400b40 8b45e048 98483b45 d0731b8b 45e08d50
                                            .E.H.H;E.s..E..P
400b50 018955e0 4863d048 8b45d848 01d00fb6
                                             ..U.Hc.H.E.H....
400b60 000fb6c0 eb05b800 00000089 45f08b45
                                            ....E..E
400b70 e8c1e010 89c28b45 ecc1e008 01c28b45
                                            ....E..E....E
400b80 f001d089 45f48b45 e48d5001 8955e448
                                            ....E...E...P...U.H
400b90 63d0488b 45f84801 c28b45f4 c1e81283
                                            c.H.E.H...E....
400ba0 e03f89c0 0fb680c0 20600088 028b45e4
                                            .?...E.
400bb0 8d500189 55e44863 d0488b45 f84801c2
                                            .P..U.Hc.H.E.H..
400bc0 8b45f4c1 e80c83e0 3f89c00f b680c020
                                            .E.....?...
400bd0 60008802 8b45e48d 50018955 e44863d0
                                             `....E..P..U.Hc.
400be0 488b45f8 4801c28b 45f4c1e8 0683e03f
                                            H.E.H...E....?
400bf0 89c00fb6 80c02060 0088028b 45e48d50
                                            ...... `....E...P
400c00 018955e4 4863d048 8b45f848 01c28b45
                                            ..U.Hc.H.E.H...E
400c10 f483e03f 89c00fb6 80c02060 0088028b
                                            ...?....`....
400c20 45e04898 483b45d0 0f82b6fe ffffc745
                                            E.H.H; E.....E
400c30 e0000000 00eb2448 8b45c848 8b108b45
                                            ....$H.E.H...E
400c40 e0489848 29c24889 d0488d50 ff488b45
                                            .H.H).H..H.P.H.E
```

```
400c50 f84801d0 c6003d83 45e00148 8b4dd048
                                             .H...=.E..H.M.H
400c60 baabaaaa aaaaaaaa aa4889c8 48f7e248
                                             400c70 d1ea4889 d04801c0 4801d048 29c14889
                                             ..H..H..H..H).H.
                                             ....!`.;E...H.E
400c80 ca8b0495 00216000 3b45e07f aa488b45
400c90 f8c9c366 2e0f1f84 00000000 000f1f00
                                             ...f.........
400ca0 41574189 ff415649 89f64155 4989d541
                                             AWA..AVI..AUI..A
400cb0 544c8d25 48112000 55488d2d 48112000
                                             TL.%H. .UH.-H. .
400cc0 534c29e5 31db48c1 fd034883 ec08e835
                                             SL).1.H...H...5
400cd0 faffff48 85ed741e 0f1f8400 00000000
                                             ...H..t......
400ce0 4c89ea4c 89f64489 ff41ff14 dc4883c3
                                             L..L..D..A...H..
400cf0 014839eb 75ea4883 c4085b5d 415c415d
                                             .H9.u.H...[]A\A]
400d00 415e415f c366662e 0f1f8400 00000000
                                             A^A_.ff.....
400d10 f3c3
Contents of section .fini:
 400d14 4883ec08 4883c408 c3
                                             H. . . H. . . .
Contents of section .rodata:
 400d20 01000200 00000000 33343536 37383930
                                             .......34567890
                                             123456789012.%s%
400d30 31323334 35363738 39303132 00257325
400d40 730a0000 00000000 796f7520 77696e21
                                             s....you win!
400d50 20746865 20736563 72657420 69733a0a
                                              the secret is:.
400d60 0062616e 67617261 6e670000 00000000
                                             .bangarang.....
400d70 74686973 2070726f 6772616d 20746573
                                             this program tes
400d80 74732074 68652069 6d706c65 6d656e74
                                             ts the implement
400d90 6174696f 6e206f66 20612064 796e616d
                                             ation of a dynam
400da0 6963616c 6c79206c 696e6b65 64206c69
                                             ically linked li
400db0 62726172 792e0067 65745f73 756d2e63
                                             brary..get sum.c
400dc0 00726573 756c7420 3d3d2031 30007265
                                             .result == 10.re
400dd0 73756c74 203d3d20 34006d61 696e00
                                             sult == 4.main.
Contents of section .eh_frame_hdr:
400de0 011b033b 44000000 07000000 50f9ffff
                                             ...;D.....P...
400df0 90000000 00faffff 60000000 edfaffff
                                              . . . . . . . . ` . . . . . . .
400e00 b8000000 adfbffff d8000000 8afcffff
                                              . . . . . . . . . . . . . . . .
400e10 00010000 c0feffff 20010000 30ffffff
                                             400e20 68010000
                                             h...
Contents of section .eh_frame:
400e28 14000000 000000000 017a5200 01781001
                                             .....zR..x..
400e38 1b0c0708 90010710 14000000 1c000000
                                             . . . . . . . . . . . . . . . .
400e48 98f9ffff 2a000000 00000000 00000000
                                             ....*........
400e58 14000000 00000000 017a5200 01781001
                                             ....zR..x..
400e68 1b0c0708 90010000 24000000 1c000000
                                             ......$....
400e78 b8f8ffff b0000000 000e1046 0e184a0f
                                             ....F..J.
400e88 0b770880 003f1a3b 2a332422 00000000
                                              .w...?.;*3$"....
400e98 1c000000 44000000 2dfaffff c0000000
                                             ....D...-....
400ea8 00410e10 8602430d 0602bb0c 07080000
                                             .A....C......
400eb8 24000000 64000000 cdfaffff dd000000
                                             $...d.......
400ec8 00410e10 8602430d 06488303 02d00c07
                                             .A....C..H.....
400ed8 08000000 00000000 1c000000 8c000000
                                             . . . . . . . . . . . . . . . . .
400ee8 82fbffff 29020000 00410e10 8602430d
                                             ....)....A....C.
400ef8 06032402 0c070800 44000000 ac000000
                                             ..$....D.....
400f08 98fdffff 65000000 00420e10 8f02450e
                                              ....e....B....E.
400f18 188e0345 0e208d04 450e288c 05480e30
                                             ...E. ..E.(..H.0
400f28 8606480e 3883074d 0e406c0e 38410e30
                                             ..H.8..M.@l.8A.0
400f38 410e2842 0e20420e 18420e10 420e0800
                                             A.(B. B..B..B...
```

400f48			c0fdffff	02000000	
	00000000		00000000		
	s of sect	_	_array:		
	a0084000				@
	s of sect	-	_array:		
	80084000				@
	s of secti	-			
601e10	00000000	00000000			
	s of sect:	•	nic:		
601e18	01000000		01000000	00000000	
601e28	01000000	00000000	80000000	00000000	
601e38	0c000000	00000000	08074000	00000000	
601e48	0d000000	00000000	140d4000	00000000	
601e58	19000000	00000000	001e6000	00000000	
601e68	1b000000	00000000	08000000	00000000	
601e78	1a000000	00000000	081e6000	00000000	
601e88	1c000000	00000000	08000000	00000000	
601e98	f5feff6f	00000000	98024000	00000000	0@
601ea8	05000000	00000000	98044000	00000000	@
601eb8	06000000	00000000	d0024000	00000000	
601ec8	0a000000	00000000	0e010000	00000000	
601ed8	0b000000	00000000	18000000	00000000	
601ee8	15000000	00000000	00000000	00000000	
601ef8	03000000	00000000	00206000	00000000	`
601f08	02000000	00000000	f0000000	00000000	
601f18	14000000	00000000	07000000	00000000	
601f28	17000000	00000000	18064000	00000000	
601f38	07000000	00000000	00064000	00000000	
601f48	08000000	00000000	18000000	00000000	
601f58	09000000	00000000	18000000	00000000	
601f68	feffff6f	00000000	d0054000	00000000	0@
601f78	ffffff6f	00000000	01000000	00000000	0
601f88	f0ffff6f	00000000	a6054000	00000000	0@
601f98	00000000	00000000	00000000	00000000	
	00000000		00000000	00000000	
601fb8	00000000		00000000	00000000	
601fc8	00000000	00000000	00000000	00000000	
601fd8			00000000	00000000	
	00000000	00000000	00000000	00000000	
	s of sect				
	00000000				
Contents	s of sect	ion .got.	olt:		
	181e6000			00000000	
	00000000		46074000	00000000	F.@
602020	56074000	00000000	66074000		V.@f.@
	76074000		86074000	00000000	v.@@
	96074000		a6074000	00000000	@
602050	b6074000	00000000	c6074000	00000000	@
602060		00000000	-		@
	s of sect		:		•
	00000000			00000000	
	280d4000		3d0d4000	00000000	(.@=.@
	480d4000		00000000	00000000	H.@
		3220000		, , , , , , , , , , , , , , , , , , , ,	- (

```
6020c0 41424344 45464748 494a4b4c 4d4e4f50
                                              ABCDEFGHIJKLMNOP
 6020d0 51525354 55565758 595a6162 63646566
                                              QRSTUVWXYZabcdef
 6020e0 6768696a 6b6c6d6e 6f707172 73747576
                                              ghijklmnopgrstuv
 6020f0 7778797a 30313233 34353637 38392b2f
                                             wxyz0123456789+/
 602100 00000000 02000000 01000000
Contents of section .comment:
 0000 4743433a 20285562 756e7475 20342e38 GCC: (Ubuntu 4.8
 0010 2e342d32 7562756e 7475317e 31342e30 .4-2ubuntu1~14.0
 0020 34292034 2e382e34 00474343 3a202855 4) 4.8.4.GCC: (U
 0030 62756e74 7520342e 382e322d 31397562 buntu 4.8.2-19ub
 0040 756e7475 31292034 2e382e32 00
                                            untu1) 4.8.2.
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -S 4
4:
       file format elf64-x86-64
Disassembly of section .init:
0000000000400708 < init>:
  400708:
                48 83 ec 08
                                         sub
                                                $0x8,%rsp
  40070c:
                48 8b 05 e5 18 20 00
                                                0x2018e5(%rip),%rax
                                         mov
                                                                           # 601ff
8 < fini+0x2012e4>
  400713:
                48 85 c0
                                         test
                                                %rax,%rax
                74 05
                                                40071d <_init+0x15>
  400716:
                                         jе
                e8 a3 00 00 00
  400718:
                                         callq
                                                4007c0 < gmon start @plt>
  40071d:
                48 83 c4 08
                                         add
                                                $0x8,%rsp
  400721:
                с3
                                         retq
Disassembly of section .plt:
0000000000400730 <puts@plt-0x10>:
  400730:
                ff 35 d2 18 20 00
                                         pushq
                                                0x2018d2(%rip)
                                                                      # 602008 < f
ini+0x2012f4>
  400736:
                ff 25 d4 18 20 00
                                         jmpq
                                                *0x2018d4(%rip)
                                                                       # 602010 <_
fini+0x2012fc>
  40073c:
                0f 1f 40 00
                                         nopl
                                                0x0(%rax)
0000000000400740 <puts@plt>:
                ff 25 d2 18 20 00
  400740:
                                         jmpq
                                                *0x2018d2(%rip)
                                                                       # 602018 <
fini+0x201304>
  400746:
                68 00 00 00 00
                                         pushq
                                                $0x0
  40074b:
                e9 e0 ff ff ff
                                         jmpq
                                                400730 <_init+0x28>
000000000400750 <secretoperation@plt>:
                ff 25 ca 18 20 00
  400750:
                                         jmpq
                                                *0x2018ca(%rip)
                                                                       # 602020 <_
fini+0x20130c>
  400756:
                68 01 00 00 00
                                         pushq
                                                $0x1
  40075b:
                e9 d0 ff ff ff
                                         jmpq
                                                400730 < init+0x28>
0000000000400760 <strlen@plt>:
                ff 25 c2 18 20 00
  400760:
                                         jmpq
                                                *0x2018c2(%rip)
                                                                      # 602028 <
fini+0x201314>
```

.

400766: 40076b:	68 02 00 00 e9 c0 ff f		pushq jmpq	\$0x2 400730 <_init+0x28>				
000000000400770 <stack_chk_fail@plt>:</stack_chk_fail@plt>								
400770: fini+0x20131c>	o <stack_o ff 25 ba 18</stack_o 		jmpq	*0x2018ba(%rip)	# 602030 <_			
400776: 40077b:	68 03 00 00 e9 b0 ff f		pushq jmpq	\$0x3 400730 <_init+0x28>				
0000000000040078	10 <pre>nrin+f0n</pre>	l+~ ı						
400780:	ff 25 b2 18		jmpq	*0x2018b2(%rip)	# 602038 <_			
fini+0x201324>			J 1 1	, p	_			
400786:	68 04 00 00		pushq	\$0×4				
40078b:	e9 a0 ff f	f ff	jmpq	400730 <_init+0x28>				
0000000000040079	0 < assert	fail@plt>:						
400790:	ff 25 aa 18		jmpq	*0x2018aa(%rip)	# 602040 <_			
fini+0x20132c>								
400796: 40079b:	68 05 00 00 e9 90 ff f		pushq	\$0x5				
400/90:	69 90 11 1	1 11	jmpq	400730 <_init+0x28>				
00000000004007a	0 <libc_s< td=""><td>tart_main@plt</td><td>>:</td><td></td><td></td></libc_s<>	tart_main@plt	>:					
4007a0:	ff 25 a2 18	3 20 00	jmpq	*0x2018a2(%rip)	# 602048 <_			
fini+0x201334>	60 06 00 0		and the second	+0. 6				
4007a6: 4007ab:	68 06 00 00 e9 80 ff f		pushq jmpq	\$0x6 400730 <_init+0x28>				
400700.	C9 00 11 1		Jiiibd	400/30 _INIT+0X20>				
00000000004007b	0 <calloc@p< td=""><td>lt>:</td><td></td><td></td><td></td></calloc@p<>	lt>:						
4007b0:	ff 25 9a 18	3 20 00	jmpq	*0x20189a(%rip)	# 602050 <_			
fini+0x20133c>	60 07 00 04			+0.7				
4007b6: 4007bb:	68 07 00 00 e9 70 ff f		pushq jmpq	\$0x7 400730 <_init+0x28>				
400700.	C9 /0 11 1		Jiiibd	400/30 _INIT+0X20>				
00000000004007	0 <gmon_s< td=""><td>tart@plt>:</td><td></td><td></td><td></td></gmon_s<>	tart@plt>:						
4007c0:	ff 25 92 18	3 20 00	jmpq	*0x201892(%rip)	# 602058 <_			
fini+0x201344>	CO 00 00 0			¢00				
4007c6: 4007cb:	68 08 00 00 e9 60 ff f		pushq jmpq	\$0x8 400730 <_init+0x28>				
4007 CD:	C5 00 11 1		Jiiipq	400750 _INIT! OX202				
00000000004007c								
4007d0:	ff 25 8a 18	3 20 00	jmpq	*0x20188a(%rip)	# 602060 <_			
fini+0x20134c> 4007d6:	68 09 00 00	2 00	nucha	¢0×0				
4007db:	e9 50 ff f		pushq jmpq	\$0x9 400730 <_init+0x28>				
4007451	C3 30 11 1		J.mpq	400730 <u>1111110720</u>				
Disassembly of section .text:								
0000000000040076								
4007e0:	31 ed		xor	%ebp,%ebp				
4007e2:	49 89 d1		mov	%rdx,%r9				
4007e5: 4007e6:	5e 48 89 e2		pop mov	%rsi %rsp,%rdx				
4007e0:	48 83 e4 f	9	and	\$0xffffffffffffff6,%r	sn			
.00,001	.5 55 64 16	-	G.14	+3X, 01	- P			

```
4007ed:
                 50
                                           push
                                                   %rax
                 54
                                                   %rsp
  4007ee:
                                           push
                 49 c7 c0 10 0d 40 00
  4007ef:
                                           mov
                                                   $0x400d10,%r8
  4007f6:
                 48 c7 c1 a0 0c 40 00
                                                   $0x400ca0,%rcx
                                           mov
  4007fd:
                 48 c7 c7 cd 08 40 00
                                           mov
                                                   $0x4008cd,%rdi
  400804:
                 e8 97 ff ff ff
                                                   4007a0 <__libc_start_main@plt>
                                           callq
  400809:
                 f4
                                           hlt
                 66 0f 1f 44 00 00
                                                   0x0(%rax,%rax,1)
  40080a:
                                           nopw
  400810:
                 b8 17 21 60 00
                                           mov
                                                   $0x602117,%eax
                 55
  400815:
                                           push
                                                   %rbp
  400816:
                 48 2d 10 21 60 00
                                           sub
                                                   $0x602110,%rax
  40081c:
                 48 83 f8 0e
                                           cmp
                                                   $0xe,%rax
  400820:
                 48 89 e5
                                           mov
                                                   %rsp,%rbp
  400823:
                 77 02
                                                   400827 <getlogin_r@plt+0x57>
                                           jа
  400825:
                 5d
                                                   %rbp
                                           pop
  400826:
                 с3
                                           retq
  400827:
                 b8 00 00 00 00
                                           mov
                                                   $0x0,%eax
                 48 85 c0
  40082c:
                                           test
                                                   %rax,%rax
  40082f:
                 74 f4
                                           jе
                                                   400825 <getlogin_r@plt+0x55>
                 5d
  400831:
                                           pop
                 bf 10 21 60 00
  400832:
                                           mov
                                                   $0x602110,%edi
                 ff e0
  400837:
                                           jmpq
                                                   *%rax
                 0f 1f 80 00 00 00 00
                                           nopl
                                                   0x0(%rax)
  400839:
  400840:
                 b8 10 21 60 00
                                           mov
                                                   $0x602110,%eax
                 55
  400845:
                                           push
                                                   %rbp
                 48 2d 10 21 60 00
                                                   $0x602110,%rax
  400846:
                                           sub
  40084c:
                 48 c1 f8 03
                                                   $0x3,%rax
                                           sar
                 48 89 e5
  400850:
                                                   %rsp,%rbp
                                           mov
  400853:
                 48 89 c2
                                                   %rax,%rdx
                                           mov
                 48 c1 ea 3f
  400856:
                                                   $0x3f,%rdx
                                           shr
  40085a:
                 48 01 d0
                                           add
                                                   %rdx,%rax
  40085d:
                 48 d1 f8
                                           sar
                                                   %rax
  400860:
                 75 02
                                           ine
                                                   400864 <getlogin_r@plt+0x94>
  400862:
                 5d
                                                   %rbp
                                           pop
  400863:
                 с3
                                           retq
                 ba 00 00 00 00
  400864:
                                                   $0x0,%edx
                                           mov
  400869:
                 48 85 d2
                                           test
                                                   %rdx,%rdx
                 74 f4
                                                   400862 < getlogin r@plt+0x92>
  40086c:
                                           jе
  40086e:
                 5d
                                                   %rbp
                                           pop
                 48 89 c6
                                                   %rax,%rsi
  40086f:
                                           mov
  400872:
                 bf 10 21 60 00
                                           mov
                                                   $0x602110,%edi
  400877:
                 ff e2
                                                   *%rdx
                                           jmpq
                 0f 1f 80 00 00 00 00
  400879:
                                           nopl
                                                   0x0(%rax)
                 80 3d 85 18 20 00 00
  400880:
                                           cmpb
                                                   $0x0,0x201885(%rip)
                                                                                # 60210
c < edata>
                                                   40089a <getlogin_r@plt+0xca>
                 75 11
  400887:
                                           jne
  400889:
                 55
                                           push
                                                   %rbp
                 48 89 e5
                                                   %rsp,%rbp
  40088a:
                                           mov
                 e8 7e ff ff ff
                                                   400810 <getlogin_r@plt+0x40>
  40088d:
                                           callq
  400892:
                 5d
                                           pop
                 c6 05 72 18 20 00 01
  400893:
                                           movb
                                                   $0x1,0x201872(%rip)
                                                                                # 60210
c <_edata>
                 f3 c3
  40089a:
                                           repz retq
```

```
40089c:
                 0f 1f 40 00
                                                  0x0(%rax)
                                           nopl
                 48 83 3d 68 15 20 00
  4008a0:
                                                  $0x0,0x201568(%rip)
                                                                               # 601e1
                                           cmpq
0 <_fini+0x2010fc>
  4008a7:
                 00
                 74 1e
                                                  4008c8 <getlogin_r@plt+0xf8>
  4008a8:
                                           jе
                 b8 00 00 00 00
  4008aa:
                                           mov
                                                  $0x0,%eax
                 48 85 c0
  4008af:
                                           test
                                                  %rax,%rax
                 74 14
  4008b2:
                                                  4008c8 <getlogin_r@plt+0xf8>
                                           jе
  4008b4:
                 55
                                                  %rbp
                                           push
                 bf 10 1e 60 00
  4008b5:
                                                  $0x601e10,%edi
                                          mov
  4008ba:
                 48 89 e5
                                           mov
                                                  %rsp,%rbp
  4008bd:
                 ff d0
                                           callq
                                                  *%rax
  4008bf:
                 5d
                                                  %rbp
                                           pop
                 e9 7b ff ff ff
                                                  400840 <getlogin_r@plt+0x70>
  4008c0:
                                           jmpq
  4008c5:
                 0f 1f 00
                                           nopl
                                                  (%rax)
  4008c8:
                 e9 73 ff ff ff
                                           jmpq
                                                  400840 <getlogin_r@plt+0x70>
  4008cd:
                 55
                                                  %rbp
                                           push
  4008ce:
                 48 89 e5
                                                  %rsp,%rbp
                                          mov
  4008d1:
                 48 83 ec 10
                                           sub
                                                  $0x10,%rsp
                 c7 45 f4 01 00 00 00
  4008d5:
                                          movl
                                                  $0x1,-0xc(%rbp)
                 c7 45 f8 02 00 00 00
                                                  $0x2,-0x8(%rbp)
  4008dc:
                                           movl
                 c7 45 fc 00 00 00 00
                                                  $0x0,-0x4(%rbp)
  4008e3:
                                           movl
                 bf 70 0d 40 00
                                                  $0x400d70,%edi
  4008ea:
                                           mov
                 e8 4c fe ff ff
  4008ef:
                                           callq
                                                  400740 <puts@plt>
  4008f4:
                 be 06 00 00 00
                                                  $0x6,%esi
                                           mov
                 bf 03 00 00 00
  4008f9:
                                                  $0x3,%edi
                                           mov
  4008fe:
                 e8 4d fe ff ff
                                           callq
                                                  400750 <secretoperation@plt>
                 89 45 fc
                                                  %eax,-0x4(%rbp)
  400903:
                                           mov
  400906:
                 83 7d fc 0a
                                           cmpl
                                                  $0xa,-0x4(%rbp)
                 74 19
                                                  400925 <getlogin_r@plt+0x155>
  40090a:
                                           jе
  40090c:
                 b9 da 0d 40 00
                                                  $0x400dda,%ecx
                                           mov
  400911:
                 ba 12 00 00 00
                                                  $0x12,%edx
                                           mov
  400916:
                 be b7 0d 40 00
                                                  $0x400db7,%esi
                                           mov
  40091b:
                 bf c1 0d 40 00
                                                  $0x400dc1,%edi
                                           mov
  400920:
                 e8 6b fe ff ff
                                           callq
                                                  400790 <__assert_fail@plt>
  400925:
                 8b 55 f8
                                                  -0x8(%rbp),%edx
                                           mov
  400928:
                 8b 45 f4
                                           mov
                                                  -0xc(%rbp),%eax
                 89 d6
  40092b:
                                                  %edx,%esi
                                           mov
  40092d:
                89 c7
                                                  %eax,%edi
                                           mov
                e8 1c fe ff ff
  40092f:
                                           callq
                                                  400750 <secretoperation@plt>
  400934:
                 89 45 fc
                                           mov
                                                  %eax,-0x4(%rbp)
                 83 7d fc 04
  400937:
                                           cmpl
                                                  $0x4,-0x4(%rbp)
                                                  400956 <getlogin_r@plt+0x186>
  40093b:
                74 19
                                           jе
  40093d:
                 b9 da 0d 40 00
                                                  $0x400dda,%ecx
                                          mov
  400942:
                 ba 14 00 00 00
                                           mov
                                                  $0x14,%edx
                 be b7 0d 40 00
  400947:
                                           mov
                                                  $0x400db7,%esi
  40094c:
                 bf ce 0d 40 00
                                           mov
                                                  $0x400dce,%edi
                 e8 3a fe ff ff
                                                  400790 <__assert_fail@plt>
  400951:
                                           callq
                 48 8b 05 33 17 20 00
  400956:
                                           mov
                                                  0x201733(%rip),%rax
                                                                               # 60209
0 <_fini+0x20137c>
  40095d:
                 48 89 c7
                                           mov
                                                  %rax,%rdi
  400960:
                 e8 28 00 00 00
                                           callq
                                                  40098d <getlogin_r@plt+0x1bd>
  400965:
                 48 89 c2
                                           mov
                                                  %rax,%rdx
```

```
400968:
                 48 8b 0d 31 17 20 00
                                                                               # 6020a
                                                  0x201731(%rip),%rcx
                                           mov
0 < fini+0x20138c>
  40096f:
                 48 8b 05 22 17 20 00
                                                  0x201722(%rip),%rax
                                                                               # 60209
                                           mov
8 < fini+0x201384>
  400976:
                 48 89 ce
                                                  %rcx,%rsi
                                           mov
  400979:
                 48 89 c7
                                                  %rax,%rdi
                                           mov
  40097c:
                 b8 00 00 00 00
                                                  $0x0,%eax
                                           mov
  400981:
                 e8 fa fd ff ff
                                           callq
                                                  400780 <printf@plt>
  400986:
                 b8 00 00 00 00
                                           mov
                                                  $0x0,%eax
  40098b:
                 c9
                                           leaveq
  40098c:
                 c3
                                           retq
  40098d:
                 55
                                           push
                                                  %rbp
  40098e:
                 48 89 e5
                                                  %rsp,%rbp
                                           mov
  400991:
                 53
                                                  %rbx
                                           push
  400992:
                 48 81 ec 38 04 00 00
                                                  $0x438,%rsp
                                           sub
  400999:
                 48 89 bd c8 fb ff ff
                                           mov
                                                  %rdi,-0x438(%rbp)
  4009a0:
                 64 48 8b 04 25 28 00
                                                  %fs:0x28,%rax
                                           mov
  4009a7:
                 00 00
  4009a9:
                 48 89 45 e8
                                           mov
                                                  %rax,-0x18(%rbp)
                 31 c0
  4009ad:
                                           xor
                                                  %eax,%eax
                 48 8d 85 e0 fb ff ff
                                                  -0x420(%rbp),%rax
  4009af:
                                           lea
                 be 00 04 00 00
                                                  $0x400,%esi
  4009b6:
                                           mov
                 48 89 c7
                                                  %rax,%rdi
  4009bb:
                                           mov
                 e8 0d fe ff ff
                                           callq
  4009be:
                                                  4007d0 <getlogin_r@plt>
                 c7 85 d4 fb ff ff 00
  4009c3:
                                           movl
                                                  $0x0,-0x42c(%rbp)
                 00 00 00
  4009ca:
  4009cd:
                 eb 3e
                                           jmp
                                                  400a0d <getlogin_r@plt+0x23d>
                 8b 85 d4 fb ff ff
                                           mov
  4009cf:
                                                  -0x42c(%rbp),%eax
  4009d5:
                 48 98
                                           cltq
                 0f b6 94 05 e0 fb ff
                                           movzbl -0x420(%rbp,%rax,1),%edx
  4009d7:
  4009de:
                 ff
                                                  -0x42c(%rbp),%eax
  4009df:
                 8b 85 d4 fb ff ff
                                           mov
  4009e5:
                 48 63 c8
                                           movslq %eax,%rcx
  4009e8:
                 48 8b 85 c8 fb ff ff
                                                  -0x438(%rbp),%rax
                                           mov
  4009ef:
                 48 01 c8
                                           add
                                                  %rcx,%rax
                 0f b6 00
  4009f2:
                                           movzbl (%rax),%eax
  4009f5:
                 31 c2
                                           xor
                                                  %eax,%edx
                                                  -0x42c(%rbp),%eax
                 8b 85 d4 fb ff ff
  4009f7:
                                           mov
  4009fd:
                 48 98
                                           cltq
                 88 94 05 e0 fb ff ff
                                                  %dl,-0x420(%rbp,%rax,1)
  4009ff:
                                           mov
                 83 85 d4 fb ff ff 01
  400a06:
                                           addl
                                                  $0x1,-0x42c(%rbp)
                                                  -0x42c(%rbp),%eax
                 8b 85 d4 fb ff ff
  400a0d:
                                           mov
  400a13:
                 48 63 d8
                                           movslq %eax,%rbx
                 48 8d 85 e0 fb ff ff
  400a16:
                                           lea
                                                  -0x420(%rbp),%rax
  400a1d:
                 48 89 c7
                                           mov
                                                  %rax,%rdi
                 e8 3b fd ff ff
                                                  400760 <strlen@plt>
  400a20:
                                           callq
  400a25:
                 48 39 c3
                                           cmp
                                                  %rax,%rbx
                 72 a5
  400a28:
                                           jb
                                                  4009cf <getlogin_r@plt+0x1ff>
                 8b 85 d4 fb ff ff
  400a2a:
                                           mov
                                                  -0x42c(%rbp),%eax
                 48 63 c8
  400a30:
                                           movslq %eax,%rcx
                 48 8d 95 d8 fb ff ff
  400a33:
                                           lea
                                                  -0x428(%rbp),%rdx
                 48 8d 85 e0 fb ff ff
  400a3a:
                                                  -0x420(%rbp),%rax
                                           lea
  400a41:
                 48 89 ce
                                           mov
                                                  %rcx,%rsi
```

```
400a44:
               48 89 c7
                                        mov
                                                %rax,%rdi
               e8 1e 00 00 00
400a47:
                                        callq
                                                400a6a <getlogin r@plt+0x29a>
               48 8b 75 e8
400a4c:
                                        mov
                                                -0x18(%rbp),%rsi
              64 48 33 34 25 28 00
400a50:
                                        xor
                                                %fs:0x28,%rsi
               00 00
400a57:
               74 05
                                                400a60 <getlogin_r@plt+0x290>
400a59:
                                        jе
400a5b:
               e8 10 fd ff ff
                                        callq
                                                400770 <__stack_chk_fail@plt>
               48 81 c4 38 04 00 00
400a60:
                                        add
                                                $0x438,%rsp
400a67:
              5b
                                                %rbx
                                        pop
                                                %rbp
               5d
400a68:
                                        pop
400a69:
               с3
                                        retq
400a6a:
               55
                                                %rbp
                                        push
400a6b:
               48 89 e5
                                                %rsp,%rbp
                                        mov
400a6e:
               48 83 ec 40
                                                $0x40,%rsp
                                        sub
400a72:
              48 89 7d d8
                                                %rdi,-0x28(%rbp)
                                        mov
400a76:
              48 89 75 d0
                                        mov
                                                %rsi,-0x30(%rbp)
400a7a:
              48 89 55 c8
                                        mov
                                                %rdx,-0x38(%rbp)
              48 8b 45 d0
                                        mov
400a7e:
                                                -0x30(%rbp),%rax
400a82:
               48 83 c0 02
                                        add
                                                $0x2,%rax
              48 ba ab aa aa aa
400a86:
                                        movabs $0xaaaaaaaaaaaaaab,%rdx
400a8d:
               aa aa aa
              48 f7 e2
                                                %rdx
400a90:
                                        mul
               48 89 d0
                                                %rdx,%rax
400a93:
                                        mov
400a96:
               48 d1 e8
                                        shr
                                                %rax
              48 8d 14 85 00 00 00
400a99:
                                        lea
                                                0x0(,%rax,4),%rdx
               00
400aa0:
400aa1:
              48 8b 45 c8
                                                -0x38(%rbp),%rax
                                        mov
               48 89 10
400aa5:
                                                %rdx,(%rax)
                                        mov
400aa8:
              48 8b 45 c8
                                                -0x38(%rbp),%rax
                                        mov
              48 8b 00
                                                (%rax),%rax
400aac:
                                        mov
400aaf:
              be 01 00 00 00
                                                $0x1,%esi
                                        mov
400ab4:
               48 89 c7
                                                %rax,%rdi
                                        mov
400ab7:
              e8 f4 fc ff ff
                                        calla
                                                4007b0 <calloc@plt>
              48 89 45 f8
400abc:
                                                %rax,-0x8(%rbp)
                                        mov
400ac0:
              48 83 7d f8 00
                                                $0x0,-0x8(%rbp)
                                        cmpq
400ac5:
              75 0a
                                                400ad1 <getlogin r@plt+0x301>
                                        jne
400ac7:
              b8 00 00 00 00
                                        mov
                                                $0x0,%eax
              e9 c0 01 00 00
                                                400c91 <getlogin r@plt+0x4c1>
400acc:
                                        jmpq
400ad1:
               c7 45 e0 00 00 00 00
                                        movl
                                                $0x0,-0x20(%rbp)
               c7 45 e4 00 00 00 00
                                                $0x0,-0x1c(%rbp)
400ad8:
                                        movl
400adf:
              e9 3b 01 00 00
                                        jmpq
                                                400c1f <getlogin_r@plt+0x44f>
400ae4:
              8b 45 e0
                                        mov
                                                -0x20(%rbp),%eax
400ae7:
              48 98
                                        cltq
              48 3b 45 d0
400ae9:
                                        cmp
                                                -0x30(%rbp),%rax
400aed:
              73 1b
                                        jae
                                                400b0a <getlogin_r@plt+0x33a>
                                                -0x20(%rbp),%eax
               8b 45 e0
400aef:
                                        mov
400af2:
              8d 50 01
                                        lea
                                                0x1(%rax),%edx
               89 55 e0
                                                %edx,-0x20(%rbp)
400af5:
                                        mov
400af8:
              48 63 d0
                                        movslq %eax,%rdx
400afb:
              48 8b 45 d8
                                        mov
                                                -0x28(%rbp),%rax
400aff:
               48 01 d0
                                        add
                                                %rdx,%rax
                                        movzbl (%rax),%eax
400b02:
               0f b6 00
400b05:
               0f b6 c0
                                        movzbl %al,%eax
```

```
400b08:
               eb 05
                                                400b0f <getlogin_r@plt+0x33f>
                                         jmp
               b8 00 00 00 00
400b0a:
                                                $0x0,%eax
                                         mov
400b0f:
               89 45 e8
                                         mov
                                                %eax,-0x18(%rbp)
               8b 45 e0
                                                -0x20(%rbp),%eax
400b12:
                                         mov
               48 98
                                         cltq
400b15:
               48 3b 45 d0
                                                -0x30(%rbp),%rax
400b17:
                                         cmp
               73 1b
                                                400b38 <getlogin_r@plt+0x368>
400b1b:
                                         jae
               8b 45 e0
400b1d:
                                                -0x20(%rbp),%eax
                                         mov
400b20:
               8d 50 01
                                         lea
                                                0x1(%rax),%edx
              89 55 e0
                                                %edx,-0x20(%rbp)
400b23:
                                         mov
400b26:
               48 63 d0
                                         movslq %eax,%rdx
400b29:
               48 8b 45 d8
                                                -0x28(%rbp),%rax
                                         mov
              48 01 d0
                                                %rdx,%rax
400b2d:
                                         add
400b30:
               0f b6 00
                                         movzbl (%rax),%eax
400b33:
               0f b6 c0
                                         movzbl %al,%eax
400b36:
               eb 05
                                         jmp
                                                400b3d <getlogin_r@plt+0x36d>
400b38:
               b8 00 00 00 00
                                                $0x0,%eax
                                         mov
400b3d:
               89 45 ec
                                                %eax,-0x14(%rbp)
                                         mov
400b40:
               8b 45 e0
                                         mov
                                                -0x20(%rbp),%eax
               48 98
400b43:
                                         clta
               48 3b 45 d0
                                                -0x30(%rbp),%rax
400b45:
                                         cmp
              73 1b
                                                400b66 <getlogin_r@plt+0x396>
400b49:
                                         jae
               8b 45 e0
                                                -0x20(%rbp),%eax
400b4b:
                                         mov
400b4e:
               8d 50 01
                                         lea
                                                0x1(%rax),%edx
               89 55 e0
400b51:
                                                %edx,-0x20(%rbp)
                                         mov
               48 63 d0
400b54:
                                         movslq %eax,%rdx
400b57:
               48 8b 45 d8
                                                -0x28(%rbp),%rax
                                         mov
400b5b:
               48 01 d0
                                                %rdx,%rax
                                         add
400b5e:
               0f b6 00
                                         movzbl (%rax),%eax
               0f b6 c0
                                         movzbl %al,%eax
400b61:
400b64:
               eb 05
                                                400b6b <getlogin_r@plt+0x39b>
                                         jmp
400b66:
               b8 00 00 00 00
                                                $0x0,%eax
                                         mov
400b6b:
               89 45 f0
                                                %eax,-0x10(%rbp)
                                         mov
400b6e:
               8b 45 e8
                                                -0x18(%rbp),%eax
                                         mov
400b71:
               c1 e0 10
                                         shl
                                                $0x10,%eax
400b74:
               89 c2
                                                %eax,%edx
                                         mov
400b76:
               8b 45 ec
                                         mov
                                                -0x14(%rbp),%eax
               c1 e0 08
400b79:
                                         shl
                                                $0x8,%eax
400b7c:
               01 c2
                                         add
                                                %eax,%edx
               8b 45 f0
                                                -0x10(%rbp),%eax
400b7e:
                                         mov
400b81:
               01 d0
                                         add
                                                %edx,%eax
400b83:
               89 45 f4
                                                %eax,-0xc(%rbp)
                                        mov
400b86:
               8b 45 e4
                                        mov
                                                -0x1c(%rbp),%eax
400b89:
               8d 50 01
                                         lea
                                                0x1(%rax),%edx
400b8c:
               89 55 e4
                                         mov
                                                %edx,-0x1c(%rbp)
               48 63 d0
400b8f:
                                         movslq %eax,%rdx
400b92:
               48 8b 45 f8
                                         mov
                                                -0x8(%rbp),%rax
               48 01 c2
                                                %rax,%rdx
400b96:
                                         add
400b99:
               8b 45 f4
                                         mov
                                                -0xc(%rbp),%eax
400b9c:
               c1 e8 12
                                         shr
                                                $0x12,%eax
400b9f:
               83 e0 3f
                                         and
                                                $0x3f,%eax
400ba2:
               89 c0
                                                %eax,%eax
                                         mov
400ba4:
               0f b6 80 c0 20 60 00
                                        movzbl 0x6020c0(%rax),%eax
```

```
400bab:
               88 02
                                                %al,(%rdx)
                                         mov
400bad:
               8b 45 e4
                                                -0x1c(%rbp),%eax
                                         mov
400bb0:
               8d 50 01
                                         lea
                                                0x1(%rax),%edx
               89 55 e4
                                                %edx,-0x1c(%rbp)
400bb3:
                                         mov
400bb6:
               48 63 d0
                                         movslq %eax,%rdx
               48 8b 45 f8
400bb9:
                                                -0x8(%rbp),%rax
                                         mov
               48 01 c2
400bbd:
                                         add
                                                %rax,%rdx
               8b 45 f4
400bc0:
                                                -0xc(%rbp),%eax
                                         mov
400bc3:
               c1 e8 0c
                                         shr
                                                 $0xc,%eax
               83 e0 3f
400bc6:
                                                $0x3f,%eax
                                         and
400bc9:
               89 c0
                                         mov
                                                %eax,%eax
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400bcb:
               88 02
                                                %al,(%rdx)
400bd2:
                                         mov
               8b 45 e4
                                                -0x1c(%rbp),%eax
400bd4:
                                         mov
400bd7:
               8d 50 01
                                                0x1(%rax),%edx
                                         lea
400bda:
               89 55 e4
                                         mov
                                                %edx,-0x1c(%rbp)
400bdd:
               48 63 d0
                                         movslq %eax,%rdx
400be0:
               48 8b 45 f8
                                                -0x8(%rbp),%rax
                                         mov
400be4:
               48 01 c2
                                         add
                                                %rax,%rdx
               8b 45 f4
400be7:
                                                -0xc(%rbp),%eax
                                         mov
400bea:
               c1 e8 06
                                         shr
                                                 $0x6,%eax
               83 e0 3f
400bed:
                                         and
                                                 $0x3f,%eax
               89 c0
                                                %eax,%eax
400bf0:
                                         mov
400bf2:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400bf9:
               88 02
                                                %al,(%rdx)
                                         mov
               8b 45 e4
                                                -0x1c(%rbp),%eax
400bfb:
                                         mov
400bfe:
               8d 50 01
                                         lea
                                                0x1(%rax),%edx
400c01:
               89 55 e4
                                                %edx_{\bullet}-0x1c(%rbp)
                                         mov
400c04:
               48 63 d0
                                         movslq %eax,%rdx
               48 8b 45 f8
400c07:
                                                -0x8(%rbp),%rax
                                         mov
400c0b:
               48 01 c2
                                                %rax,%rdx
                                         add
400c0e:
               8b 45 f4
                                                -0xc(%rbp),%eax
                                         mov
400c11:
               83 e0 3f
                                         and
                                                 $0x3f,%eax
               89 c0
400c14:
                                         mov
                                                %eax,%eax
400c16:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400c1d:
               88 02
                                                %al,(%rdx)
                                         mov
400c1f:
               8b 45 e0
                                         mov
                                                -0x20(%rbp),%eax
               48 98
400c22:
                                         cltq
400c24:
               48 3b 45 d0
                                                -0x30(%rbp),%rax
                                         cmp
               0f 82 b6 fe ff ff
                                                400ae4 <getlogin_r@plt+0x314>
400c28:
                                         jЬ
400c2e:
               c7 45 e0 00 00 00 00
                                         movl
                                                $0x0,-0x20(%rbp)
               eb 24
400c35:
                                                400c5b <getlogin_r@plt+0x48b>
                                         jmp
400c37:
               48 8b 45 c8
                                         mov
                                                -0x38(%rbp),%rax
400c3b:
               48 8b 10
                                         mov
                                                 (%rax),%rdx
400c3e:
               8b 45 e0
                                         mov
                                                -0x20(%rbp),%eax
               48 98
400c41:
                                         cltq
400c43:
               48 29 c2
                                         sub
                                                %rax,%rdx
               48 89 d0
400c46:
                                         mov
                                                %rdx,%rax
400c49:
               48 8d 50 ff
                                         lea
                                                -0x1(%rax),%rdx
               48 8b 45 f8
400c4d:
                                         mov
                                                -0x8(%rbp),%rax
400c51:
               48 01 d0
                                         add
                                                %rdx,%rax
               c6 00 3d
                                                 $0x3d,(%rax)
400c54:
                                         movb
400c57:
               83 45 e0 01
                                         addl
                                                 $0x1,-0x20(%rbp)
```

```
400c5b:
                 48 8b 4d d0
                                                  -0x30(%rbp),%rcx
                                           mov
                 48 ba ab aa aa aa
  400c5f:
                                           movabs $0xaaaaaaaaaaaaaaab,%rdx
  400c66:
                 aa aa aa
                 48 89 c8
                                                  %rcx,%rax
  400c69:
                                           mov
                 48 f7 e2
                                                  %rdx
  400c6c:
                                           mul
                 48 d1 ea
                                           shr
                                                  %rdx
  400c6f:
  400c72:
                 48 89 d0
                                                  %rdx,%rax
                                           mov
                 48 01 c0
  400c75:
                                           add
                                                  %rax,%rax
  400c78:
                 48 01 d0
                                           add
                                                  %rdx,%rax
                 48 29 c1
  400c7b:
                                           sub
                                                  %rax,%rcx
  400c7e:
                 48 89 ca
                                           mov
                                                  %rcx,%rdx
  400c81:
                 8b 04 95 00 21 60 00
                                                  0x602100(,%rdx,4),%eax
                                           mov
  400c88:
                 3b 45 e0
                                                  -0x20(%rbp),%eax
                                           cmp
  400c8b:
                 7f aa
                                                  400c37 <getlogin_r@plt+0x467>
                                           jg
  400c8d:
                 48 8b 45 f8
                                           mov
                                                  -0x8(%rbp),%rax
  400c91:
                 c9
                                           leaveq
  400c92:
                 с3
                                           retq
                 66 2e 0f 1f 84 00 00
  400c93:
                                           nopw
                                                  %cs:0x0(%rax,%rax,1)
  400c9a:
                 00 00 00
                 0f 1f 00
                                                  (%rax)
  400c9d:
                                           nopl
                41 57
                                                  %r15
  400ca0:
                                           push
                41 89 ff
                                                  %edi,%r15d
  400ca2:
                                           mov
                 41 56
                                                  %r14
  400ca5:
                                           push
  400ca7:
                49 89 f6
                                           mov
                                                  %rsi,%r14
                 41 55
  400caa:
                                           push
                                                  %r13
                 49 89 d5
                                                  %rdx,%r13
  400cac:
                                           mov
  400caf:
                 41 54
                                           push
                                                  %r12
                 4c 8d 25 48 11 20 00
  400cb1:
                                           lea
                                                  0x201148(%rip),%r12
                                                                               # 601e0
0 <_fini+0x2010ec>
  400cb8:
                55
                                           push
                                                  %rbp
  400cb9:
                 48 8d 2d 48 11 20 00
                                           lea
                                                  0x201148(%rip),%rbp
                                                                               # 601e0
8 < fini+0x2010f4>
  400cc0:
                 53
                                           push
                                                  %rbx
  400cc1:
                 4c 29 e5
                                                  %r12,%rbp
                                           sub
  400cc4:
                 31 db
                                           xor
                                                  %ebx,%ebx
                 48 c1 fd 03
  400cc6:
                                                  $0x3,%rbp
                                           sar
                 48 83 ec 08
  400cca:
                                           sub
                                                  $0x8,%rsp
                 e8 35 fa ff ff
                                                  400708 < init>
  400cce:
                                           callq
  400cd3:
                 48 85 ed
                                           test
                                                  %rbp,%rbp
                 74 1e
                                                  400cf6 <getlogin_r@plt+0x526>
  400cd6:
                                           jе
  400cd8:
                 0f 1f 84 00 00 00 00
                                          nopl
                                                  0x0(%rax,%rax,1)
  400cdf:
                 00
  400ce0:
                 4c 89 ea
                                           mov
                                                  %r13,%rdx
  400ce3:
                 4c 89 f6
                                           mov
                                                  %r14,%rsi
  400ce6:
                 44 89 ff
                                           mov
                                                  %r15d,%edi
                 41 ff 14 dc
                                                  *(%r12,%rbx,8)
  400ce9:
                                           callq
  400ced:
                 48 83 c3 01
                                           add
                                                  $0x1,%rbx
                 48 39 eb
                                                  %rbp,%rbx
  400cf1:
                                           cmp
                 75 ea
                                                  400ce0 <getlogin_r@plt+0x510>
  400cf4:
                                           jne
                 48 83 c4 08
  400cf6:
                                           add
                                                  $0x8,%rsp
  400cfa:
                 5b
                                           pop
                                                  %rbx
  400cfb:
                 5d
                                                  %rbp
                                           pop
  400cfc:
                 41 5c
                                           pop
                                                  %r12
```

```
400cfe:
                41 5d
                                               %r13
                                        pop
  400d00:
                41 5e
                                               %r14
                                        pop
                41 5f
                                               %r15
  400d02:
                                        pop
  400d04:
                с3
                                        retq
                66 66 2e 0f 1f 84 00
                                        data32 nopw %cs:0x0(%rax,%rax,1)
  400d05:
  400d0c:
                00 00 00 00
  400d10:
               f3 c3
                                        repz retq
Disassembly of section .fini:
0000000000400d14 < fini>:
  400d14:
                48 83 ec 08
                                               $0x8,%rsp
                                        sub
  400d18:
                48 83 c4 08
                                        add
                                               $0x8,%rsp
  400d1c:
                с3
                                        reta
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objcopy --redefine-sym old=new 4
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
  1 2 3 4 howto.txt iamspecial lib361.c lib361.so secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ rm 4
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cd
Dpate85@Dhrumil:~$ cd dpate85
Dpate85@Dhrumil:~/dpate85$ ;s
-bash: syntax error near unexpected token `;'
Dpate85@Dhrumil:~/dpate85$ ls
hw1 hw2 README.md
Dpate85@Dhrumil:~/dpate85$ cd ...
Dpate85@Dhrumil:~$ cd public
Dpate85@Dhrumil:~/public$ ls
hw1 hw2
Dpate85@Dhrumil:~/public$ cd hw2
Dpate85@Dhrumil:~/public/hw2$ ls
puzzles
Dpate85@Dhrumil:~/public/hw2$ cd puzzles
Dpate85@Dhrumil:~/public/hw2/puzzles$ ls
0 1 2 3 4
Dpate85@Dhrumil:~/public/hw2/puzzles$ cp -r ~/public/hw2/puzzles/4 ~/dpate85/hw2/
puzzles/
Dpate85@Dhrumil:~/public/hw2/puzzles$ cd
Dpate85@Dhrumil:~$ ls
```

```
dpate85 public
Dpate85@Dhrumil:~$ cd dpate85
Dpate85@Dhrumil:~/dpate85$ ls
hw1 hw2 README.md
Dpate85@Dhrumil:~/dpate85$ cd hw2
Dpate85@Dhrumil:~/dpate85/hw2$ ls
puzzles
Dpate85@Dhrumil:~/dpate85/hw2$ cd puzzles
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
   1 2 3 4 howto.txt iamspecial lib361.c lib361.so secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cd dpate85
-bash: cd: dpate85: No such file or directory
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
   1 2 3 4 howto.txt iamspecial lib361.c lib361.so secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cd
Dpate85@Dhrumil:~$ ls
dpate85 public
Dpate85@Dhrumil:~$ cd ..
Dpate85@Dhrumil:/home$ ls
Dpate85
Dpate85@Dhrumil:/home$ cd ...
Dpate85@Dhrumil:/$ ls
bin
     dev home
                      initrd.img.old lib64
                                                  media opt
                                                                     sbin
                                                               root
                                                                           Sys
   vmlinuz
usr
boot etc initrd.img lib
                                      lost+found mnt
                                                         proc
                                                               run
                                                                     srv
                                                                           tmp
var vmlinuz.old
Dpate85@Dhrumil:/$ cd usr
Dpate85@Dhrumil:/usr$ ls
bin games include lib local sbin share src
Dpate85@Dhrumil:/usr$ cd local
Dpate85@Dhrumil:/usr/local$ ls
bin etc games include lib man sbin share src
Dpate85@Dhrumil:/usr/local$ cd lib
Dpate85@Dhrumil:/usr/local/lib$ ls
python2.7 python3.4
Dpate85@Dhrumil:/usr/local/lib$ vi lib361.c
Dpate85@Dhrumil:/usr/local/lib$ sudo vi lib361.c
Dpate85@Dhrumil:/usr/local/lib$ gcc -shared -o lib361.so -fPIC lib361.c
/usr/bin/ld: cannot open output file lib361.so: Permission denied
collect2: error: ld returned 1 exit status
Dpate85@Dhrumil:/usr/local/lib$ ls
lib361.c python2.7 python3.4
Dpate85@Dhrumil:/usr/local/lib$ sudo qcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:/usr/local/lib$ ls
lib361.c lib361.so python2.7 python3.4
Dpate85@Dhrumil:/usr/local/lib$ cd
Dpate85@Dhrumil:~$ ls
dpate85 public
Dpate85@Dhrumil:~$ cd dpate85
```

```
Dpate85@Dhrumil:~/dpate85$ ls
hw1
     hw2 README.md
Dpate85@Dhrumil:~/dpate85$ cd hw2
Dpate85@Dhrumil:~/dpate85/hw2$ ls
Dpate85@Dhrumil:~/dpate85/hw2$ cd puzzles
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
   1 2 3 4 howto.txt iamspecial lib361.c lib361.so secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cd
Dpate85@Dhrumil:~$ ls
dpate85 public
Dpate85@Dhrumil:~$ cd ..
Dpate85@Dhrumil:/home$ ls
Dpate85
Dpate85@Dhrumil:/home$ cd .
Dpate85@Dhrumil:/home$ cd ..
Dpate85@Dhrumil:/$ ls
bin
      dev home
                       initrd.img.old lib64
                                                     media
                                                            opt
                                                                  root
                                                                        sbin
                                                                               sys
    vmlinuz
usr
boot etc initrd.img
                       lib
                                        lost+found
                                                    mnt
                                                            proc
                                                                  run
                                                                         srv
                                                                               tmp
var vmlinuz.old
Dpate85@Dhrumil:/$ cd etc
Dpate85@Dhrumil:/etc$ ls
                         groff
acpi
                                          mime.types
                                                                    rmt
adduser.conf
                                          mke2fs.conf
                        group
                                                                    rpc
                                          modprobe.d
                                                                    rsyslog.conf
aditime
                         group-
alternatives
                         grub.d
                                          modules
                                                                    rsyslog.d
apm
                         gshadow
                                          mtab
                                                                    samba
                         qshadow-
                                          nanorc
                                                                    screenrc
apparmor
                         hdparm.conf
                                          network
apparmor.d
                                                                    securetty
apport
                         host.conf
                                          networks
                                                                    security
                         hostname
                                                                    selinux
apt
                                          newt
at.deny
                         hosts
                                          nologin
                                                                    services
                         hosts.allow
                                          nscd.conf
bash.bashrc
                                                                    sgml
bash_completion
                         hosts.deny
                                          nsswitch.conf
                                                                    shadow
bash_completion.d
                         init
                                                                    shadow-
                                          opt
bindresvport.blacklist
                        init.d
                                          os-release
                                                                    shells
                         initramfs-tools
                                          overlayroot.conf
blkid.conf
                                                                    skel
blkid.tab
                                          overlayroot.local.conf
                         inputro
                                                                    ssh
                                          pam.conf
byobu
                         insserv
                                                                    ssl
ca-certificates
                         insserv.conf
                                          pam.d
                                                                    subgid
ca-certificates.conf
                         insserv.conf.d
                                          passwd
                                                                    subgid-
calendar
                         iproute2
                                          passwd-
                                                                    subuid
chatscripts
                                          perl
                                                                    subuid-
                         issue
                         issue.net
cloud
                                          pm
                                                                    sudoers
console-setup
                         kbd
                                          polkit-1
                                                                    sudoers.d
cron.d
                         kernel
                                          pollinate
                                                                    sysctl.conf
                                          popularity-contest.conf
cron.daily
                         kernel-img.conf
                                                                    sysctl.d
cron.hourly
                         landscape
                                          ppp
                                                                    systemd
```

```
ldap
                                          profile
                                                                    terminfo
cron.monthly
                         ld.so.cache
                                          profile.d
                                                                    timezone
crontab
                         ld.so.conf
                                          protocols
                                                                    ucf.conf
cron.weekly
crypttab
                        ld.so.conf.d
                                                                    udev
                                          python
dbus-1
                         legal
                                                                    ufw
                                          python2.7
debconf.conf
                         libaudit.conf
                                          python3
                                                                    updatedb.conf
debian version
                        libnl-3
                                          python3.4
                                                                    update-manager
default
                         locale.alias
                                          rc0.d
                                                                    update-motd.d
deluser.conf
                         localtime
                                          rc1.d
                                                                    update-notifier
depmod.d
                         logcheck
                                          rc2.d
                                                                    upstart-xsessio
ns
dhcp
                         login.defs
                                          rc3.d
                                                                    vim
dpkg
                         logrotate.conf
                                          rc4.d
                                                                    vmware-tools
ec2_version
                         logrotate.d
                                          rc5.d
                                                                    vtrqb
environment
                         lsb-release
                                          rc6.d
                                                                    w3m
                         ltrace.conf
                                          rc.local
fonts
                                                                    waagent.conf
fstab
                        magic
                                          rcS.d
                                                                    wgetrc
fstab.d
                        magic.mime
                                                                    X11
                                          request-key.conf
fuse.conf
                        mailcap
                                          request-key.d
                                                                    xda
qai.conf
                        mailcap.order
                                          resolvconf
                                                                    xml
adb
                        manpath.config
                                          resolv.conf
                                                                    zsh_command_not
_found
Dpate85@Dhrumil:/etc$ ls *.conf
adduser.conf
                      qai.conf
                                        libaudit.conf
                                                         overlayroot.conf
                                                                                   r
syslog.conf
blkid.conf
                      hdparm.conf
                                        logrotate.conf
                                                         overlayroot.local.conf
                                                                                   S
vsctl.conf
                      host.conf
ca-certificates.conf
                                        ltrace.conf
                                                         pam.conf
                                                                                   u
cf.conf
                                        mke2fs.conf
debconf.conf
                       insserv.conf
                                                         popularity-contest.conf
pdatedb.conf
                                        nscd.conf
deluser.conf
                      kernel-img.conf
                                                         request-key.conf
                                                                                   W
aagent.conf
                      ld.so.conf
                                        nsswitch.conf
                                                         resolv.conf
fuse.conf
Dpate85@Dhrumil:/etc$ sudo vi ls.do.conf
Dpate85@Dhrumil:/etc$ sudo vi ls.so.conf
Dpate85@Dhrumil:/etc$ sudo vi ld.so.conf
Dpate85@Dhrumil:/etc$ cd
Dpate85@Dhrumil:~$ cd dpate85
Dpate85@Dhrumil:~/dpate85$ ls
    hw2 README.md
hw1
Dpate85@Dhrumil:~/dpate85$ cd hw2
Dpate85@Dhrumil:~/dpate85/hw2$ ls
puzzles
Dpate85@Dhrumil:~/dpate85/hw2$ cd puzzles
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
   1 2 3 4 howto.txt iamspecial
                                      lib361.c lib361.so secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: qet_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -s 4
```

```
Contents of section .interp:
400238 2f6c6962 36342f6c 642d6c69 6e75782d
                                           /lib64/ld-linux-
400248 7838362d 36342e73 6f2e3200
                                           x86-64.so.2.
Contents of section .note.ABI-tag:
400254 04000000 10000000 01000000 474e5500
                                           . . . . . . . . . . . . . . GNU .
400264 00000000 02000000 06000000 18000000
                                           . . . . . . . . . . . . . . . .
Contents of section .note.gnu.build-id:
400274 04000000 14000000 03000000 474e5500
                                           . . . . . . . . . . . . . GNU .
400284 516c99c4 5c7b1cd5 13589f91 ae029c0f
                                           Ql..\{...X.....
400294 1528d553
                                           .(.S
Contents of section .gnu.hash:
400298 03000000 0e0000000 01000000 06000000
                                           . . . . . . . . . . . . . . . .
4002a8 88c02001 00044009 0e000000 10000000
                                           .. ...@......
4002b8 12000000 4245d5ec bbe3927c d871581c
                                           ....BE.....|.qX.
 4002c8 b98df10e ebd3ef0e
Contents of section .dvnsvm:
 4002e0 00000000 00000000 0b000000 20000000
                                           400300 8a000000 12000000 00000000 00000000
                                           . . . . . . . . . . . . . . . .
400310 00000000 00000000 6a000000 12000000
                                           . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . .
400330 bc000000 12000000 00000000 00000000
400340 00000000 00000000 8f000000 12000000
400360 ae000000 12000000 00000000 00000000
400370 00000000 00000000 a0000000 12000000
400390 ce000000 12000000 00000000 00000000
4003a0 00000000 00000000 b5000000 12000000
. . . . . . . . . . . . . . . .
4003c0 27000000 20000000 00000000 00000000
4003d0 00000000 000000000 c3000000 12000000
                                           . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . .
4003f0 36000000 20000000 00000000 00000000
                                           6... .........
400400 00000000 00000000 4a000000 20000000
                                           .....J...
. . . . . . . . . . . . . . . .
400420 e0000000 10001800 0c216000 00000000
                                           . . . . . . . . ! ` . . . . .
400430 00000000 00000000 f3000000 10001900
                                           . . . . . . . . . . . . . . . .
400440 10216000 00000000 00000000 00000000
                                           .!`...........
                                           . . . . . . . . . ! ` . . . . .
400450 e7000000 10001900 0c216000 00000000
400460 00000000 00000000 64000000 12000b00
                                           . . . . . . . d . . . . . .
400470 08074000 00000000 00000000 00000000
                                           400480 7a000000 12000e00 140d4000 00000000
                                           400490 00000000 00000000
Contents of section .dynstr:
400498 006c6962 3336312e 736f005f 49544d5f
                                           .lib361.so. ITM
4004a8 64657265 67697374 6572544d 436c6f6e
                                           deregisterTMClon
                                           eTable.__gmon_st
4004b8 65546162 6c65005f 5f676d6f 6e5f7374
                                           art__._Jv_Regist
4004c8 6172745f 5f005f4a 765f5265 67697374
4004d8 6572436c 61737365 73005f49 544d5f72
                                           erClasses. ITM r
```

```
4004e8 65676973 74657254 4d436c6f 6e655461
                                              egisterTMCloneTa
 4004f8 626c6500 5f696e69 74007365 63726574
                                              ble. init.secret
 400508 6f706572 6174696f 6e005f66 696e6900
                                              operation._fini.
 400518 6c696263 2e736f2e 36007075 7473005f
                                              libc.so.6.puts.
 400528 5f737461 636b5f63 686b5f66 61696c00
                                              _stack_chk_fail.
 400538 5f5f6173 73657274 5f666169 6c007072
                                              assert fail.pr
 400548 696e7466 0063616c 6c6f6300 7374726c
                                              intf.calloc.strl
 400558 656e0067 65746c6f 67696e5f 72005f5f
                                              en.getlogin_r.__
 400568 6c696263 5f737461 72745f6d 61696e00
                                              libc_start_main.
 400578 5f656461 7461005f 5f627373 5f737461
                                              _edata.__bss_sta
 400588 7274005f 656e6400 474c4942 435f322e
                                              rt._end.GLIBC_2.
 400598 3400474c 4942435f 322e322e 3500
                                              4.GLIBC 2.2.5.
Contents of section .gnu.version:
 4005a6 00000000 02000000 02000300 02000200
 4005b6 02000200 00000200 00000000 01000100
 4005c6 01000100 0100
Contents of section .gnu.version_r:
 4005d0 01000200 80000000 10000000 00000000
 4005e0 1469690d 00000300 f8000000 10000000
 4005f0 751a6909 00000200 02010000 00000000
                                              u.i.........
Contents of section .rela.dyn:
 400600 f81f6000 00000000 06000000 0a000000
                                              . . ` . . . . . . . . . . . . .
 400610 00000000 00000000
Contents of section .rela.plt:
 400618 18206000 00000000 07000000 02000000
 400628 00000000 00000000 20206000 00000000
 400638 07000000 03000000 00000000 00000000
 400648 28206000 00000000 07000000 04000000
                                              ( `..........
 400658 00000000 00000000 30206000 00000000
                                              . . . . . . . . 0 ` . . . . .
 400668 07000000 05000000 00000000 00000000
 400678 38206000 00000000 07000000 06000000
                                              8 `..........
 400688 00000000 00000000 40206000 00000000
                                              400698 07000000 07000000 00000000 00000000
                                              . . . . . . . . . . . . . . . .
 4006a8 48206000 00000000 07000000 08000000
                                              H `.......
 4006b8 00000000 00000000 50206000 00000000
                                              .....P `.....
 4006c8 07000000 09000000 00000000 00000000
                                              . . . . . . . . . . . . . . . . .
 4006d8 58206000 00000000 07000000 0a000000
                                              Χ `.........
 4006e8 00000000 00000000 60206000 00000000
 4006f8 07000000 0b000000 00000000 00000000
                                              . . . . . . . . . . . . . . . .
Contents of section .init:
 400708 4883ec08 488b05e5 18200048 85c07405
                                              H...H... .H..t.
 400718 e8a30000 004883c4 08c3
                                              . . . . . H . . . .
Contents of section .plt:
                                              .5.. ..%.. ...@.
 400730 ff35d218 2000ff25 d4182000 0f1f4000
 400740 ff25d218 20006800 000000e9 e0ffffff
                                              .%.. .h......
 400750 ff25ca18 20006801 000000e9 d0ffffff
                                              .%.. .h......
                                              .%.. .h......
 400760 ff25c218 20006802 000000e9 c0ffffff
 400770 ff25ba18 20006803 000000e9 b0ffffff
                                              .%.. .h......
 400780 ff25b218 20006804 000000e9 a0ffffff
                                              .%.. .h......
 400790 ff25aa18 20006805 000000e9 90ffffff
                                              .%.. .h......
 4007a0 ff25a218 20006806 000000e9 80ffffff
                                              .%.. .h......
 4007b0 ff259a18 20006807 000000e9 70ffffff
                                              .%.. .h....p...
 4007c0 ff259218 20006808 000000e9 60ffffff
                                              .%.. .h....`...
```

```
4007d0 ff258a18 20006809 000000e9 50ffffff
                                            .%.. .h....P...
Contents of section .text:
 4007e0 31ed4989 d15e4889 e24883e4 f0505449
                                            1.I..^H..H...PTI
4007f0 c7c0100d 400048c7 c1a00c40 0048c7c7
                                            ....@.H....@.H..
400800 cd084000 e897ffff fff4660f 1f440000
                                            ..@....f..D..
400810 b8172160 0055482d 10216000 4883f80e
                                            ..!`.UH-.!`.H...
400820 4889e577 025dc3b8 00000000 4885c074
                                            H..w.].....H..t
400830 f45dbf10 216000ff e00f1f80 00000000
                                            .]..!`......
400840 b8102160 0055482d 10216000 48c1f803
                                            ..!`.UH-.!`.H...
400850 4889e548 89c248c1 ea3f4801 d048d1f8
                                            H..H..H..?H..H..
400860 75025dc3 ba000000 004885d2 74f45d48
                                            u.].....H..t.]H
                                            ....!`.......
400870 89c6bf10 216000ff e20f1f80 00000000
400880 803d8518 20000075 11554889 e5e87eff
                                            .=.. ..u.UH...~.
400890 ffff5dc6 05721820 0001f3c3 0f1f4000
                                            ..]..r. .....@.
4008a0 48833d68 15200000 741eb800 00000048
                                            H.=h. ..t....H
                                            ..t.U...`.H....]
 4008b0 85c07414 55bf101e 60004889 e5ffd05d
 4008c0 e97bffff ff0f1f00 e973ffff ff554889
                                            .{.....s..UH.
4008d0 e54883ec 10c745f4 01000000 c745f802
                                            .H....E....E..
4008e0 000000c7 45fc0000 0000bf70 0d4000e8
                                            ....E....p.@..
4008f0 4cfeffff be060000 00bf0300 0000e84d
                                            400900 feffff89 45fc837d fc0a7419 b9da0d40
                                            ....E..}..t....@
400910 00ba1200 0000beb7 0d4000bf c10d4000
                                            400920 e86bfeff ff8b55f8 8b45f489 d689c7e8
                                            .k....U..E....
400930 1cfeffff 8945fc83 7dfc0474 19b9da0d
                                            ....E..}..t....
400940 4000ba14 000000be b70d4000 bfce0d40
                                            @....@....@
400950 00e83afe ffff488b 05331720 004889c7
                                            ..:...H..3. .H..
400960 e8280000 004889c2 488b0d31 17200048
                                            .(...H..H..1. .H
400970 8b052217 20004889 ce4889c7 b8000000
                                            ..". .H..H.....
400980 00e8fafd ffffb800 000000c9 c3554889
                                            .....UH.
400990 e5534881 ec380400 004889bd c8fbffff
                                            .SH..8...H.....
4009a0 64488b04 25280000 00488945 e831c048
                                            dH..%(...H.E.1.H
4009b0 8d85e0fb ffffbe00 04000048 89c7e80d
                                            4009c0 feffffc7 85d4fbff ff000000 00eb3e8b
                                            4009d0 85d4fbff ff48980f b69405e0 fbffff8b
                                            .....H........
4009e0 85d4fbff ff4863c8 488b85c8 fbffff48
                                            ....Hc.H.....H
4009f0 01c80fb6 0031c28b 85d4fbff ff489888
                                            400a00 9405e0fb ffff8385 d4fbffff 018b85d4
                                            . . . . . . . . . . . . . . . .
400a10 fbffff48 63d8488d 85e0fbff ff4889c7
                                            ...Hc.H.....H..
400a20 e83bfdff ff4839c3 72a58b85 d4fbffff
                                            .;...H9.r.....
400a30 4863c848 8d95d8fb ffff488d 85e0fbff
                                            Hc.H....H....
 400a40 ff4889ce 4889c7e8 1e000000 488b75e8
                                            .H..H......H.u.
 400a50 64483334 25280000 007405e8 10fdffff
                                            dH34%(...t....
 400a60 4881c438 0400005b 5dc35548 89e54883
                                            H..8...[].UH..H.
400a70 ec404889 7dd84889 75d04889 55c8488b
                                            .@H.}.H.u.H.U.H.
 400a80 45d04883 c00248ba abaaaaaa aaaaaaaa
                                            E.H...H.......
400a90 48f7e248 89d048d1 e8488d14 85000000
                                            H..H..H..H.....
 400aa0 00488b45 c8488910 488b45c8 488b00be
                                            .H.E.H..H.E.H...
400ab0 01000000 4889c7e8 f4fcffff 488945f8
                                            ....H.......H.E.
 400ac0 48837df8 00750ab8 00000000 e9c00100
                                            H. }..u......
400ad0 00c745e0 00000000 c745e400 000000e9
                                            ..E.....E....
 400ae0 3b010000 8b45e048 98483b45 d0731b8b
                                            ;....E.H.H;E.s..
400af0 45e08d50 018955e0 4863d048 8b45d848
                                            E..P..U.Hc.H.E.H
 400b00 01d00fb6 000fb6c0 eb05b800 00000089
                                            . . . . . . . . . . . . . . . .
```

```
400b10 45e88b45 e0489848 3b45d073 1b8b45e0
                                             E..E.H.H; E.s..E.
 400b20 8d500189 55e04863 d0488b45 d84801d0
                                             .P..U.Hc.H.E.H..
 400b30 0fb6000f b6c0eb05 b8000000 008945ec
                                             ....E.
 400b40 8b45e048 98483b45 d0731b8b 45e08d50
                                             .E.H.H; E.s..E..P
 400b50 018955e0 4863d048 8b45d848 01d00fb6
                                             ..U.Hc.H.E.H....
 400b60 000fb6c0 eb05b800 00000089 45f08b45
                                             ....E..E
 400b70 e8c1e010 89c28b45 ecc1e008 01c28b45
                                             ....E..E....E
 400b80 f001d089 45f48b45 e48d5001 8955e448
                                             ....E...E...P...U.H
 400b90 63d0488b 45f84801 c28b45f4 c1e81283
                                             c.H.E.H...E....
 400ba0 e03f89c0 0fb680c0 20600088 028b45e4
                                             .?...E.
 400bb0 8d500189 55e44863 d0488b45 f84801c2
                                             .P..U.Hc.H.E.H..
 400bc0 8b45f4c1 e80c83e0 3f89c00f b680c020
                                             .E....?...
                                             `....E..P..U.Hc.
 400bd0 60008802 8b45e48d 50018955 e44863d0
                                             H.E.H...E....?
 400be0 488b45f8 4801c28b 45f4c1e8 0683e03f
 400bf0 89c00fb6 80c02060 0088028b 45e48d50
                                             ...... `....E...P
 400c00 018955e4 4863d048 8b45f848 01c28b45
                                             ..U.Hc.H.E.H...E
 400c10 f483e03f 89c00fb6 80c02060 0088028b
                                             ...?.....`....
 400c20 45e04898 483b45d0 0f82b6fe ffffc745
                                             E.H.H; E.....E
                                             .....$H.E.H...E
 400c30 e0000000 00eb2448 8b45c848 8b108b45
 400c40 e0489848 29c24889 d0488d50 ff488b45
                                             .H.H).H..H.P.H.E
 400c50 f84801d0 c6003d83 45e00148 8b4dd048
                                             .H...=.E..H.M.H
 400c60 baabaaaa aaaaaaaa aa4889c8 48f7e248
                                             ........H..H..H
 400c70 d1ea4889 d04801c0 4801d048 29c14889
                                             ..H..H..H..H).H.
 400c80 ca8b0495 00216000 3b45e07f aa488b45
                                             ....!`.;E...H.E
 400c90 f8c9c366 2e0f1f84 00000000 000f1f00
                                             ...f.........
 400ca0 41574189 ff415649 89f64155 4989d541
                                             AWA..AVI..AUI..A
 400cb0 544c8d25 48112000 55488d2d 48112000
                                             TL.%H. .UH.-H. .
 400cc0 534c29e5 31db48c1 fd034883 ec08e835
                                             SL).1.H...H...5
 400cd0 faffff48 85ed741e 0f1f8400 00000000
                                             ...H..t......
 400ce0 4c89ea4c 89f64489 ff41ff14 dc4883c3
                                             L..L..D..A...H..
 400cf0 014839eb 75ea4883 c4085b5d 415c415d
                                             .H9.u.H...[]A\A]
 400d00 415e415f c366662e 0f1f8400 00000000
                                             A^A_.ff......
 400d10 f3c3
Contents of section .fini:
 400d14 4883ec08 4883c408 c3
                                             H...H...
Contents of section .rodata:
                                             ......34567890
 400d20 01000200 00000000 33343536 37383930
 400d30 31323334 35363738 39303132 00257325
                                             123456789012.%s%
                                             s....you win!
 400d40 730a0000 00000000 796f7520 77696e21
 400d50 20746865 20736563 72657420 69733a0a
                                              the secret is:.
 400d60 0062616e 67617261 6e670000 00000000
                                             .bangarang.....
 400d70 74686973 2070726f 6772616d 20746573
                                             this program tes
 400d80 74732074 68652069 6d706c65 6d656e74
                                             ts the implement
 400d90 6174696f 6e206f66 20612064 796e616d
                                             ation of a dynam
 400da0 6963616c 6c79206c 696e6b65 64206c69
                                             ically linked li
 400db0 62726172 792e0067 65745f73 756d2e63
                                             brary..get_sum.c
 400dc0 00726573 756c7420 3d3d2031 30007265
                                             .result == 10.re
 400dd0 73756c74 203d3d20 34006d61 696e00
                                             sult == 4.main.
Contents of section .eh frame hdr:
 400de0 011b033b 44000000 07000000 50f9ffff
                                             ...;D.....P...
 400df0 90000000 00faffff 60000000 edfaffff
                                             . . . . . . . . ` . . . . . . .
 400e00 b8000000 adfbffff d8000000 8afcffff
                                             . . . . . . . . . . . . . . . . .
 400e10 00010000 c0feffff 20010000 30ffffff
```

400e20 68010000	h
Contents of section .eh_frame:	
400e28 14000000 00000000 017a5200 01781001	zRx
400e38 1b0c0708 90010710 14000000 1c000000	
400e48 98f9ffff 2a000000 00000000 00000000	-D
400e58 14000000 00000000 017a5200 01781001	zRx
400e68 1b0c0708 90010000 24000000 1c000000	\$
400e78 b8f8ffff b0000000 000e1046 0e184a0f	FJ.
400e88 0b770880 003f1a3b 2a332422 00000000	.w?.;*3\$"
400e98 1c000000 44000000 2dfaffff c0000000	D
400ea8 00410e10 8602430d 0602bb0c 07080000	.AC
400eb8 24000000 64000000 cdfaffff dd000000	\$d
400ec8 00410e10 8602430d 06488303 02d00c07	.ACH
400ed8 08000000 00000000 1c000000 8c000000	
400ee8 82fbffff 29020000 00410e10 8602430d)AC.
400ef8 06032402 0c070800 44000000 ac000000	\$D
400f08 98fdffff 65000000 00420e10 8f02450e	eBE.
400f18 188e0345 0e208d04 450e288c 05480e30	EE.(H.0
400f28 8606480e 3883074d 0e406c0e 38410e30	H.8M.@l.8A.0
400f38 410e2842 0e20420e 18420e10 420e0800	A.(B. BBB
400f48 14000000 f4000000 c0fdffff 02000000	
400f58 00000000 00000000 00000000	
Contents of section .init_array:	
601e00 a0084000 00000000	@
Contents of section .fini_array:	
601e08 80084000 00000000	@
Contents of section .jcr:	
contents of section ijer.	
601-10 0000000 00000000	
601e10 00000000 00000000	
Contents of section .dynamic:	
Contents of section .dynamic: 601e18 01000000 00000000 01000000 00000000	
Contents of section .dynamic: 601e18 01000000 00000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000	
Contents of section .dynamic: 601e18 01000000 00000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000	
Contents of section .dynamic: 601e18 01000000 00000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000	
Contents of section .dynamic: 601e18 01000000 00000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000	
Contents of section .dynamic: 601e18 01000000 00000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e98 f5feff6f 00000000 98024000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e98 f5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98044000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e98 f5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 d0024000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e98 f5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98044000 00000000 601eb8 06000000 00000000 0e010000 00000000	
Contents of section .dynamic: 601e18 0100000 00000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 140d4000 00000000 601e48 0d00000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e98 f5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98044000 00000000 601eb8 06000000 00000000 00000000 00000000 601ec8 0a000000 00000000 0e010000 00000000 601ed8 0b000000 00000000 18000000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140044000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e98 f5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98044000 00000000 601eb8 06000000 00000000 00024000 00000000 601ec8 0a000000 00000000 18000000 00000000 601ed8 0b000000 00000000 00000000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e88 55feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98024000 00000000 601eb8 06000000 00000000 08000000 00000000 601ec8 0a000000 00000000 0e010000 00000000 601ec8 15000000 00000000 00000000 00000000 601ee8 15000000 00000000 00000000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e88 5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98044000 00000000 601eb8 06000000 00000000 00024000 00000000 601ec8 0a000000 00000000 0e010000 00000000 601ee8 15000000 00000000 18000000 00000000 601ef8 03000000 00000000 00206000 00000000 601ef8 03000000 00000000 00000000 000000000 601ef8 03000000 00000000 00000000 0000000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e88 55feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98024000 00000000 601eb8 06000000 00000000 08000000 00000000 601ec8 0a000000 00000000 0e010000 00000000 601ec8 15000000 00000000 00000000 00000000 601ee8 15000000 00000000 00000000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e88 5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98044000 00000000 601eb8 06000000 00000000 00024000 00000000 601ec8 0a000000 00000000 0e010000 00000000 601ee8 15000000 00000000 18000000 00000000 601ef8 03000000 00000000 00206000 00000000 601ef8 03000000 00000000 00000000 000000000 601ef8 03000000 00000000 00000000 0000000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e98 f5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98044000 00000000 601eb8 06000000 00000000 00024000 00000000 601ec8 0a000000 00000000 0e010000 00000000 601ee8 15000000 00000000 18000000 00000000 601ef8 03000000 00000000 00000000 00000000 601ef8 03000000 00000000 00000000 00000000 601ef8 03000000 00000000 00000000 000000000 601f08 02000000 00000000 07000000 00000000	
Contents of section .dynamic: 601e18 01000000 00000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d00000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e88 1c5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98024000 00000000 601ea8 05000000 00000000 08000000 00000000 601eb8 06000000 00000000 0e010000 00000000 601ec8 0a000000 00000000 0e010000 00000000 601e68 15000000 00000000 18000000 00000000 601e68 15000000 00000000 00000000 00000000 601e78 13000000 00000000 00000000 00000000 601e78 14000000 00000000 07000000 00000000 601f18 14000000 00000000 18064000 00000000	
Contents of section .dynamic: 601e18 01000000 000000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e98 f5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98024000 00000000 601eb8 06000000 00000000 08000000 00000000 601ec8 0a000000 00000000 00024000 00000000 601ec8 0a000000 00000000 18000000 00000000 601e68 15000000 00000000 00000000 00000000 601e18 03000000 00000000 00000000 00000000 601e18 15000000 00000000 00000000 00000000 601f18 14000000 00000000 18064000 00000000 601f18 14000000 00000000 18064000 000000000 601f38 07000000 00000000 18064000 000000000	
Contents of section .dynamic: 601e18 01000000 00000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 08000000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e98 f5feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98044000 00000000 601eb8 06000000 00000000 00024000 00000000 601ec8 0a000000 00000000 0e010000 00000000 601ed8 0b000000 00000000 18000000 00000000 601ef8 03000000 00000000 00206000 00000000 601f18 14000000 00000000 18064000 00000000 601f38 07000000 00000000 18000000 00000000 601f38 07000000 00000000 18000000 00000000	
Contents of section .dynamic: 601e18 01000000 00000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 08074000 00000000 601e48 0d000000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 081e6000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e88 15feff6f 00000000 98024000 00000000 601ea8 05000000 00000000 98044000 00000000 601eb8 06000000 00000000 00024000 00000000 601ec8 0a000000 00000000 18000000 00000000 601ed8 0b000000 00000000 18000000 00000000 601ef8 03000000 00000000 00000000 00000000 601f18 14000000 00000000 18064000 00000000 601f38 07000000 00000000 18000000 00000000	
Contents of section .dynamic: 601e18 01000000 00000000 01000000 00000000 601e28 01000000 00000000 80000000 00000000 601e38 0c000000 00000000 140d4000 00000000 601e48 0d00000 00000000 140d4000 00000000 601e58 19000000 00000000 001e6000 00000000 601e68 1b000000 00000000 08000000 00000000 601e78 1a000000 00000000 081e6000 00000000 601e88 1c000000 00000000 08000000 00000000 601e88 1c000000 00000000 98024000 00000000 601ea8 05000000 00000000 98024000 00000000 601ea8 05000000 00000000 00024000 00000000 601eb8 06000000 00000000 0e010000 00000000 601ec8 0a000000 00000000 18000000 00000000 601ed8 0b000000 00000000 18000000 00000000 601f18 14000000 00000000 18000000 00000000 601f18 14000000 00000000 18000000 00000000 601f38 07000000 00000000 18000000 00000000 601f38 07000000 00000000 18000000 00000000 601f48 08000000 00000000 18000000 00000000 601f58 09000000 00000000 18000000 00000000 601f58 09000000 00000000 18000000 00000000	

```
601f98 00000000 00000000 00000000 00000000
 601fa8 00000000 00000000 00000000 00000000
 601fb8 00000000 00000000 00000000 00000000
 601fc8 00000000 00000000 00000000 00000000
 601fd8 00000000 00000000 00000000 00000000
 601fe8 00000000 00000000 00000000 00000000
Contents of section .got:
 601ff8 00000000 00000000
Contents of section .got.plt:
 602000 181e6000 00000000 00000000 00000000
                                            . . ` . . . . . . . . . . . . .
 602010 00000000 00000000 46074000 00000000
                                            .....F.@....
 602020 56074000 00000000 66074000 00000000
                                            V.@....f.@....
 602030 76074000 00000000 86074000 00000000
                                            602040 96074000 00000000 a6074000 00000000
                                            ..@.....@....
 602050 b6074000 00000000 c6074000 00000000
                                            602060 d6074000 00000000
                                            .....
Contents of section .data:
 . . . . . . . . . . . . . . . .
 602090 280d4000 00000000 3d0d4000 00000000
                                            (.@....=.@.....
 6020a0 480d4000 00000000 00000000 00000000
                                            H.@.....
 . . . . . . . . . . . . . . . .
 6020c0 41424344 45464748 494a4b4c 4d4e4f50
                                            ABCDEFGHIJKLMNOP
 6020d0 51525354 55565758 595a6162 63646566
                                            ORSTUVWXYZabcdef
 6020e0 6768696a 6b6c6d6e 6f707172 73747576
                                            ghijklmnopgrstuv
 6020f0 7778797a 30313233 34353637 38392b2f
                                            wxyz0123456789+/
 602100 00000000 02000000 01000000
                                            . . . . . . . . . . . .
Contents of section .comment:
 0000 4743433a 20285562 756e7475 20342e38 GCC: (Ubuntu 4.8
 0010 2e342d32 7562756e 7475317e 31342e30
                                          .4-2ubuntu1~14.0
 0020 34292034 2e382e34 00474343 3a202855
                                          4) 4.8.4.GCC: (U
 0030 62756e74 7520342e 382e322d 31397562
                                          buntu 4.8.2-19ub
 0040 756e7475 31292034 2e382e32 00
                                          untu1) 4.8.2.
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -S 4
4:
      file format elf64-x86-64
Disassembly of section .init:
0000000000400708 < init>:
  400708:
               48 83 ec 08
                                       sub
                                              $0x8,%rsp
  40070c:
               48 8b 05 e5 18 20 00
                                              0x2018e5(%rip),%rax
                                                                        # 601ff
                                       mov
8 < fini+0x2012e4>
               48 85 c0
  400713:
                                       test
                                              %rax,%rax
               74 05
  400716:
                                       jе
                                              40071d < init+0x15>
               e8 a3 00 00 00
                                              4007c0 <__gmon_start__@plt>
  400718:
                                       callq
  40071d:
               48 83 c4 08
                                       add
                                              $0x8,%rsp
  400721:
               с3
                                       retq
Disassembly of section .plt:
0000000000400730 <puts@plt-0x10>:
               ff 35 d2 18 20 00
  400730:
                                       pushg 0x2018d2(%rip)
                                                                   # 602008 < f
```

ini+0x2012f4> 400736:	ff	25	d4	18	20	00	jmpq	*0×2018d4(%rip)	# 60	02010 <_
fini+0x2012fc>			٠.	10			764	10X201041(011p)	" 00	
40073c:	0f	1f	40	00			nopl	0x0(%rax)		
000000000400740 <puts@plt>:</puts@plt>										
400740:	ff	25	d2	18	20	00	jmpq	*0x2018d2(%rip)	# 60	02018 <_
fini+0x201304>	60	00	00	00	00		nucha	# A v A		
400746: 40074b:				00 ff			pushq jmpq	\$0x0 400730 <_init+0x28>		
400740.	CJ	CU	' '	' '	' '		Jiiibd	400/30 _IIII110X20>		
000000000040075				•						
400750:	ff	25	ca	18	20	00	jmpq	*0x2018ca(%rip)	# 60	02020 <_
fini+0x20130c>										
400756:				00			pushq	\$0x1		
40075b:	e9	αv	ТТ	ff	TT		jmpq	400730 <_init+0x28>		
000000000400760 <strlen@plt>:</strlen@plt>										
400760:	ff	25	c2	18	20	00	jmpq	*0x2018c2(%rip)	# 60	02028 <_
fini+0x201314>										
400766:		-		00			pushq	\$0x2		
40076b:	e9	с0	ff	ff	ff		jmpq	400730 <_init+0x28>		
000000000040077	0 <	s.	tacl	k cl	nk t	fail@nlt>	•			
400770:				18			jmpq	*0x2018ba(%rip)	# 60	02030 <
fini+0x20131c>							J 1 1	μ,		_
400776:	68	03	00	00	00		pushq	\$0x3		
40077b:	e9	b0	ff	ff	ff		jmpq	400730 <_init+0x28>		
000000000040078	a -	nrii	n + f/	an 1 -	+ <					
400780:				18		00	jmpq	*0x2018b2(%rip)	# 60	02038 <_
fini+0x201324>		23	52	10	20	00	Jiiipq	#0X201002 (01 1p)	# 00	72030 _
400786:	68	04	00	00	00		pushq	\$0×4		
40078b:				ff			jmpq '	400730 <_init+0x28>		
	_									
000000000040079							·	.02010(0)	ш сс	2040 .
400790: fini+0x20132c>	ТТ	25	aa	18	20	00	jmpq	*0x2018aa(%rip)	# 00	02040 <_
400796:	68	05	aa	00	aa		pushq	\$0x5		
40079b:							jmpq	400730 <_init+0x28>		
40079b: e9 90 ff ff ff jmpq 400730 <_init+0x28>										
00000000004007a							>:			
4007a0:	ff	25	a2	18	20	00	jmpq	*0x2018a2(%rip)	# 60	02048 <_
fini+0x201334>								+0.0		
4007a6:				00			pushq	\$0x6		
4007ab:	е9	00	11	11	11		jmpq	400730 <_init+0x28>		
00000000004007b	0 <	cal	loc	gpl ⁻	t>:					
4007b0:				18		00	jmpq	*0x20189a(%rip)	# 60	02050 <_
fini+0x20133c>										
4007b6:				00			pushq	\$0×7		
4007bb:	e9	70	† f	ff	ff		jmpq	400730 <_init+0x28>		

```
0000000004007c0 <__gmon_start__@plt>:
                ff 25 92 18 20 00
  4007c0:
                                                  *0x201892(%rip)
                                                                          # 602058 <
                                          jmpq
fini+0x201344>
  4007c6:
                 68 08 00 00 00
                                          pushq
                                                  $0x8
                 e9 60 ff ff ff
  4007cb:
                                          jmpq
                                                  400730 <_init+0x28>
0000000004007d0 <getlogin_r@plt>:
                 ff 25 8a 18 20 00
  4007d0:
                                                  *0x20188a(%rip)
                                                                          # 602060 <_
                                          jmpq
fini+0x20134c>
  4007d6:
                 68 09 00 00 00
                                          pushq
                                                  $0x9
  4007db:
                e9 50 ff ff ff
                                          jmpq
                                                  400730 <_init+0x28>
Disassembly of section .text:
000000000004007e0 <.text>:
  4007e0:
                 31 ed
                                          xor
                                                  %ebp,%ebp
  4007e2:
                 49 89 d1
                                                  %rdx,%r9
                                          mov
                 5e
  4007e5:
                                                  %rsi
                                          pop
  4007e6:
                 48 89 e2
                                          mov
                                                  %rsp,%rdx
                 48 83 e4 f0
  4007e9:
                                          and
                                                  $0xffffffffffffff,%rsp
                 50
  4007ed:
                                          push
                                                  %rax
                 54
  4007ee:
                                          push
                                                  %rsp
                 49 c7 c0 10 0d 40 00
                                                  $0x400d10,%r8
  4007ef:
                                          mov
                 48 c7 c1 a0 0c 40 00
  4007f6:
                                          mov
                                                  $0x400ca0,%rcx
                 48 c7 c7 cd 08 40 00
  4007fd:
                                          mov
                                                  $0x4008cd,%rdi
                 e8 97 ff ff ff
                                                  4007a0 < libc start main@plt>
  400804:
                                          callq
  400809:
                 f4
                                          hlt
                 66 0f 1f 44 00 00
  40080a:
                                          nopw
                                                  0x0(%rax,%rax,1)
  400810:
                 b8 17 21 60 00
                                          mov
                                                  $0x602117,%eax
                 55
  400815:
                                                  %rbp
                                          push
  400816:
                 48 2d 10 21 60 00
                                                  $0x602110,%rax
                                          sub
  40081c:
                 48 83 f8 0e
                                                  $0xe,%rax
                                          cmp
                 48 89 e5
  400820:
                                          mov
                                                  %rsp,%rbp
  400823:
                 77 02
                                                  400827 <getlogin r@plt+0x57>
                                          jа
  400825:
                 5d
                                                  %rbp
                                          pop
  400826:
                 с3
                                          retq
  400827:
                 b8 00 00 00 00
                                          mov
                                                  $0x0,%eax
                 48 85 c0
  40082c:
                                          test
                                                  %rax,%rax
  40082f:
                 74 f4
                                                  400825 <getlogin_r@plt+0x55>
                                          jе
  400831:
                 5d
                                                  %rbp
                                          pop
  400832:
                bf 10 21 60 00
                                          mov
                                                  $0x602110,%edi
  400837:
                 ff e0
                                                  *%rax
                                          jmpq
  400839:
                 0f 1f 80 00 00 00 00
                                          nopl
                                                  0x0(%rax)
  400840:
                 b8 10 21 60 00
                                          mov
                                                  $0x602110,%eax
  400845:
                 55
                                          push
                                                  %rbp
                 48 2d 10 21 60 00
  400846:
                                          sub
                                                  $0x602110,%rax
  40084c:
                 48 c1 f8 03
                                                  $0x3,%rax
                                          sar
                 48 89 e5
  400850:
                                          mov
                                                  %rsp,%rbp
  400853:
                 48 89 c2
                                          mov
                                                  %rax,%rdx
                 48 c1 ea 3f
  400856:
                                          shr
                                                  $0x3f,%rdx
                 48 01 d0
  40085a:
                                          add
                                                  %rdx,%rax
                 48 d1 f8
  40085d:
                                          sar
                                                  %rax
  400860:
                 75 02
                                          jne
                                                  400864 <getlogin_r@plt+0x94>
```

```
400862:
                 5d
                                                  %rbp
                                           pop
  400863:
                 с3
                                           retq
  400864:
                 ba 00 00 00 00
                                           mov
                                                  $0x0,%edx
                 48 85 d2
  400869:
                                                  %rdx,%rdx
                                           test
                 74 f4
                                                  400862 <getlogin_r@plt+0x92>
  40086c:
                                           jе
  40086e:
                 5d
                                                  %rbp
                                           pop
                 48 89 c6
  40086f:
                                                  %rax,%rsi
                                           mov
                 bf 10 21 60 00
  400872:
                                                  $0x602110,%edi
                                           mov
  400877:
                 ff e2
                                           jmpq
                                                  *%rdx
                 0f 1f 80 00 00 00 00
  400879:
                                           nopl
                                                  0x0(%rax)
  400880:
                 80 3d 85 18 20 00 00
                                           cmpb
                                                  $0x0,0x201885(%rip)
                                                                                # 60210
c <_edata>
  400887:
                 75 11
                                           ine
                                                  40089a <getlogin_r@plt+0xca>
  400889:
                 55
                                           push
                                                  %rbp
  40088a:
                 48 89 e5
                                           mov
                                                  %rsp,%rbp
  40088d:
                 e8 7e ff ff ff
                                           callq
                                                  400810 <getlogin_r@plt+0x40>
  400892:
                 5d
                                           pop
                                                  %rbp
                                                  $0x1,0x201872(%rip)
  400893:
                 c6 05 72 18 20 00 01
                                           movb
                                                                                # 60210
c <_edata>
  40089a:
                 f3 c3
                                           repz retq
  40089c:
                 0f 1f 40 00
                                           nopl
                                                  0x0(%rax)
                 48 83 3d 68 15 20 00
  4008a0:
                                           cmpq
                                                   $0x0,0x201568(%rip)
                                                                                # 601e1
0 < fini+0x2010fc>
  4008a7:
                 00
                 74 1e
  4008a8:
                                           jе
                                                  4008c8 <getlogin_r@plt+0xf8>
                 b8 00 00 00 00
  4008aa:
                                           mov
                                                  $0x0,%eax
  4008af:
                 48 85 c0
                                           test
                                                  %rax,%rax
                 74 14
  4008b2:
                                                  4008c8 <getlogin r@plt+0xf8>
                                           jе
  4008b4:
                 55
                                           push
                                                  %rbp
                 bf 10 1e 60 00
  4008b5:
                                                   $0x601e10,%edi
                                           mov
  4008ba:
                 48 89 e5
                                                  %rsp,%rbp
                                           mov
  4008bd:
                 ff d0
                                           callq
                                                  *%rax
  4008bf:
                 5d
                                           pop
                                                  %rbp
                 e9 7b ff ff ff
                                                  400840 <getlogin_r@plt+0x70>
  4008c0:
                                           jmpq
  4008c5:
                 0f 1f 00
                                           nopl
                                                  (%rax)
                 e9 73 ff ff ff
  4008c8:
                                                  400840 < \text{getlogin r@plt+0x70}
                                           jmpq
  4008cd:
                 55
                                           push
                                                  %rbp
                 48 89 e5
                                                  %rsp,%rbp
  4008ce:
                                           mov
  4008d1:
                 48 83 ec 10
                                           sub
                                                  $0x10,%rsp
                 c7 45 f4 01 00 00 00
                                                  $0x1,-0xc(%rbp)
  4008d5:
                                           movl
  4008dc:
                 c7 45 f8 02 00 00 00
                                           movl
                                                  $0x2,-0x8(%rbp)
                 c7 45 fc 00 00 00 00
  4008e3:
                                           movl
                                                  $0x0,-0x4(%rbp)
                 bf 70 0d 40 00
  4008ea:
                                           mov
                                                  $0x400d70,%edi
                 e8 4c fe ff ff
  4008ef:
                                           callq
                                                  400740 <puts@plt>
  4008f4:
                 be 06 00 00 00
                                           mov
                                                  $0x6,%esi
                 bf 03 00 00 00
                                                   $0x3,%edi
  4008f9:
                                           mov
  4008fe:
                 e8 4d fe ff ff
                                           callq
                                                  400750 <secretoperation@plt>
                 89 45 fc
                                                  %eax,-0x4(%rbp)
  400903:
                                           mov
                 83 7d fc 0a
  400906:
                                           cmpl
                                                  $0xa,-0x4(%rbp)
                                                  400925 <getlogin_r@plt+0x155>
                 74 19
  40090a:
                                           jе
                 b9 da 0d 40 00
  40090c:
                                           mov
                                                   $0x400dda,%ecx
                 ba 12 00 00 00
                                                  $0x12,%edx
  400911:
                                           mov
  400916:
                 be b7 0d 40 00
                                           mov
                                                  $0x400db7,%esi
```

```
40091b:
                 bf c1 0d 40 00
                                                  $0x400dc1,%edi
                                          mov
                 e8 6b fe ff ff
                                                  400790 <__assert_fail@plt>
  400920:
                                          callq
                8b 55 f8
                                                  -0x8(%rbp),%edx
  400925:
                                          mov
                8b 45 f4
  400928:
                                                  -0xc(%rbp),%eax
                                          mov
                89 d6
  40092b:
                                                  %edx,%esi
                                          mov
                89 c7
                                                  %eax,%edi
  40092d:
                                          mov
  40092f:
                e8 1c fe ff ff
                                                  400750 <secretoperation@plt>
                                          callq
                89 45 fc
                                                  %eax,-0x4(%rbp)
  400934:
                                          mov
  400937:
                83 7d fc 04
                                          cmpl
                                                  $0x4,-0x4(%rbp)
                74 19
                                                  400956 <getlogin_r@plt+0x186>
  40093b:
                                          jе
  40093d:
                b9 da 0d 40 00
                                          mov
                                                  $0x400dda,%ecx
  400942:
                ba 14 00 00 00
                                                  $0x14,%edx
                                          mov
  400947:
                be b7 0d 40 00
                                                  $0x400db7,%esi
                                          mov
  40094c:
                bf ce 0d 40 00
                                                  $0x400dce,%edi
                                          mov
  400951:
                e8 3a fe ff ff
                                          callq
                                                  400790 <__assert_fail@plt>
  400956:
                48 8b 05 33 17 20 00
                                          mov
                                                  0x201733(%rip),%rax
                                                                              # 60209
0 <_fini+0x20137c>
  40095d:
                48 89 c7
                                                  %rax,%rdi
                                          mov
  400960:
                 e8 28 00 00 00
                                          callq
                                                  40098d <getlogin_r@plt+0x1bd>
  400965:
                48 89 c2
                                          mov
                                                  %rax,%rdx
                48 8b 0d 31 17 20 00
  400968:
                                          mov
                                                  0x201731(%rip),%rcx
                                                                              # 6020a
0 < fini+0x20138c>
                48 8b 05 22 17 20 00
                                                  0x201722(%rip),%rax
  40096f:
                                          mov
                                                                              # 60209
8 < fini+0x201384>
  400976:
                48 89 ce
                                                  %rcx,%rsi
                                          mov
  400979:
                 48 89 c7
                                                  %rax,%rdi
                                          mov
  40097c:
                b8 00 00 00 00
                                          mov
                                                  $0x0,%eax
                 e8 fa fd ff ff
                                                  400780 <printf@plt>
  400981:
                                          callq
  400986:
                b8 00 00 00 00
                                                  $0x0,%eax
                                          mov
                 с9
  40098b:
                                          leaveq
  40098c:
                 с3
                                          retq
  40098d:
                 55
                                          push
                                                  %rbp
  40098e:
                48 89 e5
                                          mov
                                                  %rsp,%rbp
  400991:
                53
                                                  %rbx
                                          push
  400992:
                48 81 ec 38 04 00 00
                                          sub
                                                  $0x438,%rsp
                48 89 bd c8 fb ff ff
                                                  %rdi,-0x438(%rbp)
  400999:
                                          mov
  4009a0:
                64 48 8b 04 25 28 00
                                          mov
                                                  %fs:0x28,%rax
                 00 00
  4009a7:
  4009a9:
                48 89 45 e8
                                                  %rax,-0x18(%rbp)
                                          mov
                                                  %eax,%eax
  4009ad:
                31 c0
                                          xor
  4009af:
                48 8d 85 e0 fb ff ff
                                          lea
                                                  -0x420(%rbp),%rax
  4009b6:
                be 00 04 00 00
                                          mov
                                                  $0x400,%esi
  4009bb:
                48 89 c7
                                          mov
                                                  %rax,%rdi
                 e8 0d fe ff ff
                                                  4007d0 <getlogin_r@plt>
  4009be:
                                          calla
  4009c3:
                 c7 85 d4 fb ff ff 00
                                          movl
                                                  $0x0,-0x42c(%rbp)
                 00 00 00
  4009ca:
                                                  400a0d <getlogin_r@plt+0x23d>
  4009cd:
                 eb 3e
                                          jmp
                 8b 85 d4 fb ff ff
                                                  -0x42c(%rbp),%eax
  4009cf:
                                          mov
  4009d5:
                 48 98
                                          cltq
  4009d7:
                 0f b6 94 05 e0 fb ff
                                          movzbl -0x420(%rbp,%rax,1),%edx
                 ff
  4009de:
  4009df:
                 8b 85 d4 fb ff ff
                                                  -0x42c(%rbp),%eax
                                          mov
  4009e5:
                 48 63 c8
                                          movslq %eax,%rcx
```

```
4009e8:
               48 8b 85 c8 fb ff ff
                                                -0x438(%rbp),%rax
                                        mov
4009ef:
               48 01 c8
                                        add
                                                %rcx,%rax
               0f b6 00
                                        movzbl (%rax),%eax
4009f2:
               31 c2
4009f5:
                                                %eax,%edx
                                        xor
               8b 85 d4 fb ff ff
                                                -0x42c(%rbp),%eax
4009f7:
                                        mov
               48 98
4009fd:
                                        cltq
4009ff:
               88 94 05 e0 fb ff ff
                                                %dl,-0x420(%rbp,%rax,1)
                                        mov
              83 85 d4 fb ff ff 01
                                                $0x1,-0x42c(%rbp)
400a06:
                                        addl
400a0d:
              8b 85 d4 fb ff ff
                                        mov
                                                -0x42c(%rbp),%eax
              48 63 d8
400a13:
                                        movslq %eax,%rbx
400a16:
              48 8d 85 e0 fb ff ff
                                        lea
                                                -0x420(%rbp),%rax
400a1d:
              48 89 c7
                                                %rax,%rdi
                                        mov
400a20:
              e8 3b fd ff ff
                                        callq
                                                400760 <strlen@plt>
400a25:
              48 39 c3
                                                %rax,%rbx
                                        cmp
400a28:
              72 a5
                                        jb
                                                4009cf <getlogin_r@plt+0x1ff>
                                        mov
400a2a:
              8b 85 d4 fb ff ff
                                                -0x42c(%rbp),%eax
400a30:
              48 63 c8
                                        movslq %eax,%rcx
              48 8d 95 d8 fb ff ff
400a33:
                                        lea
                                                -0x428(%rbp),%rdx
400a3a:
               48 8d 85 e0 fb ff ff
                                        lea
                                                -0x420(%rbp),%rax
              48 89 ce
400a41:
                                        mov
                                                %rcx,%rsi
              48 89 c7
                                                %rax,%rdi
400a44:
                                        mov
               e8 1e 00 00 00
                                                400a6a <getlogin_r@plt+0x29a>
400a47:
                                        callq
              48 8b 75 e8
                                                -0x18(%rbp),%rsi
400a4c:
                                        mov
              64 48 33 34 25 28 00
400a50:
                                        xor
                                                %fs:0x28,%rsi
400a57:
               00 00
               74 05
                                                400a60 <getlogin r@plt+0x290>
400a59:
                                        jе
400a5b:
               e8 10 fd ff ff
                                        callq
                                                400770 <__stack_chk_fail@plt>
               48 81 c4 38 04 00 00
400a60:
                                        add
                                                $0x438,%rsp
400a67:
               5b
                                                %rbx
                                        pop
              5d
                                                %rbp
400a68:
                                        pop
400a69:
               с3
                                        retq
400a6a:
              55
                                        push
                                                %rbp
400a6b:
              48 89 e5
                                                %rsp,%rbp
                                        mov
400a6e:
              48 83 ec 40
                                                $0x40,%rsp
                                        sub
400a72:
              48 89 7d d8
                                        mov
                                                %rdi,-0x28(%rbp)
              48 89 75 d0
400a76:
                                                %rsi,-0x30(%rbp)
                                        mov
400a7a:
              48 89 55 c8
                                        mov
                                                %rdx,-0x38(%rbp)
              48 8b 45 d0
400a7e:
                                        mov
                                                -0x30(%rbp),%rax
400a82:
              48 83 c0 02
                                        add
                                                $0x2,%rax
              48 ba ab aa aa aa
400a86:
                                        movabs $0xaaaaaaaaaaaaab,%rdx
400a8d:
               aa aa aa
               48 f7 e2
400a90:
                                        mul
                                                %rdx
400a93:
               48 89 d0
                                        mov
                                                %rdx,%rax
400a96:
               48 d1 e8
                                        shr
                                                %rax
400a99:
               48 8d 14 85 00 00 00
                                        lea
                                                0x0(,%rax,4),%rdx
               00
400aa0:
400aa1:
              48 8b 45 c8
                                        mov
                                                -0x38(%rbp),%rax
               48 89 10
                                                %rdx,(%rax)
400aa5:
                                        mov
400aa8:
              48 8b 45 c8
                                        mov
                                                -0x38(%rbp),%rax
                                                (%rax),%rax
400aac:
              48 8b 00
                                        mov
400aaf:
              be 01 00 00 00
                                        mov
                                                $0x1,%esi
              48 89 c7
                                                %rax,%rdi
400ab4:
                                        mov
              e8 f4 fc ff ff
                                                4007b0 <calloc@plt>
400ab7:
                                        callq
```

```
400abc:
               48 89 45 f8
                                                %rax,-0x8(%rbp)
                                        mov
              48 83 7d f8 00
                                                $0x0,-0x8(%rbp)
400ac0:
                                        cmpq
              75 0a
                                                400ad1 <getlogin_r@plt+0x301>
400ac5:
                                        jne
              b8 00 00 00 00
400ac7:
                                        mov
                                                $0x0,%eax
              e9 c0 01 00 00
                                                400c91 <getlogin_r@plt+0x4c1>
400acc:
                                        jmpq
              c7 45 e0 00 00 00 00
                                                $0x0,-0x20(%rbp)
400ad1:
                                        movl
400ad8:
               c7 45 e4 00 00 00 00
                                                $0x0.-0x1c(%rbp)
                                        movl
              e9 3b 01 00 00
400adf:
                                                400c1f <getlogin_r@plt+0x44f>
                                        jmpq
400ae4:
              8b 45 e0
                                        mov
                                                -0x20(%rbp),%eax
              48 98
400ae7:
                                        cltq
400ae9:
              48 3b 45 d0
                                        cmp
                                                -0x30(%rbp),%rax
400aed:
              73 1b
                                                400b0a <getlogin_r@plt+0x33a>
                                        jae
400aef:
              8b 45 e0
                                                -0x20(%rbp),%eax
                                        mov
400af2:
              8d 50 01
                                        lea
                                                0x1(%rax),%edx
400af5:
              89 55 e0
                                                %edx,-0x20(%rbp)
                                        mov
400af8:
              48 63 d0
                                        movslq %eax,%rdx
400afb:
              48 8b 45 d8
                                        mov
                                                -0x28(%rbp),%rax
              48 01 d0
400aff:
                                        add
                                                %rdx,%rax
                                        movzbl (%rax),%eax
400b02:
               0f b6 00
              0f b6 c0
                                        movzbl %al,%eax
400b05:
              eb 05
                                                400b0f <getlogin_r@plt+0x33f>
400b08:
                                        jmp
              b8 00 00 00 00
400b0a:
                                        mov
                                                $0x0,%eax
              89 45 e8
                                                %eax,-0x18(%rbp)
400b0f:
                                        mov
                                                -0x20(%rbp),%eax
400b12:
              8b 45 e0
                                        mov
              48 98
400b15:
                                        cltq
              48 3b 45 d0
                                                -0x30(%rbp),%rax
400b17:
                                        cmp
400b1b:
              73 1b
                                        jae
                                                400b38 <getlogin_r@plt+0x368>
                                                -0x20(%rbp),%eax
400b1d:
              8b 45 e0
                                        mov
400b20:
              8d 50 01
                                                0x1(%rax),%edx
                                        lea
              89 55 e0
                                                %edx,-0x20(%rbp)
400b23:
                                        mov
400b26:
              48 63 d0
                                        movslq %eax,%rdx
400b29:
              48 8b 45 d8
                                        mov
                                                -0x28(%rbp),%rax
400b2d:
              48 01 d0
                                        add
                                                %rdx,%rax
400b30:
              0f b6 00
                                        movzbl (%rax),%eax
400b33:
              0f b6 c0
                                        movzbl %al,%eax
400b36:
              eb 05
                                                400b3d <getlogin r@plt+0x36d>
                                        jmp
400b38:
              b8 00 00 00 00
                                        mov
                                                $0x0,%eax
              89 45 ec
                                                %eax,-0x14(%rbp)
400b3d:
                                        mov
400b40:
              8b 45 e0
                                                -0x20(%rbp),%eax
                                        mov
              48 98
400b43:
                                        cltq
400b45:
              48 3b 45 d0
                                        cmp
                                                -0x30(%rbp),%rax
              73 1b
400b49:
                                        jae
                                                400b66 <getlogin_r@plt+0x396>
400b4b:
              8b 45 e0
                                        mov
                                                -0x20(%rbp),%eax
              8d 50 01
400b4e:
                                        lea
                                                0x1(%rax),%edx
400b51:
              89 55 e0
                                        mov
                                                %edx,-0x20(%rbp)
              48 63 d0
                                        movslq %eax,%rdx
400b54:
400b57:
              48 8b 45 d8
                                        mov
                                                -0x28(%rbp),%rax
              48 01 d0
                                                %rdx,%rax
400b5b:
                                        add
                                        movzbl (%rax),%eax
400b5e:
              0f b6 00
400b61:
              0f b6 c0
                                        movzbl %al,%eax
400b64:
              eb 05
                                        jmp
                                                400b6b <getlogin_r@plt+0x39b>
400b66:
               b8 00 00 00 00
                                                $0x0,%eax
                                        mov
                                                %eax,-0x10(%rbp)
400b6b:
              89 45 f0
                                        mov
```

```
400b6e:
               8b 45 e8
                                                -0x18(%rbp),%eax
                                         mov
400b71:
               c1 e0 10
                                         shl
                                                 $0x10,%eax
400b74:
               89 c2
                                                %eax,%edx
                                         mov
400b76:
               8b 45 ec
                                                -0x14(%rbp),%eax
                                         mov
400b79:
               c1 e0 08
                                                 $0x8,%eax
                                         shl
                                                %eax,%edx
400b7c:
               01 c2
                                         add
               8b 45 f0
                                                -0x10(%rbp),%eax
400b7e:
                                         mov
400b81:
               01 d0
                                                %edx,%eax
                                         add
400b83:
               89 45 f4
                                                %eax,-0xc(%rbp)
                                         mov
               8b 45 e4
                                                -0x1c(%rbp),%eax
400b86:
                                         mov
400b89:
               8d 50 01
                                         lea
                                                0x1(%rax),%edx
               89 55 e4
                                                %edx,-0x1c(%rbp)
400b8c:
                                         mov
               48 63 d0
400b8f:
                                         movslq %eax,%rdx
               48 8b 45 f8
                                                -0x8(%rbp),%rax
400b92:
                                         mov
400b96:
               48 01 c2
                                                %rax,%rdx
                                         add
                                                -0xc(%rbp),%eax
400b99:
               8b 45 f4
                                         mov
400b9c:
               c1 e8 12
                                         shr
                                                 $0x12,%eax
400b9f:
               83 e0 3f
                                                $0x3f,%eax
                                         and
400ba2:
               89 c0
                                         mov
                                                %eax,%eax
400ba4:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400bab:
               88 02
                                         mov
                                                %al,(%rdx)
               8b 45 e4
400bad:
                                         mov
                                                -0x1c(%rbp),%eax
               8d 50 01
                                                0x1(%rax),%edx
400bb0:
                                         lea
               89 55 e4
400bb3:
                                         mov
                                                %edx,-0x1c(%rbp)
400bb6:
               48 63 d0
                                         movslq %eax,%rdx
               48 8b 45 f8
400bb9:
                                                -0x8(%rbp),%rax
                                         mov
400bbd:
               48 01 c2
                                         add
                                                %rax,%rdx
               8b 45 f4
                                                -0xc(%rbp),%eax
400bc0:
                                         mov
400bc3:
               c1 e8 0c
                                                 $0xc,%eax
                                         shr
               83 e0 3f
                                                 $0x3f,%eax
400bc6:
                                         and
400bc9:
               89 c0
                                                %eax,%eax
                                         mov
400bcb:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400bd2:
               88 02
                                                %al,(%rdx)
                                         mov
                                                -0x1c(%rbp),%eax
               8b 45 e4
400bd4:
                                         mov
400bd7:
               8d 50 01
                                         lea
                                                0x1(%rax),%edx
400bda:
               89 55 e4
                                                %edx,-0x1c(%rbp)
                                         mov
400bdd:
               48 63 d0
                                         movslq %eax,%rdx
400be0:
               48 8b 45 f8
                                                -0x8(%rbp),%rax
                                         mov
400be4:
               48 01 c2
                                         add
                                                %rax,%rdx
               8b 45 f4
400be7:
                                         mov
                                                -0xc(%rbp),%eax
400bea:
               c1 e8 06
                                         shr
                                                $0x6,%eax
400bed:
               83 e0 3f
                                         and
                                                $0x3f,%eax
400bf0:
               89 c0
                                         mov
                                                %eax,%eax
400bf2:
               0f b6 80 c0 20 60 00
                                         movzbl 0x6020c0(%rax),%eax
400bf9:
               88 02
                                         mov
                                                %al,(%rdx)
               8b 45 e4
400bfb:
                                         mov
                                                -0x1c(%rbp),%eax
                                                0x1(%rax),%edx
400bfe:
               8d 50 01
                                         lea
                                                %edx,-0x1c(%rbp)
400c01:
               89 55 e4
                                         mov
400c04:
               48 63 d0
                                         movslq %eax,%rdx
400c07:
               48 8b 45 f8
                                         mov
                                                -0x8(%rbp),%rax
400c0b:
               48 01 c2
                                         add
                                                %rax,%rdx
               8b 45 f4
                                                -0xc(%rbp),%eax
400c0e:
                                         mov
400c11:
               83 e0 3f
                                         and
                                                 $0x3f,%eax
```

```
400c14:
                 89 c0
                                                  %eax,%eax
                                           mov
                 0f b6 80 c0 20 60 00
  400c16:
                                           movzbl 0x6020c0(%rax),%eax
  400c1d:
                 88 02
                                           mov
                                                  %al,(%rdx)
                 8b 45 e0
  400c1f:
                                                  -0x20(%rbp),%eax
                                           mov
                 48 98
                                           cltq
  400c22:
                 48 3b 45 d0
  400c24:
                                           cmp
                                                  -0x30(%rbp),%rax
  400c28:
                 0f 82 b6 fe ff ff
                                                  400ae4 <getlogin_r@plt+0x314>
                                           jb
                 c7 45 e0 00 00 00 00
  400c2e:
                                           movl
                                                  $0x0,-0x20(%rbp)
  400c35:
                 eb 24
                                           jmp
                                                  400c5b <getlogin_r@plt+0x48b>
                 48 8b 45 c8
  400c37:
                                           mov
                                                  -0x38(%rbp),%rax
  400c3b:
                 48 8b 10
                                           mov
                                                  (%rax),%rdx
                 8b 45 e0
                                                  -0x20(%rbp),%eax
  400c3e:
                                           mov
                 48 98
  400c41:
                                           cltq
  400c43:
                 48 29 c2
                                                  %rax,%rdx
                                           sub
  400c46:
                 48 89 d0
                                           mov
                                                  %rdx,%rax
                 48 8d 50 ff
  400c49:
                                           lea
                                                  -0x1(%rax),%rdx
  400c4d:
                 48 8b 45 f8
                                           mov
                                                  -0x8(%rbp),%rax
  400c51:
                48 01 d0
                                           add
                                                  %rdx,%rax
  400c54:
                 c6 00 3d
                                           movb
                                                  $0x3d,(%rax)
                 83 45 e0 01
                                                  $0x1,-0x20(%rbp)
  400c57:
                                           addl
                 48 8b 4d d0
                                                  -0x30(%rbp),%rcx
  400c5b:
                                           mov
                 48 ba ab aa aa aa
  400c5f:
                                           movabs $0xaaaaaaaaaaaaaaab,%rdx
  400c66:
                 aa aa aa
  400c69:
                 48 89 c8
                                           mov
                                                  %rcx,%rax
  400c6c:
                 48 f7 e2
                                           mul
                                                  %rdx
                 48 d1 ea
                                                  %rdx
  400c6f:
                                           shr
  400c72:
                 48 89 d0
                                                  %rdx,%rax
                                           mov
  400c75:
                 48 01 c0
                                                  %rax,%rax
                                           add
  400c78:
                 48 01 d0
                                           add
                                                  %rdx,%rax
                 48 29 c1
  400c7b:
                                           sub
                                                  %rax,%rcx
  400c7e:
                 48 89 ca
                                                  %rcx,%rdx
                                           mov
  400c81:
                 8b 04 95 00 21 60 00
                                           mov
                                                  0x602100(,%rdx,4),%eax
                 3b 45 e0
  400c88:
                                           cmp
                                                  -0x20(%rbp),%eax
  400c8b:
                 7f aa
                                                  400c37 <getlogin_r@plt+0x467>
                                           jg
  400c8d:
                 48 8b 45 f8
                                           mov
                                                  -0x8(%rbp),%rax
  400c91:
                 с9
                                           leaveg
  400c92:
                 с3
                                           retq
                 66 2e 0f 1f 84 00 00
  400c93:
                                           nopw
                                                  %cs:0x0(%rax,%rax,1)
  400c9a:
                 00 00 00
                 0f 1f 00
                                                  (%rax)
  400c9d:
                                           nopl
  400ca0:
                 41 57
                                           push
                                                  %r15
                                                  %edi,%r15d
  400ca2:
                 41 89 ff
                                           mov
  400ca5:
                 41 56
                                           push
                                                  %r14
  400ca7:
                 49 89 f6
                                           mov
                                                  %rsi,%r14
  400caa:
                 41 55
                                           push
                                                  %r13
                 49 89 d5
  400cac:
                                           mov
                                                  %rdx,%r13
  400caf:
                 41 54
                                           push
                                                  %r12
                 4c 8d 25 48 11 20 00
  400cb1:
                                           lea
                                                  0x201148(%rip),%r12
                                                                               # 601e0
0 <_fini+0x2010ec>
  400cb8:
                                           push
                 48 8d 2d 48 11 20 00
  400cb9:
                                           lea
                                                  0x201148(%rip),%rbp
                                                                               # 601e0
8 <_fini+0x2010f4>
  400cc0:
                 53
                                           push
                                                  %rbx
```

```
400cc1:
                4c 29 e5
                                                 %r12,%rbp
                                         sub
                31 db
                                                 %ebx,%ebx
  400cc4:
                                         xor
                48 c1 fd 03
                                                 $0x3,%rbp
  400cc6:
                                         sar
                48 83 ec 08
                                                 $0x8,%rsp
  400cca:
                                         sub
                e8 35 fa ff ff
                                                400708 <_init>
  400cce:
                                         callq
                48 85 ed
                                         test
                                                 %rbp,%rbp
  400cd3:
  400cd6:
                74 1e
                                                 400cf6 <getlogin_r@plt+0x526>
                                         ie
                0f 1f 84 00 00 00 00
                                                 0x0(%rax,%rax,1)
  400cd8:
                                         nopl
  400cdf:
                00
                4c 89 ea
                                                 %r13,%rdx
  400ce0:
                                         mov
  400ce3:
                4c 89 f6
                                         mov
                                                 %r14,%rsi
  400ce6:
                44 89 ff
                                                 %r15d,%edi
                                         mov
  400ce9:
                41 ff 14 dc
                                         callq
                                                *(%r12,%rbx,8)
  400ced:
                48 83 c3 01
                                         add
                                                 $0x1,%rbx
  400cf1:
                48 39 eb
                                         cmp
                                                 %rbp,%rbx
                                                 400ce0 <getlogin_r@plt+0x510>
  400cf4:
                75 ea
                                         jne
  400cf6:
                48 83 c4 08
                                         add
                                                 $0x8,%rsp
                5b
  400cfa:
                                         pop
                                                 %rbx
  400cfb:
                5d
                                         pop
                                                 %rbp
                41 5c
                                                %r12
  400cfc:
                                         qoq
                41 5d
                                                 %r13
  400cfe:
                                         pop
                41 5e
                                                %r14
  400d00:
                                         pop
  400d02:
                41 5f
                                                 %r15
                                         pop
  400d04:
                с3
                                         retq
                66 66 2e 0f 1f 84 00
  400d05:
                                         data32 nopw %cs:0x0(%rax,%rax,1)
                00 00 00 00
  400d0c:
  400d10:
                f3 c3
                                         repz retq
Disassembly of section .fini:
0000000000400d14 <_fini>:
  400d14:
                48 83 ec 08
                                         sub
                                                 $0x8,%rsp
                48 83 c4 08
  400d18:
                                         add
                                                 $0x8,%rsp
                с3
  400d1c:
                                         reta
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ldd 4
        linux-vdso.so.1 => (0x00007fff137cd000)
        lib361.so => /lib/x86_64-linux-gnu/lib361.so (0x00007f353cbc1000)
        libc.so.6 => /lib/x86 64-linux-qnu/libc.so.6 (0x00007f353c7fc000)
        /lib64/ld-linux-x86-64.so.2 (0x000055eda9ef7000)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cd
Dpate85@Dhrumil:~$ cd ..
Dpate85@Dhrumil:/home$ cd ...
Dpate85@Dhrumil:/$ cd usr
Dpate85@Dhrumil:/usr$ cd local
Dpate85@Dhrumil:/usr/local$ cd lib
Dpate85@Dhrumil:/usr/local/lib$ ls
lib361.c lib361.so python2.7 python3.4
Dpate85@Dhrumil:/usr/local/lib$ sudo rm lib361.c lib361.so
Dpate85@Dhrumil:/usr/local/lib$ ls
python2.7 python3.4
Dpate85@Dhrumil:/usr/local/lib$ cd ...
Dpate85@Dhrumil:/usr/local$ cd ...
Dpate85@Dhrumil:/usr$ cd ...
```