```
Last login: Fri Jan 22 22:36:57 on console
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 Fri Jan 22 19:03:26 UTC 2016

  System load:  0.08              Processes:           115
  Usage of /:   5.6% of 28.80GB   Users logged in:     0
  Memory usage: 6%                IP address for eth0: 10.2.0.4
  Swap usage:   0%

  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

22 packages can be updated.
21 updates are security updates.


Last login: Fri Jan 22 19:03:28 2016 from 131-193-219-142.east.wireless.uic.edu
Dpate85@Dhrumil:~$ ls
dpate85  public
Dpate85@Dhrumil:~$ cd public
Dpate85@Dhrumil:~/public$ git pull
remote: Counting objects: 11, done.
remote: Compressing objects: 100% (8/8), done.
Unpacking objects: 100% (9/9), done.
remote: Total 9 (delta 4), reused 0 (delta 0)
From git.uicbits.net:cs361-s16/public
   9d1ae15..91e0ae2  master     -> origin/master
Updating 9d1ae15..91e0ae2
Fast-forward
 hw2/puzzles/0 | Bin 0 -> 6456 bytes
 hw2/puzzles/1 | Bin 0 -> 14994 bytes
 hw2/puzzles/2 | Bin 0 -> 10392 bytes
 hw2/puzzles/3 | Bin 0 -> 10584 bytes
 hw2/puzzles/4 | Bin 0 -> 10584 bytes
 5 files changed, 0 insertions(+), 0 deletions(-)
 create mode 100755 hw2/puzzles/0
 create mode 100755 hw2/puzzles/1
 create mode 100755 hw2/puzzles/2
 create mode 100755 hw2/puzzles/3
 create mode 100755 hw2/puzzles/4
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$ cat 0
ELF>?@@8@8      @@@@@?88@8@@@?
                                 ?
                                   ``?? ((`(`?TT@T@DDP?tdD
                                                          D
                                                           @D
                                                             @DDQ?tdR?td``??/lib64/ld-linux-x86-64.so.2GNUGNU2_???}@q?aaS¿}ɔ??
                                        /!A(S 6libc.so.6puts__stack_chk_failpbuitfcall?`` `(`0`8`@`H`PH?H??ibc_start_main__gmon_start__GLIBC_2.4GLIBC_2.2.5ii
 H??t?H???5?
 ?%?
 @?%?
 h??????%?
 h???????%?
 h??????%?
 h?????%?
 h?????%?
 h?????%?
 h?????%z
 h?p???1?I??^H??H???PTI???
@H??0
@H???@?????fD??`UH-?`H??H??w]øH??t?]??`?????`UH-?`H??H??H???H?H??u]úH??t?]H?p?`????=e
 uUH???~???]?R
???@H?=x H?s??tU H?U?H??H?Ñ?w??????UH??SH??8H??????dH?%(H?E?1?H???????H???z???ü?????>??????H?????????????Hc?H??????H??1????H?????????????????????Hc?H??????H??????H9?r???????Hc?H??????H??????H??H???H?u?dH3
4%(t????H??8[]?UH??H??@H?}?H?u?H?U?H7E?H??H?????????H??H??H??H?E?H?H?E?H??H???a???H?E?H?}?u
????E??E??;?E?H?H;E?sE??P?U?Hc?H?E?H??????7E?E?H?H;E?sE??P?U?Hc?H?E?H???????E?E?H?H;E?sE??P?U?Hc?H?E?H???????E??E????E??E?Æ?E?P?U?Hc?H?E?HE???????????`??E?P?U?Hc?H?E?HE???
                ?????????`??E?P?U?Hc?H?E?HE???????????`??E?H?H;E???????E??$H?E?H??E?H?H)?H??H??H??H??H??H?H)?H?u??`;E??H?E???f.?AWA??AVI??AUI??ATL
?%? UH?-? SL)?1?H??H??????H??t?L??D??A??H??H9?u?H?[]A\A]A^A_??f.???H?H??0123456789012345678 9%s%s
%dthis one is a gimme! You don't have to do anything!
you lose :(
you win! the secret is:
bananacake@
           ????????\?????????????????\???dzRx
                                        8???*zRx
                                               $x????FJ
N                                                     ??;*3$"D????SA?C
H?????A?C
$ ?????)A?C
D?????eB?E?E ?E(?H0?H8?M@l8A0A(B BB??????@?@
?                                        (@
???o?@?@?@
x
 `?h@P@ ???o @???o???@(`f@v@?@?@?@?@?@?
@?
@?
@?
@
@
  @ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/GCC: (Ubuntu 4.8.4-2ubuntu1~14.04) 4.8.4GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2.shstrtab.interp.note.ABI-tag.note.gnu.build-id.gnu.hash.dynsy
m.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
                                        8@8T@T !t@t$4???o?@>
                                                             ?@?F?@?xN???[???o @ jP@th@h?
          ~(@(yP@P???@????
@?
        ??
@?
?D
  @D
    D??
       @?
         ? ?(`(???```? ?`??0?M9?Dpate85@Dhrumil:~/public/hw2/puzzles$ clear

Dpate85@Dhrumil:~/public/hw2/puzzles$ ls
0  1  2  3  4
Dpate85@Dhrumil:~/public/hw2/puzzles$ cd ..
Dpate85@Dhrumil:~/public/hw2$ ls
puzzles
Dpate85@Dhrumil:~/public/hw2$ cp puzzles ./dpate85
cp: omitting directory ‘puzzles’
Dpate85@Dhrumil:~/public/hw2$ ls
puzzles
Dpate85@Dhrumil:~/public/hw2$ cd ..
Dpate85@Dhrumil:~/public$ ls
hw1  hw2
Dpate85@Dhrumil:~/public$ cd
Dpate85@Dhrumil:~$ cp ./public/hw2 ./dpate85/
cp: omitting directory ‘./public/hw2’
Dpate85@Dhrumil:~$ cp ./public/hw2. ./dpate85/
cp: cannot stat ‘./public/hw2.’: No such file or directory
Dpate85@Dhrumil:~$ cp -r ./public/hw2 ./dpate85/
```

```
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
0  1  2  3  4
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./0
this one is a gimme! You don't have to do anything!

you win! the secret is:
dEFTR1ENAw==
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi howto.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./1
behold! I will only tell you the secret password if you enter the random number I just generated!
^C
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./0
this one is a gimme! You don't have to do anything!

you win! the secret is:
dEFTR1ENAw==
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s 0

Symbol table '.dynsym' contains 9 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@GLIBC_2.2.5 (2)
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strlen@GLIBC_2.2.5 (2)
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __stack_chk_fail@GLIBC_2.4 (3)
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND printf@GLIBC_2.2.5 (2)
     5: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIBC_2.2.5 (2)
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND calloc@GLIBC_2.2.5 (2)
     7: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     8: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getlogin_r@GLIBC_2.2.5 (2)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf  0
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
     --segments          An alias for --program-headers
  -S --section-headers   Display the sections' header
     --sections          An alias for --section-headers
  -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
     --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)
  -u --unwind            Display the unwind info (if present)
  -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,=frames,
               =frames-interp,=str,=loc,=Ranges,=pubtypes,
               =gdb_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
  -v --version           Display the version number of readelf
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -a 0
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:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Advanced Micro Devices X86-64
  Version:                           0x1
  Entry point address:               0x4005e0
  Start of program headers:          64 (bytes into file)
  Start of section headers:          4664 (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:
  [Nr] Name              Type             Address           Offset
       Size              EntSize          Flags  Link  Info  Align
  [ 0]                   NULL             0000000000000000  00000000
       0000000000000000  0000000000000000           0     0     0
  [ 1] .interp           PROGBITS         0000000000400238  00000238
       000000000000001c  0000000000000000   A       0     0     1
  [ 2] .note.ABI-tag     NOTE             0000000000400254  00000254
       0000000000000020  0000000000000000   A       0     0     4
  [ 3] .note.gnu.build-i NOTE             0000000000400274  00000274
       0000000000000024  0000000000000000   A       0     0     4
  [ 4] .gnu.hash         GNU_HASH         0000000000400298  00000298
       000000000000001c  0000000000000000   A       5     0     8
  [ 5] .dynsym           DYNSYM           00000000004002b8  000002b8
       00000000000000d8  0000000000000018   A       6     1     8
  [ 6] .dynstr           STRTAB           0000000000400390  00000390
       0000000000000078  0000000000000000   A       0     0     1
  [ 7] .gnu.version      VERSYM           0000000000400408  00000408
       0000000000000012  0000000000000002   A       5     0     2
  [ 8] .gnu.version_r    VERNEED          0000000000400420  00000420
       0000000000000030  0000000000000000   A       6     1     8
  [ 9] .rela.dyn         RELA             0000000000400450  00000450
       0000000000000018  0000000000000018   A       5     0     8
  [10] .rela.plt         RELA             0000000000400468  00000468
       00000000000000c0  0000000000000018   A       5    12     8
  [11] .init             PROGBITS         0000000000400528  00000528
```

```
       000000000000001a  0000000000000000  AX       0     0     4
  [12] .plt              PROGBITS         0000000000400550  00000550
       0000000000000090  0000000000000010  AX       0     0     16
  [13] .text             PROGBITS         00000000004005e0  000005e0
       00000000000004c2  0000000000000000  AX       0     0     16
  [14] .fini             PROGBITS         0000000000400aa4  00000aa4
       0000000000000009  0000000000000000  AX       0     0     4
  [15] .rodata           PROGBITS         0000000000400ab0  00000ab0
       0000000000000094  0000000000000000   A       0     0     8
  [16] .eh_frame_hdr     PROGBITS         0000000000400b44  00000b44
       0000000000000044  0000000000000000   A       0     0     4
  [17] .eh_frame         PROGBITS         0000000000400b88  00000b88
       000000000000013c  0000000000000000   A       0     0     8
  [18] .init_array       INIT_ARRAY       0000000000600e10  00000e10
       0000000000000008  0000000000000000  WA       0     0     8
  [19] .fini_array       FINI_ARRAY       0000000000600e18  00000e18
       0000000000000008  0000000000000000  WA       0     0     8
  [20] .jcr              PROGBITS         0000000000600e20  00000e20
       0000000000000008  0000000000000000  WA       0     0     8
  [21] .dynamic          DYNAMIC          0000000000600e28  00000e28
       00000000000001d0  0000000000000010  WA       6     0     8
  [22] .got              PROGBITS         0000000000600ff8  00000ff8
       0000000000000008  0000000000000008  WA       0     0     8
  [23] .got.plt          PROGBITS         0000000000601000  00001000
       0000000000000058  0000000000000008  WA       0     0     8
  [24] .data             PROGBITS         0000000000601060  00001060
       000000000000008c  0000000000000000  WA       0     0     32
  [25] .bss              NOBITS           00000000006010ec  000010ec
       0000000000000004  0000000000000000  WA       0     0     1
  [26] .comment          PROGBITS         0000000000000000  000010ec
       000000000000004d  0000000000000001  MS       0     0     1
  [27] .shstrtab         STRTAB           0000000000000000  00001139
       00000000000000f8  0000000000000000           0     0     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:
  Type           Offset             VirtAddr           PhysAddr
                 FileSiz            MemSiz              Flags  Align
  PHDR           0x0000000000000040 0x0000000000400040 0x0000000000400040
                 0x00000000000001f8 0x00000000000001f8  R E    8
  INTERP         0x0000000000000238 0x0000000000400238 0x0000000000400238
                 0x000000000000001c 0x000000000000001c  R      1
      [Requesting program interpreter: /lib64/ld-linux-x86-64.so.2]
  LOAD           0x0000000000000000 0x0000000000400000 0x0000000000400000
                 0x00000000000006cc4 0x00000000000006cc4  R E    200000
  LOAD           0x0000000000000e10 0x0000000000600e10 0x0000000000600e10
                 0x00000000000002dc 0x00000000000002e0  RW     200000
  DYNAMIC        0x0000000000000e28 0x0000000000600e28 0x0000000000600e28
                 0x00000000000001d0 0x00000000000001d0  RW     8
  NOTE           0x0000000000000254 0x0000000000400254 0x0000000000400254
                 0x0000000000000044 0x0000000000000044  R      4
  GNU_EH_FRAME   0x0000000000000b44 0x0000000000400b44 0x0000000000400b44
                 0x0000000000000044 0x0000000000000044  R      4
  GNU_STACK      0x0000000000000000 0x0000000000000000 0x0000000000000000
                 0x0000000000000000 0x0000000000000000  RW     10
  GNU_RELRO      0x0000000000000e10 0x0000000000600e10 0x0000000000600e10
                 0x00000000000001f0 0x00000000000001f0  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_frame_hdr .eh_frame
   03     .init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
   04     .dynamic
   05     .note.ABI-tag .note.gnu.build-id
   06     .eh_frame_hdr
   07
   08     .init_array .fini_array .jcr .dynamic .got

Dynamic section at offset 0xe28 contains 24 entries:
  Tag        Type                         Name/Value
 0x0000000000000001 (NEEDED)             Shared library: [libc.so.6]
 0x000000000000000c (INIT)               0x400528
 0x000000000000000d (FINI)               0x400aa4
 0x0000000000000019 (INIT_ARRAY)         0x600e10
 0x000000000000001b (INIT_ARRAYSZ)       8 (bytes)
 0x000000000000001a (FINI_ARRAY)         0x600e18
 0x000000000000001c (FINI_ARRAYSZ)       8 (bytes)
 0x000000006ffffef5 (GNU_HASH)           0x400298
 0x0000000000000005 (STRTAB)             0x400390
 0x0000000000000006 (SYMTAB)             0x4002b8
 0x000000000000000a (STRSZ)              120 (bytes)
 0x000000000000000b (SYMENT)             24 (bytes)
 0x0000000000000015 (DEBUG)              0x0
 0x0000000000000003 (PLTGOT)             0x601000
 0x0000000000000002 (PLTRELSZ)           192 (bytes)
 0x0000000000000014 (PLTREL)             RELA
 0x0000000000000017 (JMPREL)             0x400468
 0x0000000000000007 (RELA)               0x400450
 0x0000000000000008 (RELASZ)             24 (bytes)
 0x0000000000000009 (RELAENT)            24 (bytes)
 0x000000006ffffffe (VERNEED)            0x400420
 0x000000006fffffff (VERNEEDNUM)         1
 0x000000006ffffff0 (VERSYM)             0x400408
 0x0000000000000000 (NULL)               0x0

Relocation section '.rela.dyn' at offset 0x450 contains 1 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000600ff8  000700000006 R_X86_64_GLOB_DAT 0000000000000000 __gmon_start__ + 0

Relocation section '.rela.plt' at offset 0x468 contains 8 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000601018  000100000007 R_X86_64_JUMP_SLO 0000000000000000 puts + 0
000000601020  000200000007 R_X86_64_JUMP_SLO 0000000000000000 strlen + 0
000000601028  000300000007 R_X86_64_JUMP_SLO 0000000000000000 __stack_chk_fail + 0
000000601030  000400000007 R_X86_64_JUMP_SLO 0000000000000000 printf + 0
000000601038  000500000007 R_X86_64_JUMP_SLO 0000000000000000 __libc_start_main + 0
000000601040  000600000007 R_X86_64_JUMP_SLO 0000000000000000 calloc + 0
000000601048  000700000007 R_X86_64_JUMP_SLO 0000000000000000 __gmon_start__ + 0
000000601050  000800000007 R_X86_64_JUMP_SLO 0000000000000000 getlogin_r + 0

The decoding of unwind sections for machine type Advanced Micro Devices X86-64 is not currently supported.

Symbol table '.dynsym' contains 9 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@GLIBC_2.2.5 (2)
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strlen@GLIBC_2.2.5 (2)
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __stack_chk_fail@GLIBC_2.4 (3)
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND printf@GLIBC_2.2.5 (2)
     5: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIBC_2.2.5 (2)
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND calloc@GLIBC_2.2.5 (2)
     7: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     8: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getlogin_r@GLIBC_2.2.5 (2)

Version symbols section '.gnu.version' contains 9 entries:
 Addr: 0000000000400408  Offset: 0x000408  Link: 5 (.dynsym)
  000:   0 (*local*)       2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)   3 (GLIBC_2.4)
  004:   2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)   0 (*local*)
```

```
  008:   2 (GLIBC_2.2.5)

Version needs section '.gnu.version_r' contains 1 entries:
 Addr: 0x0000000000400420  Offset: 0x000420  Link: 6 (.dynstr)
  000000: Version: 1  File: libc.so.6  Cnt: 2
  0x0010:   Name: GLIBC_2.4  Flags: none  Version: 3
  0x0020:   Name: GLIBC_2.2.5  Flags: none  Version: 2

Displaying notes found at file offset 0x00000254 with length 0x00000020:
  Owner                 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:
  Owner                 Data size       Description
  GNU                  0x00000014       NT_GNU_BUILD_ID (unique build ID bitstring)
    Build ID: 325f0485a7b47d4071ff616153d7a07bdd9f94de
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ clear

Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./1
behold! I will only tell you the secret password if you enter the random number I just generated!
^C
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s 1

Symbol table '.dynsym' contains 13 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@GLIBC_2.2.5 (2)
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strlen@GLIBC_2.2.5 (2)
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __stack_chk_fail@GLIBC_2.4 (3)
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND printf@GLIBC_2.2.5 (2)
     5: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIBC_2.2.5 (2)
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND srand@GLIBC_2.2.5 (2)
     7: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND calloc@GLIBC_2.2.5 (2)
     8: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     9: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND time@GLIBC_2.2.5 (2)
    10: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getlogin_r@GLIBC_2.2.5 (2)
    11: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __isoc99_scanf@GLIBC_2.7 (4)
    12: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND rand@GLIBC_2.2.5 (2)

Symbol table '.symtab' contains 91 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000400238     0 SECTION LOCAL  DEFAULT    1
     2: 0000000000400254     0 SECTION LOCAL  DEFAULT    2
     3: 0000000000400274     0 SECTION LOCAL  DEFAULT    3
     4: 0000000000400298     0 SECTION LOCAL  DEFAULT    4
     5: 00000000004002b8     0 SECTION LOCAL  DEFAULT    5
     6: 00000000004003f0     0 SECTION LOCAL  DEFAULT    6
     7: 000000000040048c     0 SECTION LOCAL  DEFAULT    7
     8: 00000000004004a8     0 SECTION LOCAL  DEFAULT    8
     9: 00000000004004e8     0 SECTION LOCAL  DEFAULT    9
    10: 0000000000400500     0 SECTION LOCAL  DEFAULT   10
    11: 0000000000400620     0 SECTION LOCAL  DEFAULT   11
    12: 0000000000400640     0 SECTION LOCAL  DEFAULT   12
    13: 0000000000400710     0 SECTION LOCAL  DEFAULT   13
    14: 0000000000400c44     0 SECTION LOCAL  DEFAULT   14
    15: 0000000000400c50     0 SECTION LOCAL  DEFAULT   15
    16: 0000000000400d0c     0 SECTION LOCAL  DEFAULT   16
    17: 0000000000400d58     0 SECTION LOCAL  DEFAULT   17
    18: 0000000000601e10     0 SECTION LOCAL  DEFAULT   18
    19: 0000000000601e18     0 SECTION LOCAL  DEFAULT   19
    20: 0000000000601e20     0 SECTION LOCAL  DEFAULT   20
    21: 0000000000601e28     0 SECTION LOCAL  DEFAULT   21
    22: 0000000000601ff8     0 SECTION LOCAL  DEFAULT   22
    23: 0000000000602000     0 SECTION LOCAL  DEFAULT   23
    24: 0000000000602080     0 SECTION LOCAL  DEFAULT   24
    25: 000000000060210c     0 SECTION LOCAL  DEFAULT   25
    26: 0000000000000000     0 SECTION LOCAL  DEFAULT   26
    27: 0000000000000000     0 SECTION LOCAL  DEFAULT   27
    28: 0000000000000000     0 SECTION LOCAL  DEFAULT   28
    29: 0000000000000000     0 SECTION LOCAL  DEFAULT   29
    30: 0000000000000000     0 SECTION LOCAL  DEFAULT   30
    31: 0000000000000000     0 SECTION LOCAL  DEFAULT   31
    32: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    33: 0000000000601e20     0 OBJECT  LOCAL  DEFAULT   20 __JCR_LIST__
    34: 0000000000400740     0 FUNC    LOCAL  DEFAULT   13 deregister_tm_clones
    35: 0000000000400770     0 FUNC    LOCAL  DEFAULT   13 register_tm_clones
    36: 00000000004007b0     0 FUNC    LOCAL  DEFAULT   13 __do_global_dtors_aux
    37: 000000000060210c     1 OBJECT  LOCAL  DEFAULT   25 completed.6973
    38: 0000000000601e18     0 OBJECT  LOCAL  DEFAULT   19 __do_global_dtors_aux_fin
    39: 00000000004007d0     0 FUNC    LOCAL  DEFAULT   13 frame_dummy
    40: 0000000000601e10     0 OBJECT  LOCAL  DEFAULT   18 __frame_dummy_init_array_
    41: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS gdb.c
    42: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS b64.c
    43: 00000000006020c0    64 OBJECT  LOCAL  DEFAULT   24 encoding_table
    44: 0000000000602100    12 OBJECT  LOCAL  DEFAULT   24 mod_table
    45: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    46: 0000000000400eb0     0 OBJECT  LOCAL  DEFAULT   17 __FRAME_END__
    47: 0000000000601e20     0 OBJECT  LOCAL  DEFAULT   20 __JCR_END__
    48: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS
    49: 0000000000601e18     0 NOTYPE  LOCAL  DEFAULT   18 __init_array_end
    50: 0000000000601e28     0 OBJECT  LOCAL  DEFAULT   21 _DYNAMIC
    51: 0000000000601e10     0 NOTYPE  LOCAL  DEFAULT   18 __init_array_start
    52: 0000000000602000     0 OBJECT  LOCAL  DEFAULT   23 _GLOBAL_OFFSET_TABLE_
    53: 0000000000400c40     2 FUNC    GLOBAL DEFAULT   13 __libc_csu_fini
    54: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
    55: 0000000000602080     0 NOTYPE  WEAK   DEFAULT   24 data_start
    56: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@@GLIBC_2.2.5
    57: 00000000006020a0     8 OBJECT  GLOBAL DEFAULT   24 d
    58: 00000000006020a8     8 OBJECT  GLOBAL DEFAULT   24 r
    59: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   24 _edata
    60: 00000000006020b8     8 OBJECT  GLOBAL DEFAULT   24 p
    61: 0000000000400c44     0 FUNC    GLOBAL DEFAULT   14 _fini
    62: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strlen@@GLIBC_2.2.5
    63: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __stack_chk_fail@@GLIBC_2
    64: 00000000006020b0     8 OBJECT  GLOBAL DEFAULT   24 f
    65: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND printf@@GLIBC_2.2.5
    66: 00000000004007fd   167 FUNC    GLOBAL DEFAULT   13 password
    67: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@@GLIBC_
    68: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND srand@@GLIBC_2.2.5
    69: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND calloc@@GLIBC_2.2.5
    70: 0000000000602080     0 NOTYPE  GLOBAL DEFAULT   24 __data_start
    71: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
    72: 0000000000602088     0 OBJECT  GLOBAL HIDDEN    24 __dso_handle
    73: 0000000000400c50     4 OBJECT  GLOBAL DEFAULT   15 _IO_stdin_used
    74: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND time@@GLIBC_2.2.5
    75: 0000000000400bd0   101 FUNC    GLOBAL DEFAULT   13 __libc_csu_init
    76: 0000000000602110     0 NOTYPE  GLOBAL DEFAULT   25 _end
    77: 0000000000400710     0 FUNC    GLOBAL DEFAULT   13 _start
    78: 00000000004009a1   553 FUNC    GLOBAL DEFAULT   13 base64_encode
    79: 0000000000602090     8 OBJECT  GLOBAL DEFAULT   24 o
    80: 0000000000602098     8 OBJECT  GLOBAL DEFAULT   24 s
    81: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   25 __bss_start
    82: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getlogin_r@@GLIBC_2.2.5
    83: 00000000004008a4    32 FUNC    GLOBAL DEFAULT   13 main
    84: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
    85: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __isoc99_scanf@@GLIBC_2.7
    86: 0000000000602110     0 OBJECT  GLOBAL HIDDEN    24 __TMC_END__
    87: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
    88: 0000000000400620     0 FUNC    GLOBAL DEFAULT   11 _init
```

```
    89: 00000000004008c4   221 FUNC    GLOBAL DEFAULT   13 generate_password
    90: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND rand@@GLIBC_2.2.5
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./1
behold! I will only tell you the secret password if you enter the random number I just generated!
64
you lose :(
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./1
behold! I will only tell you the secret password if you enter the random number I just generated!
1
you lose :(
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
The program 'gdb' can be found in the following packages:
 * gdb
 * gdb-minimal
Try: sudo apt-get install <selected package>
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo apt-get install gdb
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libc6-dbg libpython3.4
Suggested packages:
  gdb-doc gdbserver
Recommended packages:
  libc-dbg
The following NEW packages will be installed:
  gdb libc6-dbg libpython3.4
0 upgraded, 3 newly installed, 0 to remove and 19 not upgraded.
Need to get 6,958 kB of archives.
After this operation, 33.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://azure.archive.ubuntu.com/ubuntu/ trusty-updates/main libpython3.4 amd64 3.4.3-1ubuntu1~14.04.3 [1,308 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu/ trusty-updates/main gdb amd64 7.7.1-0ubuntu5~14.04.2 [2,198 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu/ trusty-updates/main libc6-dbg amd64 2.19-0ubuntu6.6 [3,452 kB]
Fetched 6,958 kB in 3s (2,198 kB/s)
Selecting previously unselected package libpython3.4:amd64.
(Reading database ... 57890 files and directories currently installed.)
Preparing to unpack .../libpython3.4_3.4.3-1ubuntu1~14.04.3_amd64.deb ...
Unpacking libpython3.4:amd64 (3.4.3-1ubuntu1~14.04.3) ...
Selecting previously unselected package gdb.
Preparing to unpack .../gdb_7.7.1-0ubuntu5~14.04.2_amd64.deb ...
Unpacking gdb (7.7.1-0ubuntu5~14.04.2) ...
Selecting previously unselected package libc6-dbg:amd64.
Preparing to unpack .../libc6-dbg_2.19-0ubuntu6.6_amd64.deb ...
Unpacking libc6-dbg:amd64 (2.19-0ubuntu6.6) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up libpython3.4:amd64 (3.4.3-1ubuntu1~14.04.3) ...
Setting up gdb (7.7.1-0ubuntu5~14.04.2) ...
Setting up libc6-dbg:amd64 (2.19-0ubuntu6.6) ...
Processing triggers for libc-bin (2.19-0ubuntu6.6) ...
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (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 <http://gnu.org/licenses/gpl.html>
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 1...done.
(gdb) b main
Breakpoint 1 at 0x4008a8: file gdb.c, line 33.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 1, main () at gdb.c:33
33      gdb.c: No such file or directory.
(gdb) c
Continuing.
behold! I will only tell you the secret password if you enter the random number I just generated!
^C
Program received signal SIGINT, Interrupt.
0x00007ffff7b00810 in __read_nocancel () at ../sysdeps/unix/syscall-template.S:81
81      ../sysdeps/unix/syscall-template.S: No such file or directory.
(gdb) b 1
Breakpoint 2 at 0x7ffff7b004d0: file ../sysdeps/unix/syscall-template.S, line 1.
(gdb) r
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 2, access () at ../sysdeps/unix/syscall-template.S:81
81      ../sysdeps/unix/syscall-template.S: No such file or directory.
(gdb) s

Breakpoint 2, access () at ../sysdeps/unix/syscall-template.S:81
81      in ../sysdeps/unix/syscall-template.S
(gdb) s

Breakpoint 2, open64 () at ../sysdeps/unix/syscall-template.S:81
81      ../sysdeps/unix/syscall-template.S: No such file or directory.
(gdb) s

Breakpoint 2, close () at ../sysdeps/unix/syscall-template.S:81
81      ../sysdeps/unix/syscall-template.S: No such file or directory.
(gdb) s

Breakpoint 2, access () at ../sysdeps/unix/syscall-template.S:81
81      ../sysdeps/unix/syscall-template.S: No such file or directory.
(gdb) s

Breakpoint 2, open64 () at ../sysdeps/unix/syscall-template.S:81
81      ../sysdeps/unix/syscall-template.S: No such file or directory.
(gdb) s

Breakpoint 2, read () at ../sysdeps/unix/syscall-template.S:81
81      ../sysdeps/unix/syscall-template.S: No such file or directory.
(gdb) s

Breakpoint 2, close () at ../sysdeps/unix/syscall-template.S:81
81      ../sysdeps/unix/syscall-template.S: No such file or directory.
(gdb) s

s
s
s
s
s
s
^C
Program received signal SIGINT, Interrupt.
0x00007ffff7de401e in do_lookup_x (new_hash=new_hash@entry=318234123, old_hash=old_hash@entry=0x7fffffffe270, result=result@entry=0x7fffffffe280, scope=<optimized out>, i=1, i@entry=0,
    flags=flags@entry=1, skip=skip@entry=0x0, undef_map=undef_map@entry=0x7ffff7ff74c0) at dl-lookup.c:236
236     dl-lookup.c: No such file or directory.
(gdb) clear
No breakpoint at this line.
(gdb) ls
Undefined command: "ls".  Try "help".
(gdb) exit
```

```
Undefined command: "exit".  Try "help".
(gdb) quit
A debugging session is active.

        Inferior 1 [process 61841] will be killed.

Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ clear

Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./1
behold! I will only tell you the secret password if you enter the random number I just generated!
^C
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -a 1
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:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Advanced Micro Devices X86-64
  Version:                           0x1
  Entry point address:               0x400710
  Start of program headers:          64 (bytes into file)
  Start of section headers:          9728 (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:         35
  Section header string table index: 32

Section Headers:
  [Nr] Name              Type             Address           Offset
       Size              EntSize          Flags  Link  Info  Align
  [ 0]                   NULL             0000000000000000  00000000
       0000000000000000  0000000000000000           0     0     0
  [ 1] .interp           PROGBITS         0000000000400238  00000238
       000000000000001c  0000000000000000  A       0     0     1
  [ 2] .note.ABI-tag     NOTE             0000000000400254  00000254
       0000000000000020  0000000000000000  A       0     0     4
  [ 3] .note.gnu.build-i NOTE             0000000000400274  00000274
       0000000000000024  0000000000000000  A       0     0     4
  [ 4] .gnu.hash         GNU_HASH         0000000000400298  00000298
       000000000000001c  0000000000000000  A       5     0     8
  [ 5] .dynsym           DYNSYM           00000000004002b8  000002b8
       0000000000000138  0000000000000018  A       6     1     8
  [ 6] .dynstr           STRTAB           00000000004003f0  000003f0
       000000000000009c  0000000000000000  A       0     0     1
  [ 7] .gnu.version      VERSYM           000000000040048c  0000048c
       000000000000001a  0000000000000002  A       5     0     2
  [ 8] .gnu.version_r    VERNEED          00000000004004a8  000004a8
       0000000000000040  0000000000000000  A       6     1     8
  [ 9] .rela.dyn         RELA             00000000004004e8  000004e8
       0000000000000018  0000000000000018  A       5     0     8
  [10] .rela.plt         RELA             0000000000400500  00000500
       0000000000000120  0000000000000018  A       5    12     8
  [11] .init             PROGBITS         0000000000400620  00000620
       000000000000001a  0000000000000000  AX      0     0     4
  [12] .plt              PROGBITS         0000000000400640  00000640
       00000000000000d0  0000000000000010  AX      0     0     16
  [13] .text             PROGBITS         0000000000400710  00000710
       0000000000000532  0000000000000000  AX      0     0     16
  [14] .fini             PROGBITS         0000000000400c44  00000c44
       0000000000000009  0000000000000000  AX      0     0     4
  [15] .rodata           PROGBITS         0000000000400c50  00000c50
       00000000000000bc  0000000000000000  A       0     0     8
  [16] .eh_frame_hdr     PROGBITS         0000000000400d0c  00000d0c
       000000000000004c  0000000000000000  A       0     0     4
  [17] .eh_frame         PROGBITS         0000000000400d58  00000d58
       000000000000015c  0000000000000000  A       0     0     8
  [18] .init_array       INIT_ARRAY       0000000000601e10  00001e10
       0000000000000008  0000000000000000  WA      0     0     8
  [19] .fini_array       FINI_ARRAY       0000000000601e18  00001e18
       0000000000000008  0000000000000000  WA      0     0     8
  [20] .jcr              PROGBITS         0000000000601e20  00001e20
       0000000000000008  0000000000000000  WA      0     0     8
  [21] .dynamic          DYNAMIC          0000000000601e28  00001e28
       00000000000001d0  0000000000000010  WA      6     0     8
  [22] .got              PROGBITS         0000000000601ff8  00001ff8
       0000000000000008  0000000000000008  WA      0     0     8
  [23] .got.plt          PROGBITS         0000000000602000  00002000
       0000000000000078  0000000000000008  WA      0     0     8
  [24] .data             PROGBITS         0000000000602080  00002080
       000000000000008c  0000000000000000  WA      0     0     32
  [25] .bss              NOBITS           000000000060210c  0000210c
       0000000000000004  0000000000000000  WA      0     0     1
  [26] .comment          PROGBITS         0000000000000000  0000210c
       000000000000004d  0000000000000001  MS      0     0     1
  [27] .debug_aranges    PROGBITS         0000000000000000  00002159
       0000000000000030  0000000000000000           0     0     1
  [28] .debug_info       PROGBITS         0000000000000000  00002189
       0000000000000161  0000000000000000           0     0     1
  [29] .debug_abbrev     PROGBITS         0000000000000000  000022ea
       000000000000008c  0000000000000000           0     0     1
  [30] .debug_line       PROGBITS         0000000000000000  00002376
       000000000000004d  0000000000000000           0     0     1
  [31] .debug_str        PROGBITS         0000000000000000  000023c3
       00000000000000f0  0000000000000001  MS      0     0     1
  [32] .shstrtab         STRTAB           0000000000000000  000024b3
       0000000000000148  0000000000000000           0     0     1
  [33] .symtab           SYMTAB           0000000000000000  00002ec0
       0000000000000888  0000000000000018          34    53     8
  [34] .strtab           STRTAB           0000000000000000  00003748
       000000000000034a  0000000000000000           0     0     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:
  Type           Offset             VirtAddr           PhysAddr
                 FileSiz            MemSiz              Flags  Align
  PHDR           0x0000000000000040 0x0000000000400040 0x0000000000400040
                 0x00000000000001f8 0x00000000000001f8  R E    8
  INTERP         0x0000000000000238 0x0000000000400238 0x0000000000400238
                 0x000000000000001c 0x000000000000001c  R      1
      [Requesting program interpreter: /lib64/ld-linux-x86-64.so.2]
  LOAD           0x0000000000000000 0x0000000000400000 0x0000000000400000
                 0x00000000000000eb4 0x00000000000000eb4  R E    200000
  LOAD           0x0000000000001e10 0x0000000000601e10 0x0000000000601e10
                 0x00000000000002fc 0x0000000000000300  RW     200000
  DYNAMIC        0x0000000000001e28 0x0000000000601e28 0x0000000000601e28
                 0x00000000000001d0 0x00000000000001d0  RW     8
  NOTE           0x0000000000000254 0x0000000000400254 0x0000000000400254
                 0x0000000000000044 0x0000000000000044  R      4
  GNU_EH_FRAME   0x0000000000000d0c 0x0000000000400d0c 0x0000000000400d0c
                 0x000000000000004c 0x000000000000004c  R      4
  GNU_STACK      0x0000000000000000 0x0000000000000000 0x0000000000000000
```

```
               0x0000000000000000 0x0000000000000000  RW     10
  GNU_RELRO      0x0000000000001e10 0x0000000000601e10 0x0000000000601e10
                 0x00000000000001f0 0x00000000000001f0  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_frame_hdr .eh_frame
   03     .init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
   04     .dynamic
   05     .note.ABI-tag .note.gnu.build-id
   06     .eh_frame_hdr
   07
   08     .init_array .fini_array .jcr .dynamic .got

Dynamic section at offset 0x1e28 contains 24 entries:
  Tag        Type                         Name/Value
 0x0000000000000001 (NEEDED)             Shared library: [libc.so.6]
 0x000000000000000c (INIT)               0x400620
 0x000000000000000d (FINI)               0x400c44
 0x0000000000000019 (INIT_ARRAY)         0x601e10
 0x000000000000001b (INIT_ARRAYSZ)       8 (bytes)
 0x000000000000001a (FINI_ARRAY)         0x601e18
 0x000000000000001c (FINI_ARRAYSZ)       8 (bytes)
 0x000000006ffffef5 (GNU_HASH)           0x400298
 0x0000000000000005 (STRTAB)             0x4003f0
 0x0000000000000006 (SYMTAB)             0x4002b8
 0x000000000000000a (STRSZ)              156 (bytes)
 0x000000000000000b (SYMENT)             24 (bytes)
 0x0000000000000015 (DEBUG)              0x0
 0x0000000000000003 (PLTGOT)             0x602000
 0x0000000000000002 (PLTRELSZ)           288 (bytes)
 0x0000000000000014 (PLTREL)             RELA
 0x0000000000000017 (JMPREL)             0x400500
 0x0000000000000007 (RELA)               0x4004e8
 0x0000000000000008 (RELASZ)             24 (bytes)
 0x0000000000000009 (RELAENT)            24 (bytes)
 0x000000006ffffffe (VERNEED)            0x4004a8
 0x000000006fffffff (VERNEEDNUM)         1
 0x000000006ffffff0 (VERSYM)             0x40048c
 0x0000000000000000 (NULL)               0x0

Relocation section '.rela.dyn' at offset 0x4e8 contains 1 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000601ff8  000800000006 R_X86_64_GLOB_DAT 0000000000000000 __gmon_start__ + 0

Relocation section '.rela.plt' at offset 0x500 contains 12 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000602018  000100000007 R_X86_64_JUMP_SLO 0000000000000000 puts + 0
000000602020  000200000007 R_X86_64_JUMP_SLO 0000000000000000 strlen + 0
000000602028  000300000007 R_X86_64_JUMP_SLO 0000000000000000 __stack_chk_fail + 0
000000602030  000400000007 R_X86_64_JUMP_SLO 0000000000000000 printf + 0
000000602038  000500000007 R_X86_64_JUMP_SLO 0000000000000000 __libc_start_main + 0
000000602040  000600000007 R_X86_64_JUMP_SLO 0000000000000000 srand + 0
000000602048  000700000007 R_X86_64_JUMP_SLO 0000000000000000 calloc + 0
000000602050  000800000007 R_X86_64_JUMP_SLO 0000000000000000 __gmon_start__ + 0
000000602058  000900000007 R_X86_64_JUMP_SLO 0000000000000000 time + 0
000000602060  000a00000007 R_X86_64_JUMP_SLO 0000000000000000 getlogin_r + 0
000000602068  000b00000007 R_X86_64_JUMP_SLO 0000000000000000 __isoc99_scanf + 0
000000602070  000c00000007 R_X86_64_JUMP_SLO 0000000000000000 rand + 0

The decoding of unwind sections for machine type Advanced Micro Devices X86-64 is not currently supported.

Symbol table '.dynsym' contains 13 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@GLIBC_2.2.5 (2)
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strlen@GLIBC_2.2.5 (2)
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __stack_chk_fail@GLIBC_2.4 (3)
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND printf@GLIBC_2.2.5 (2)
     5: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIBC_2.2.5 (2)
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND srand@GLIBC_2.2.5 (2)
     7: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND calloc@GLIBC_2.2.5 (2)
     8: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     9: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND time@GLIBC_2.2.5 (2)
    10: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getlogin_r@GLIBC_2.2.5 (2)
    11: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __isoc99_scanf@GLIBC_2.7 (4)
    12: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND rand@GLIBC_2.2.5 (2)

Symbol table '.symtab' contains 91 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000400238     0 SECTION LOCAL  DEFAULT    1
     2: 0000000000400254     0 SECTION LOCAL  DEFAULT    2
     3: 0000000000400274     0 SECTION LOCAL  DEFAULT    3
     4: 0000000000400298     0 SECTION LOCAL  DEFAULT    4
     5: 00000000004002b8     0 SECTION LOCAL  DEFAULT    5
     6: 00000000004003f0     0 SECTION LOCAL  DEFAULT    6
     7: 000000000040048c     0 SECTION LOCAL  DEFAULT    7
     8: 00000000004004a8     0 SECTION LOCAL  DEFAULT    8
     9: 00000000004004e8     0 SECTION LOCAL  DEFAULT    9
    10: 0000000000400500     0 SECTION LOCAL  DEFAULT   10
    11: 0000000000400620     0 SECTION LOCAL  DEFAULT   11
    12: 0000000000400640     0 SECTION LOCAL  DEFAULT   12
    13: 0000000000400710     0 SECTION LOCAL  DEFAULT   13
    14: 0000000000400c44     0 SECTION LOCAL  DEFAULT   14
    15: 0000000000400c50     0 SECTION LOCAL  DEFAULT   15
    16: 0000000000400d0c     0 SECTION LOCAL  DEFAULT   16
    17: 0000000000400d58     0 SECTION LOCAL  DEFAULT   17
    18: 0000000000601e10     0 SECTION LOCAL  DEFAULT   18
    19: 0000000000601e18     0 SECTION LOCAL  DEFAULT   19
    20: 0000000000601e20     0 SECTION LOCAL  DEFAULT   20
    21: 0000000000601e28     0 SECTION LOCAL  DEFAULT   21
    22: 0000000000601ff8     0 SECTION LOCAL  DEFAULT   22
    23: 0000000000602000     0 SECTION LOCAL  DEFAULT   23
    24: 0000000000602080     0 SECTION LOCAL  DEFAULT   24
    25: 000000000060210c     0 SECTION LOCAL  DEFAULT   25
    26: 0000000000000000     0 SECTION LOCAL  DEFAULT   26
    27: 0000000000000000     0 SECTION LOCAL  DEFAULT   27
    28: 0000000000000000     0 SECTION LOCAL  DEFAULT   28
    29: 0000000000000000     0 SECTION LOCAL  DEFAULT   29
    30: 0000000000000000     0 SECTION LOCAL  DEFAULT   30
    31: 0000000000000000     0 SECTION LOCAL  DEFAULT   31
    32: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    33: 0000000000601e20     0 OBJECT  LOCAL  DEFAULT   20 __JCR_LIST__
    34: 0000000000400740     0 FUNC    LOCAL  DEFAULT   13 deregister_tm_clones
    35: 0000000000400770     0 FUNC    LOCAL  DEFAULT   13 register_tm_clones
    36: 00000000004007b0     0 FUNC    LOCAL  DEFAULT   13 __do_global_dtors_aux
    37: 000000000060210c     1 OBJECT  LOCAL  DEFAULT   25 completed.6973
    38: 0000000000601e18     0 OBJECT  LOCAL  DEFAULT   19 __do_global_dtors_aux_fin
    39: 00000000004007d0     0 FUNC    LOCAL  DEFAULT   13 frame_dummy
    40: 0000000000601e10     0 OBJECT  LOCAL  DEFAULT   18 __frame_dummy_init_array_
    41: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS gdb.c
    42: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS b64.c
    43: 00000000006020c0    64 OBJECT  LOCAL  DEFAULT   24 encoding_table
    44: 0000000000602100    12 OBJECT  LOCAL  DEFAULT   24 mod_table
    45: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    46: 0000000000400eb0     0 OBJECT  LOCAL  DEFAULT   17 __FRAME_END__
    47: 0000000000601e20     0 OBJECT  LOCAL  DEFAULT   20 __JCR_END__
    48: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS
    49: 0000000000601e18     0 NOTYPE  LOCAL  DEFAULT   18 __init_array_end
    50: 0000000000601e28     0 OBJECT  LOCAL  DEFAULT   21 _DYNAMIC
    51: 0000000000601e10     0 NOTYPE  LOCAL  DEFAULT   18 __init_array_start
    52: 0000000000602000     0 OBJECT  LOCAL  DEFAULT   23 _GLOBAL_OFFSET_TABLE_
```

```
    53: 0000000000400c40     2 FUNC    GLOBAL DEFAULT   13 __libc_csu_fini
    54: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
    55: 0000000000602080     0 NOTYPE  WEAK   DEFAULT   24 data_start
    56: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@@GLIBC_2.2.5
    57: 00000000006020a0     8 OBJECT  GLOBAL DEFAULT   24 d
    58: 00000000006020a8     8 OBJECT  GLOBAL DEFAULT   24 r
    59: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   24 _edata
    60: 00000000006020b8     8 OBJECT  GLOBAL DEFAULT   24 p
    61: 0000000000400c44     0 FUNC    GLOBAL DEFAULT   14 _fini
    62: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strlen@@GLIBC_2.2.5
    63: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __stack_chk_fail@@GLIBC_2
    64: 00000000006020b0     8 OBJECT  GLOBAL DEFAULT   24 f
    65: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND printf@@GLIBC_2.2.5
    66: 00000000004007fd   167 FUNC    GLOBAL DEFAULT   13 password
    67: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@@GLIBC_
    68: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND srand@@GLIBC_2.2.5
    69: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND calloc@@GLIBC_2.2.5
    70: 0000000000602080     0 NOTYPE  GLOBAL DEFAULT   24 __data_start
    71: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
    72: 0000000000602088     0 OBJECT  GLOBAL HIDDEN    24 __dso_handle
    73: 0000000000400c50     4 OBJECT  GLOBAL DEFAULT   15 _IO_stdin_used
    74: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND time@@GLIBC_2.2.5
    75: 0000000000400bd0   101 FUNC    GLOBAL DEFAULT   13 __libc_csu_init
    76: 0000000000602110     0 NOTYPE  GLOBAL DEFAULT   25 _end
    77: 0000000000400710     0 FUNC    GLOBAL DEFAULT   13 _start
    78: 00000000004009a1   553 FUNC    GLOBAL DEFAULT   13 base64_encode
    79: 0000000000602090     8 OBJECT  GLOBAL DEFAULT   24 o
    80: 0000000000602098     8 OBJECT  GLOBAL DEFAULT   24 s
    81: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   25 __bss_start
    82: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getlogin_r@@GLIBC_2.2.5
    83: 00000000004008a4    32 FUNC    GLOBAL DEFAULT   13 main
    84: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
    85: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __isoc99_scanf@@GLIBC_2.7
    86: 0000000000602110     0 OBJECT  GLOBAL HIDDEN    24 __TMC_END__
    87: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
    88: 0000000000400620     0 FUNC    GLOBAL DEFAULT   11 _init
    89: 00000000004008c4   221 FUNC    GLOBAL DEFAULT   13 generate_password
    90: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND rand@@GLIBC_2.2.5

Version symbols section '.gnu.version' contains 13 entries:
 Addr: 000000000040048c  Offset: 0x00048c  Link: 5 (.dynsym)
  000:   0 (*local*)       2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)   3 (GLIBC_2.4)
  004:   2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)
  008:   0 (*local*)       2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)   4 (GLIBC_2.7)
  00c:   2 (GLIBC_2.2.5)

Version needs section '.gnu.version_r' contains 1 entries:
 Addr: 0x00000000004004a8  Offset: 0x0004a8  Link: 6 (.dynstr)
  000000: Version: 1  File: libc.so.6  Cnt: 3
  0x0010:   Name: GLIBC_2.7  Flags: none  Version: 4
  0x0020:   Name: GLIBC_2.4  Flags: none  Version: 3
  0x0030:   Name: GLIBC_2.2.5  Flags: none  Version: 2

Displaying notes found at file offset 0x00000254 with length 0x00000020:
  Owner                 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:
  Owner                 Data size       Description
  GNU                  0x00000014       NT_GNU_BUILD_ID (unique build ID bitstring)
    Build ID: f70ffbc08652e92fab24dc3a51eb0e386114eb3d
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (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 <http://gnu.org/licenses/gpl.html>
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 1...done.
(gdb) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 1, password () at gdb.c:17
17      gdb.c: No such file or directory.
(gdb) s
18      in gdb.c
(gdb) s
__srandom (x=1453577417) at random.c:210
210     random.c: No such file or directory.
(gdb) s
211     in random.c
(gdb) s
212     in random.c
(gdb) s
__srandom_r (seed=1453577417, buf=buf@entry=0x7ffff7dd36e0 <unsafe_state>) at random_r.c:164
164     random_r.c: No such file or directory.
(gdb) s
172     in random_r.c
(gdb) s
174     in random_r.c
(gdb) s
175     in random_r.c
(gdb) s
178     in random_r.c
(gdb) s
180     in random_r.c
(gdb) s
183     in random_r.c
(gdb) s
182     in random_r.c
(gdb) s
183     in random_r.c
(gdb) s
188     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
```

```
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
```

```
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) s
194     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
195     in random_r.c
(gdb) s
196     in random_r.c
(gdb) s
198     in random_r.c
(gdb) s
199     in random_r.c
(gdb) s
189     in random_r.c
(gdb) c
Continuing.
behold! I will only tell you the secret password if you enter the random number I just generated!
4
you lose :(
[Inferior 1 (process 61914) exited with code 01]
(gdb) b main
Breakpoint 2 at 0x4008a8: file gdb.c, line 33.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 2, main () at gdb.c:33
33      gdb.c: No such file or directory.
(gdb) c
Continuing.

Breakpoint 1, password () at gdb.c:17
17      in gdb.c
(gdb) c
Continuing.
behold! I will only tell you the secret password if you enter the random number I just generated!
2
you lose :(
[Inferior 1 (process 61927) exited with code 01]
(gdb) b main
Note: breakpoint 2 also set at pc 0x4008a8.
Breakpoint 3 at 0x4008a8: file gdb.c, line 33.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 2, main () at gdb.c:33
33      in gdb.c
(gdb) n

Breakpoint 1, password () at gdb.c:17
17      in gdb.c
(gdb) n
18      in gdb.c
(gdb) n
19      in gdb.c
(gdb) n
20      in gdb.c
(gdb) n
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
(gdb) n
5
22      in gdb.c
(gdb) n
27      in gdb.c
(gdb) n
you lose :(
28      in gdb.c
(gdb) n
29      in gdb.c
(gdb) n
main () at gdb.c:35
35      in gdb.c
(gdb) n
36      in gdb.c
(gdb) n
__libc_start_main (main=0x4008a4 <main>, argc=1, argv=0x7fffffffe678, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe668) at libc-start.c:321
321     libc-start.c: No such file or directory.
(gdb) n
[Inferior 1 (process 61933) exited with code 01]
(gdb) n
The program is not being run.
(gdb) b 1
Breakpoint 4 at 0x7ffff7a36dd0: file libc-start.c, line 1.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 4, __libc_start_main (main=0x4008a4 <main>, argc=1, argv=0x7fffffffe678, init=0x400bd0 <__libc_csu_init>, fini=0x400c40 <__libc_csu_fini>, rtld_fini=0x7ffff7dea560 <_dl_fini>,
    stack_end=0x7fffffffe668) at libc-start.c:133
133     libc-start.c: No such file or directory.
(gdb) n
137     in libc-start.c
(gdb) n
133     in libc-start.c
(gdb) n
137     in libc-start.c
(gdb) n
219     in libc-start.c
(gdb) n
137     in libc-start.c
(gdb) n
219     in libc-start.c
(gdb) n
220     in libc-start.c
(gdb) n
242     in libc-start.c
(gdb) n
245     in libc-start.c
(gdb) n
246     in libc-start.c
(gdb) n
250     in libc-start.c
(gdb) n
265     in libc-start.c
(gdb) n
274     in libc-start.c
(gdb) n
```

```
275     in libc-start.c
(gdb) n
280     in libc-start.c
(gdb) n
281     in libc-start.c
(gdb) n
284     in libc-start.c
(gdb) n
287     in libc-start.c
(gdb) n

Breakpoint 2, main () at gdb.c:33
33      gdb.c: No such file or directory.
(gdb) n

Breakpoint 1, password () at gdb.c:17
17      in gdb.c
(gdb) n
18      in gdb.c
(gdb) n
19      in gdb.c
(gdb) n
20      in gdb.c
(gdb) n
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
(gdb) n
n
22      in gdb.c
(gdb) n
27      in gdb.c
(gdb) n
you lose :(
28      in gdb.c
(gdb) n
29      in gdb.c
(gdb) n
main () at gdb.c:35
35      in gdb.c
(gdb) n
36      in gdb.c
(gdb) n
__libc_start_main (main=0x4008a4 <main>, argc=1, argv=0x7fffffffe678, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe668) at libc-start.c:321
321     libc-start.c: No such file or directory.
(gdb) n
[Inferior 1 (process 61939) exited with code 01]
(gdb) quit
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb
GNU gdb (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 <http://gnu.org/licenses/gpl.html>
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".
(gdb) file 1
Reading symbols from 1...done.
(gdb) b gdb.c
Function "gdb.c" not defined.
Make breakpoint pending on future shared library load? (y or [n]) n
(gdb) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
(gdb) n
The program is not being run.
(gdb) n
The program is not being run.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 1, password () at gdb.c:17
17      gdb.c: No such file or directory.
(gdb) n
18      in gdb.c
(gdb) n
19      in gdb.c
(gdb) n
20      in gdb.c
(gdb) n
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
(gdb) n
n
22      in gdb.c
(gdb) n
27      in gdb.c
(gdb) n
you lose :(
28      in gdb.c
(gdb) n
29      in gdb.c
(gdb) n
main () at gdb.c:35
35      in gdb.c
(gdb) n
36      in gdb.c
(gdb) n
__libc_start_main (main=0x4008a4 <main>, argc=1, argv=0x7fffffffe678, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe668) at libc-start.c:321
321     libc-start.c: No such file or directory.
(gdb) n
[Inferior 1 (process 61957) exited with code 01]
(gdb) n
The program is not being run.
(gdb) n
The program is not being run.
(gdb) n
The program is not being run.
(gdb) r main
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1 main

Breakpoint 1, password () at gdb.c:17
17      gdb.c: No such file or directory.
(gdb) n
18      in gdb.c
(gdb) n
19      in gdb.c
(gdb) n
20      in gdb.c
(gdb) n
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
(gdb) n
n
22      in gdb.c
(gdb) n
27      in gdb.c
(gdb) n
you lose :(
28      in gdb.c
```

```
(gdb) n
29      in gdb.c
(gdb) n
main () at gdb.c:35
35      in gdb.c
(gdb) n
36      in gdb.c
(gdb) n
__libc_start_main (main=0x4008a4 <main>, argc=2, argv=0x7fffffffe668, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe658) at libc-start.c:321
321     libc-start.c: No such file or directory.
(gdb) n
[Inferior 1 (process 61967) exited with code 01]
(gdb) Quit
(gdb) clear
No breakpoint at this line.
(gdb) quit
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s 2

Symbol table '.dynsym' contains 14 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND curl_easy_init@CURL_GNUTLS_3 (2)
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND curl_easy_perform@CURL_GNUTLS_3 (2)
     3: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND curl_easy_setopt@CURL_GNUTLS_3 (2)
     5: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIBC_2.2.5 (3)
     7: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     8: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
     9: 0000000000602050     0 NOTYPE  GLOBAL DEFAULT   24 _edata
    10: 0000000000602058     0 NOTYPE  GLOBAL DEFAULT   25 _end
    11: 0000000000400600     0 FUNC    GLOBAL DEFAULT   11 _init
    12: 0000000000602050     0 NOTYPE  GLOBAL DEFAULT   25 __bss_start
    13: 00000000004008f4     0 FUNC    GLOBAL DEFAULT   14 _fini
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf 2
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
     --segments          An alias for --program-headers
  -S --section-headers   Display the sections' header
     --sections          An alias for --section-headers
  -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
     --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)
  -u --unwind            Display the unwind info (if present)
  -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,=frames,
               =frames-interp,=str,=loc,=Ranges,=pubtypes,
               =gdb_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
  -v --version           Display the version number of readelf
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -a 2
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:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Advanced Micro Devices X86-64
  Version:                           0x1
  Entry point address:               0x400680
  Start of program headers:          64 (bytes into file)
  Start of section headers:          8600 (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:
  [Nr] Name              Type             Address           Offset
       Size              EntSize          Flags  Link  Info  Align
  [ 0]                   NULL             0000000000000000  00000000
       0000000000000000  0000000000000000           0     0     0
  [ 1] .interp           PROGBITS         0000000000400238  00000238
       000000000000001c  0000000000000000   A       0     0     1
  [ 2] .note.ABI-tag     NOTE             0000000000400254  00000254
       0000000000000020  0000000000000000   A       0     0     4
  [ 3] .note.gnu.build-i NOTE             0000000000400274  00000274
       0000000000000024  0000000000000000   A       0     0     4
  [ 4] .gnu.hash         GNU_HASH         0000000000400298  00000298
       0000000000000038  0000000000000000   A       5     0     8
  [ 5] .dynsym           DYNSYM           00000000004002d0  000002d0
       0000000000000150  0000000000000018   A       6     1     8
  [ 6] .dynstr           STRTAB           0000000000400420  00000420
       00000000000000f4  0000000000000000   A       0     0     1
  [ 7] .gnu.version      VERSYM           0000000000400514  00000514
       000000000000001c  0000000000000002   A       5     0     2
  [ 8] .gnu.version_r    VERNEED          0000000000400530  00000530
       0000000000000040  0000000000000000   A       6     2     8
  [ 9] .rela.dyn         RELA             0000000000400570  00000570
       0000000000000018  0000000000000018   A       5     0     8
  [10] .rela.plt         RELA             0000000000400588  00000588
       0000000000000078  0000000000000018   A       5    12     8
  [11] .init             PROGBITS         0000000000400600  00000600
       000000000000001a  0000000000000000  AX       0     0     4
  [12] .plt              PROGBITS         0000000000400620  00000620
       0000000000000060  0000000000000010  AX       0     0     16
  [13] .text             PROGBITS         0000000000400680  00000680
       0000000000000272  0000000000000000  AX       0     0     16
  [14] .fini             PROGBITS         00000000004008f4  000008f4
       0000000000000009  0000000000000000  AX       0     0     4
```

```
  [15] .rodata           PROGBITS         0000000000400900  00000900
       0000000000000031  0000000000000000   A       0     0     8
  [16] .eh_frame_hdr     PROGBITS         0000000000400934  00000934
       00000000000000f4  0000000000000000   A       0     0     4
  [17] .eh_frame         PROGBITS         0000000000400a28  00000a28
       00000000000003f4  0000000000000000   A       0     0     8
  [18] .init_array       INIT_ARRAY       0000000000601e00  00001e00
       0000000000000008  0000000000000000  WA       0     0     8
  [19] .fini_array       FINI_ARRAY       0000000000601e08  00001e08
       0000000000000008  0000000000000000  WA       0     0     8
  [20] .jcr              PROGBITS         0000000000601e10  00001e10
       0000000000000008  0000000000000000  WA       0     0     8
  [21] .dynamic          DYNAMIC          0000000000601e18  00001e18
       00000000000001e0  0000000000000010  WA       6     0     8
  [22] .got              PROGBITS         0000000000601ff8  00001ff8
       0000000000000008  0000000000000008  WA       0     0     8
  [23] .got.plt          PROGBITS         0000000000602000  00002000
       0000000000000040  0000000000000008  WA       0     0     8
  [24] .data             PROGBITS         0000000000602040  00002040
       0000000000000010  0000000000000000  WA       0     0     8
  [25] .bss              NOBITS           0000000000602050  00002050
       0000000000000008  0000000000000000  WA       0     0     1
  [26] .comment          PROGBITS         0000000000000000  00002050
       000000000000004d  0000000000000001  MS       0     0     1
  [27] .shstrtab         STRTAB           0000000000000000  0000209d
       00000000000000f8  0000000000000000           0     0     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:
  Type           Offset             VirtAddr           PhysAddr
                 FileSiz            MemSiz              Flags  Align
  PHDR           0x0000000000000040 0x0000000000400040 0x0000000000400040
                 0x00000000000001f8 0x00000000000001f8  R E    8
  INTERP         0x0000000000000238 0x0000000000400238 0x0000000000400238
                 0x000000000000001c 0x000000000000001c  R      1
      [Requesting program interpreter: /lib64/ld-linux-x86-64.so.2]
  LOAD           0x0000000000000000 0x0000000000400000 0x0000000000400000
                 0x000000000000e1c 0x000000000000e1c  R E    200000
  LOAD           0x0000000000001e00 0x0000000000601e00 0x0000000000601e00
                 0x0000000000000250 0x0000000000000258  RW     200000
  DYNAMIC        0x0000000000001e18 0x0000000000601e18 0x0000000000601e18
                 0x00000000000001e0 0x00000000000001e0  RW     8
  NOTE           0x0000000000000254 0x0000000000400254 0x0000000000400254
                 0x0000000000000044 0x0000000000000044  R      4
  GNU_EH_FRAME   0x0000000000000934 0x0000000000400934 0x0000000000400934
                 0x00000000000000f4 0x00000000000000f4  R      4
  GNU_STACK      0x0000000000000000 0x0000000000000000 0x0000000000000000
                 0x0000000000000000 0x0000000000000000  RW     10
  GNU_RELRO      0x0000000000001e00 0x0000000000601e00 0x0000000000601e00
                 0x0000000000000200 0x0000000000000200  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_frame_hdr .eh_frame
   03     .init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
   04     .dynamic
   05     .note.ABI-tag .note.gnu.build-id
   06     .eh_frame_hdr
   07
   08     .init_array .fini_array .jcr .dynamic .got

Dynamic section at offset 0x1e18 contains 25 entries:
  Tag        Type                         Name/Value
 0x0000000000000001 (NEEDED)             Shared library: [libcurl-gnutls.so.4]
 0x0000000000000001 (NEEDED)             Shared library: [libc.so.6]
 0x000000000000000c (INIT)               0x400600
 0x000000000000000d (FINI)               0x4008f4
 0x0000000000000019 (INIT_ARRAY)         0x601e00
 0x000000000000001b (INIT_ARRAYSZ)       8 (bytes)
 0x000000000000001a (FINI_ARRAY)         0x601e08
 0x000000000000001c (FINI_ARRAYSZ)       8 (bytes)
 0x000000006ffffef5 (GNU_HASH)           0x400298
 0x0000000000000005 (STRTAB)             0x400420
 0x0000000000000006 (SYMTAB)             0x4002d0
 0x000000000000000a (STRSZ)              244 (bytes)
 0x000000000000000b (SYMENT)             24 (bytes)
 0x0000000000000015 (DEBUG)              0x0
 0x0000000000000003 (PLTGOT)             0x602000
 0x0000000000000002 (PLTRELSZ)           120 (bytes)
 0x0000000000000014 (PLTREL)             RELA
 0x0000000000000017 (JMPREL)             0x400588
 0x0000000000000007 (RELA)               0x400570
 0x0000000000000008 (RELASZ)             24 (bytes)
 0x0000000000000009 (RELAENT)            24 (bytes)
 0x000000006ffffffe (VERNEED)            0x400530
 0x000000006fffffff (VERNEEDNUM)         2
 0x000000006ffffff0 (VERSYM)             0x400514
 0x0000000000000000 (NULL)               0x0

Relocation section '.rela.dyn' at offset 0x570 contains 1 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000601ff8  000700000006 R_X86_64_GLOB_DAT 0000000000000000 __gmon_start__ + 0

Relocation section '.rela.plt' at offset 0x588 contains 5 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000602018  000100000007 R_X86_64_JUMP_SLO 0000000000000000 curl_easy_init + 0
000000602020  000200000007 R_X86_64_JUMP_SLO 0000000000000000 curl_easy_perform + 0
000000602028  000400000007 R_X86_64_JUMP_SLO 0000000000000000 curl_easy_setopt + 0
000000602030  000600000007 R_X86_64_JUMP_SLO 0000000000000000 __libc_start_main + 0
000000602038  000700000007 R_X86_64_JUMP_SLO 0000000000000000 __gmon_start__ + 0

The decoding of unwind sections for machine type Advanced Micro Devices X86-64 is not currently supported.

Symbol table '.dynsym' contains 14 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND curl_easy_init@CURL_GNUTLS_3 (2)
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND curl_easy_perform@CURL_GNUTLS_3 (2)
     3: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND curl_easy_setopt@CURL_GNUTLS_3 (2)
     5: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIBC_2.2.5 (3)
     7: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     8: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
     9: 0000000000602050     0 NOTYPE  GLOBAL DEFAULT   24 _edata
    10: 0000000000602058     0 NOTYPE  GLOBAL DEFAULT   25 _end
    11: 0000000000400600     0 FUNC    GLOBAL DEFAULT   11 _init
    12: 0000000000602050     0 NOTYPE  GLOBAL DEFAULT   25 __bss_start
    13: 00000000004008f4     0 FUNC    GLOBAL DEFAULT   14 _fini

Histogram for `.gnu.hash' bucket list length (total of 3 buckets):
 Length  Number     % of total  Coverage
      0  0          (  0.0%)
      1  1          ( 33.3%)     20.0%
      2  2          ( 66.7%)    100.0%

Version symbols section '.gnu.version' contains 14 entries:
 Addr: 0000000000400514  Offset: 0x000514  Link: 5 (.dynsym)
```

```
  000:   0 (*local*)       2 (CURL_GNUTLS_3)   2 (CURL_GNUTLS_3)   0 (*local*)
  004:   2 (CURL_GNUTLS_3)   0 (*local*)       3 (GLIBC_2.2.5)   0 (*local*)
  008:   0 (*local*)       1 (*global*)      1 (*global*)      1 (*global*)
  00c:   1 (*global*)      1 (*global*)

Version needs section '.gnu.version_r' contains 2 entries:
 Addr: 0x0000000000400530  Offset: 0x000530  Link: 6 (.dynstr)
  000000: Version: 1  File: libc.so.6  Cnt: 1
  0x0010:   Name: GLIBC_2.2.5  Flags: none  Version: 3
  0x0020: Version: 1  File: libcurl-gnutls.so.4  Cnt: 1
  0x0030:   Name: CURL_GNUTLS_3  Flags: none  Version: 2

Displaying notes found at file offset 0x00000254 with length 0x00000020:
  Owner                 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:
  Owner                 Data size       Description
  GNU                  0x00000014       NT_GNU_BUILD_ID (unique build ID bitstring)
    Build ID: 18ada6ba56c33deac975256efe3955a54be4a407
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ clear

Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (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 <http://gnu.org/licenses/gpl.html>
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 1...done.
(gdb) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
(gdb) info registers
The program has no registers now.
(gdb) n
The program is not being run.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 1, password () at gdb.c:17
17      gdb.c: No such file or directory.
(gdb) i r
rax            0x0      0
rbx            0x0      0
rcx            0x0      0
rdx            0x7fffffffe688   140737488348808
rsi            0x7fffffffe678   140737488348792
rdi            0x1      1
rbp            0x7fffffffe580   0x7fffffffe580
rsp            0x7fffffffe570   0x7fffffffe570
r8             0x7ffff7dd4e80   140737351863936
r9             0x7ffff7dea560   140737351951712
r10            0x7fffffffe420   140737488348192
r11            0x7ffff7a36dd0   140737348070864
r12            0x400710 4196112
r13            0x7fffffffe670   140737488348784
r14            0x0      0
r15            0x0      0
rip            0x400805 0x400805 <password+8>
eflags         0x202    [ IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
=> 0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
=> 0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
```

```
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400811      18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
=> 0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400816      18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
=> 0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400818      18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
=> 0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
```

```
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
19      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
=> 0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400822      19      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
=> 0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) x/d %eax
A syntax error in expression, near `%eax'.
(gdb) p/d %eax
A syntax error in expression, near `%eax'.
(gdb) x/d %eax
A syntax error in expression, near `%eax'.
(gdb) ni
20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
```

```
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
=> 0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040082c      20      in gdb.c
(gdb) ni
0x000000000040082f      20      in gdb.c
(gdb) ni
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
=> 0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040083b      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
=> 0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040083f      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
```

```
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
=> 0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400842      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
=> 0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400845      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
=> 0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040084a      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
```

```
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
=> 0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
88
22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
=> 0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400852      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
=> 0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) i r eax'
Invalid register `eax''
(gdb) i r eax
eax            0x58     88
(gdb) x/d 0x58
```

```
0x58:   Cannot access memory at address 0x58
(gdb) x/d (0x58 - 0x4)
0x54:   Cannot access memory at address 0x54
(gdb) ni
0x0000000000400855      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
=> 0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) x/d (0x58 - 0x4)
0x54:   Cannot access memory at address 0x54
(gdb) i r eax
eax            0x58     88
(gdb) i r rbp
rbp            0x7fffffffe580   0x7fffffffe580
(gdb) x/d ( 0x7fffffffe580 - 0x4)
0x7fffffffe57c: 395572009
(gdb) ni
27      in gdb.c
(gdb) ni
0x0000000000400895      27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
=> 0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400898      27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
```

```
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
=> 0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
you lose :(
28      in gdb.c
(gdb) quit
A debugging session is active.

        Inferior 1 [process 62019] will be killed.

Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (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 <http://gnu.org/licenses/gpl.html>
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 1...done.
(gdb) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 1, password () at gdb.c:17
17      gdb.c: No such file or directory.
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
=> 0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
=> 0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400811      18      in gdb.c
```

```
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
=> 0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400816      18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
=> 0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400818      18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
=> 0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
19      in gdb.c
```

```
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
=> 0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400822      19      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
=> 0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
=> 0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040082c      20      in gdb.c
```

```
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
=> 0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040082f      20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
=> 0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
=> 0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
```

```
0x000000000040083b      21      in gdb.c
(gdb) ni
0x000000000040083f      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
=> 0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400842      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
=> 0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400845      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
=> 0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
```

```
End of assembler dump.
(gdb) ni
0x000000000040084a      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
=> 0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
395572009
22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
=> 0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400852      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
=> 0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
```

```
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400855      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
=> 0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
=> 0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400895      27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
=> 0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
```

```
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400898      27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
=> 0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
you lose :(
28      in gdb.c
(gdb) quit
A debugging session is active.

        Inferior 1 [process 62125] will be killed.

Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (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 <http://gnu.org/licenses/gpl.html>
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 1...done.
(gdb) disas
No frame selected.
(gdb) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 1, password () at gdb.c:17
17      gdb.c: No such file or directory.
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
=> 0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
=> 0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
```

```
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400811      18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
=> 0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) niq
Undefined command: "niq".  Try "help".
(gdb) ni
0x0000000000400816      18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
=> 0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400818      18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
```

```
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
=> 0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
19      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
=> 0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400822      19      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
=> 0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) x/d 0x400700
0x400700 <rand@plt>:    426386943
(gdb) p/d 0x400700
$1 = 4196096
(gdb) p/x rbp
No symbol "rbp" in current context.
(gdb) ni
20      in gdb.c
(gdb) disas
```

```
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
=> 0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040082c      20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
=> 0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040082f      20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
=> 0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
```

```
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
=> 0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
=> 0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040083b      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
=> 0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040083f      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
```

```
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
=> 0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400842      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
=> 0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
=> 0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400845      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
```

```
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
=> 0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) p/x $rax
$2 = 0x400c73
(gdb) p/d $eax
$3 = 4197491
(gdb) p/d $rax
$4 = 4197491
(gdb) ni
0x000000000040084a      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
=> 0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) r/x $eax
The program being debugged has been started already.
Start it from the beginning? (y or n) n
Program not restarted.
(gdb) p/x $eax
$5 = 0x0
(gdb) d/x $eax
warning: bad breakpoint number at or near '/x $eax'
Convenience variable must have integer value.
warning: bad breakpoint number at or near '$eax'
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
=> 0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
```

```
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) p/x $eax
$6 = 0x0
(gdb) p/d $eax
$7 = 0
(gdb) ni
0
22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
=> 0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) p/x ( $rbp - 0x8 )
$8 = 0x7fffffffe578
(gdb) p/d ( $rbp - 0x8 )
$9 = 140737488348536
(gdb) ni
0x0000000000400852      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
=> 0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) p/d $eax
$10 = 0
(gdb) p/x $eax
$11 = 0x0
(gdb) ni
0x0000000000400855      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
```

```
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
=> 0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) p/x $eax
$12 = 0x0
(gdb) p/d $eax
$13 = 0
(gdb) p/d ( $rbp - 0x4 )
$14 = 140737488348540
(gdb) p/x ( $rbp - 0x4 )
$15 = 0x7fffffffe57c
(gdb) p/d 0x7fffffffe57c
$16 = 140737488348540
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
=> 0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
=> 0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400895      27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
```

```
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
=> 0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400898      27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
=> 0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
you lose :(
28      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
=> 0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
29      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
```

```
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
=> 0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x00000000004008a3      29      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
=> 0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x00000000004008b2 in main () at gdb.c:33
33      in gdb.c
(gdb) disa
(gdb) quit
A debugging session is active.

        Inferior 1 [process 62210] will be killed.

Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (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 <http://gnu.org/licenses/gpl.html>
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 1...done.
(gdb) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 1, password () at gdb.c:17
17      gdb.c: No such file or directory.
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
=> 0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
```

```
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
18      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
=> 0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400811      18      in gdb.c
(gdb) dusas
Undefined command: "dusas".  Try "help".
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
=> 0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400816      18      in gdb.c
(gdb) ni
0x0000000000400818      18      in gdb.c
(gdb) ni
19      in gdb.c
(gdb) ni
0x0000000000400822      19      in gdb.c
(gdb) ni
20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
=> 0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
```

```
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) p/d $eax
$1 = 242262210
(gdb) p/d ( $rbp - 0x4 )
$2 = 140737488348540
(gdb) ni
0x000000000040082c      20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
=> 0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) p/d 0x6020a8
$3 = 6299816
(gdb) ni
0x000000000040082f      20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
=> 0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
(gdb) i r
rax            0x62     98
rbx            0x0      0
rcx            0x7ffff7b00870   140737348896880
rdx            0x7ffff7dd59e0   140737351866848
rsi            0x7ffff7ff5000   140737354092544
rdi            0x1      1
rbp            0x7fffffffe580   0x7fffffffe580
rsp            0x7fffffffe570   0x7fffffffe570
r8             0xffffffff       4294967295
```

```
r9             0x0      0
r10            0x22     34
r11            0x246    582
r12            0x400710 4196112
r13            0x7fffffffe670   140737488348784
r14            0x0      0
r15            0x0      0
rip            0x400834 0x400834 <password+55>
eflags         0x246    [ PF ZF IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
(gdb) ni
0x000000000040083b      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
=> 0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) i r
rax            0x400c73 4197491
rbx            0x0      0
rcx            0x7ffff7b00870   140737348896880
rdx            0x7ffff7dd59e0   140737351866848
rsi            0x7ffff7ff5000   140737354092544
rdi            0x1      1
rbp            0x7fffffffe580   0x7fffffffe580
rsp            0x7fffffffe570   0x7fffffffe570
r8             0xffffffff       4294967295
r9             0x0      0
r10            0x22     34
r11            0x246    582
r12            0x400710 4196112
r13            0x7fffffffe670   140737488348784
r14            0x0      0
r15            0x0      0
rip            0x40083b 0x40083b <password+62>
eflags         0x246    [ PF ZF IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
=> 0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040083f      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
```

```
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
=> 0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) i r
rax            0x400c73 4197491
rbx            0x0      0
rcx            0x7ffff7b00870   140737348896880
rdx            0x7fffffffe578   140737488348536
rsi            0x7ffff7ff5000   140737354092544
rdi            0x1      1
rbp            0x7fffffffe580   0x7fffffffe580
rsp            0x7fffffffe570   0x7fffffffe570
r8             0xffffffff       4294967295
r9             0x0      0
r10            0x22     34
r11            0x246    582
r12            0x400710 4196112
r13            0x7fffffffe670   140737488348784
r14            0x0      0
r15            0x0      0
rip            0x40083f 0x40083f <password+66>
eflags         0x246    [ PF ZF IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
=> 0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400842      21      in gdb.c
(gdb) ni
0x0000000000400845      21      in gdb.c
(gdb) ni
0x000000000040084a      21      in gdb.c
(gdb) ni
ni
22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
```

```
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
=> 0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400852      22      in gdb.c
(gdb) ni
0x0000000000400855      22      in gdb.c
(gdb) ni
27      in gdb.c
(gdb) quit
A debugging session is active.

        Inferior 1 [process 62493] will be killed.

Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (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 <http://gnu.org/licenses/gpl.html>
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 1...done.
(gdb) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
(gdb) ni
The program is not being run.
(gdb) ni
The program is not being run.
(gdb) ni
The program is not being run.
(gdb) ni
The program is not being run.
(gdb) ni
The program is not being run.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 1, password () at gdb.c:17
17      gdb.c: No such file or directory.
(gdb) ni
18      in gdb.c
(gdb) ni
0x0000000000400811      18      in gdb.c
(gdb) ni
0x0000000000400816      18      in gdb.c
(gdb) ni
0x0000000000400818      18      in gdb.c
(gdb) ni
19      in gdb.c
(gdb) ni
0x0000000000400822      19      in gdb.c
(gdb) ni
20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
=> 0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040082c      20      in gdb.c
(gdb) ni
0x000000000040082f      20      in gdb.c
(gdb) ni
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
```

```
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
=> 0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040083b      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
=> 0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040083f      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
=> 0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400842      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
```

```
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
=> 0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400845      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
=> 0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040084a      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
=> 0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) i r
rax            0x0      0
rbx            0x0      0
rcx            0x7ffff7b00870   140737348896880
rdx            0x7fffffffe578   140737488348536
```

```
rsi            0x7fffffffe578   140737488348536
rdi            0x400c73 4197491
rbp            0x7fffffffe580   0x7fffffffe580
rsp            0x7fffffffe570   0x7fffffffe570
r8             0xffffffff       4294967295
r9             0x0      0
r10            0x22     34
r11            0x246    582
r12            0x400710 4196112
r13            0x7fffffffe670   140737488348784
r14            0x0      0
r15            0x0      0
rip            0x40084a 0x40084a <password+77>
eflags         0x246    [ PF ZF IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
=> 0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
98
22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
=> 0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400852      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
=> 0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
```

```
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400855      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
=> 0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
=> 0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400895      27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
```

```
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
=> 0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400898      27      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
=> 0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
you lose :(
28      in gdb.c
(gdb) quit
A debugging session is active.

        Inferior 1 [process 62608] will be killed.

Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ disas
disas: command not found
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ packet_write_wait: Connection to 23.99.192.124: Broken pipe
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 Sat Jan 23 18:55:18 UTC 2016

  System load:  0.01              Processes:           116
  Usage of /:   5.5% of 28.80GB   Users logged in:     0
  Memory usage: 6%                IP address for eth0: 10.2.0.4
  Swap usage:   0%

  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

22 packages can be updated.
21 updates are security updates.


Last login: Sat Jan 23 18:55:26 2016 from 104-1-26-208.lightspeed.cicril.sbcglobal.net
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
0  1  2  3  4  howto.txt  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (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 <http://gnu.org/licenses/gpl.html>
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 1...done.
(gdb) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 1, password () at gdb.c:17
```

```
17      gdb.c: No such file or directory.
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
=> 0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
18      in gdb.c
(gdb) ni
0x0000000000400811      18      in gdb.c
(gdb) ni
0x0000000000400816      18      in gdb.c
(gdb) ni
0x0000000000400818      18      in gdb.c
(gdb) ni
19      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
=> 0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400822      19      in gdb.c
(gdb) p $eax
$1 = 981461572
(gdb) print $eax
$2 = 981461572
(gdb) ni
20      in gdb.c
(gdb) ni
0x000000000040082c      20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
=> 0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
```

```
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040082f      20      in gdb.c
(gdb) ni
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
(gdb) ni
0x000000000040083b      21      in gdb.c
(gdb) ni
0x000000000040083f      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
=> 0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400842      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
=> 0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400845      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
=> 0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
```

```
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040084a      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
=> 0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
981461572
22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
=> 0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400852      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
```

```
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
=> 0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400855      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
=> 0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
=> 0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040085e      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
```

```
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
=> 0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400861      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
=> 0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400866      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
=> 0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400869      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
```

```
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
=> 0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400870      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
=> 0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400877      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
=> 0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040087a      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
```

```
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
=> 0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040087d      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
=> 0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400882      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
=> 0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
you win! the secret is:
dUJSQFAOAg==
25      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
```

```
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
=> 0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040088c      25      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
=> 0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
29      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
=> 0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x00000000004008a3      29      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
```

```
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
=> 0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x00000000004008b2 in main () at gdb.c:33
33      in gdb.c
(gdb) disas
Dump of assembler code for function main:
   0x00000000004008a4 <+0>:     push   %rbp
   0x00000000004008a5 <+1>:     mov    %rsp,%rbp
   0x00000000004008a8 <+4>:     mov    $0x0,%eax
   0x00000000004008ad <+9>:     callq  0x4007fd <password>
=> 0x00000000004008b2 <+14>:    test   %al,%al
   0x00000000004008b4 <+16>:    je     0x4008bd <main+25>
   0x00000000004008b6 <+18>:    mov    $0x0,%eax
   0x00000000004008bb <+23>:    jmp    0x4008c2 <main+30>
   0x00000000004008bd <+25>:    mov    $0x1,%eax
   0x00000000004008c2 <+30>:    pop    %rbp
   0x00000000004008c3 <+31>:    retq
End of assembler dump.
(gdb) ni
0x00000000004008b4      33      in gdb.c
(gdb) disas
Dump of assembler code for function main:
   0x00000000004008a4 <+0>:     push   %rbp
   0x00000000004008a5 <+1>:     mov    %rsp,%rbp
   0x00000000004008a8 <+4>:     mov    $0x0,%eax
   0x00000000004008ad <+9>:     callq  0x4007fd <password>
   0x00000000004008b2 <+14>:    test   %al,%al
=> 0x00000000004008b4 <+16>:    je     0x4008bd <main+25>
   0x00000000004008b6 <+18>:    mov    $0x0,%eax
   0x00000000004008bb <+23>:    jmp    0x4008c2 <main+30>
   0x00000000004008bd <+25>:    mov    $0x1,%eax
   0x00000000004008c2 <+30>:    pop    %rbp
   0x00000000004008c3 <+31>:    retq
End of assembler dump.
(gdb) ni
34      in gdb.c
(gdb) disas
Dump of assembler code for function main:
   0x00000000004008a4 <+0>:     push   %rbp
   0x00000000004008a5 <+1>:     mov    %rsp,%rbp
   0x00000000004008a8 <+4>:     mov    $0x0,%eax
   0x00000000004008ad <+9>:     callq  0x4007fd <password>
   0x00000000004008b2 <+14>:    test   %al,%al
   0x00000000004008b4 <+16>:    je     0x4008bd <main+25>
=> 0x00000000004008b6 <+18>:    mov    $0x0,%eax
   0x00000000004008bb <+23>:    jmp    0x4008c2 <main+30>
   0x00000000004008bd <+25>:    mov    $0x1,%eax
   0x00000000004008c2 <+30>:    pop    %rbp
   0x00000000004008c3 <+31>:    retq
End of assembler dump.
(gdb) ni
0x00000000004008bb      34      in gdb.c
(gdb) disas
Dump of assembler code for function main:
   0x00000000004008a4 <+0>:     push   %rbp
   0x00000000004008a5 <+1>:     mov    %rsp,%rbp
   0x00000000004008a8 <+4>:     mov    $0x0,%eax
   0x00000000004008ad <+9>:     callq  0x4007fd <password>
   0x00000000004008b2 <+14>:    test   %al,%al
   0x00000000004008b4 <+16>:    je     0x4008bd <main+25>
   0x00000000004008b6 <+18>:    mov    $0x0,%eax
=> 0x00000000004008bb <+23>:    jmp    0x4008c2 <main+30>
   0x00000000004008bd <+25>:    mov    $0x1,%eax
   0x00000000004008c2 <+30>:    pop    %rbp
   0x00000000004008c3 <+31>:    retq
End of assembler dump.
(gdb) quit
A debugging session is active.

        Inferior 1 [process 63153] will be killed.

Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cat secrets.txt
0. dEFTR1ENAw==
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./1
behold! I will only tell you the secret password if you enter the random number I just generated!
981461572
you lose :(
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (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 <http://gnu.org/licenses/gpl.html>
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 1...done.
(gdb) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
(gdb) disas
No frame selected.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1

Breakpoint 1, password () at gdb.c:17
17      gdb.c: No such file or directory.
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
=> 0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
```

```
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
18      in gdb.c
(gdb) ni
0x0000000000400811      18      in gdb.c
(gdb) ni
0x0000000000400816      18      in gdb.c
(gdb) ni
0x0000000000400818      18      in gdb.c
(gdb) ni
19      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
=> 0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400822      19      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
=> 0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) p $eax
$1 = 1111437705
```

```
(gdb) ni
20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
=> 0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040082c      20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
=> 0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040082f      20      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
=> 0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
```

```
(gdb) ni
behold! I will only tell you the secret password if you enter the random number I just generated!
21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
=> 0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040083b      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
=> 0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040083f      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
=> 0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
```

```
End of assembler dump.
(gdb) ni
0x0000000000400842      21      in gdb.c
(gdb) ni
0x0000000000400845      21      in gdb.c
(gdb) ni
0x000000000040084a      21      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
=> 0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
1111437705
22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
=> 0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400852      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
=> 0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
```

```
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400855      22      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
=> 0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
=> 0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040085e      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
=> 0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
```

```
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400861      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
=> 0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400866      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
=> 0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
```

```
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400870      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
=> 0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400877      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
=> 0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040087a      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
=> 0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
```

```
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x000000000040087d      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
=> 0x000000000040087d <+128>:   mov    $0x0,%eax
   0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
0x0000000000400882      23      in gdb.c
(gdb) disas
Dump of assembler code for function password:
   0x00000000004007fd <+0>:     push   %rbp
   0x00000000004007fe <+1>:     mov    %rsp,%rbp
   0x0000000000400801 <+4>:     sub    $0x10,%rsp
   0x0000000000400805 <+8>:     movl   $0x0,-0x8(%rbp)
   0x000000000040080c <+15>:    mov    $0x0,%edi
   0x0000000000400811 <+20>:    callq  0x4006d0 <time@plt>
   0x0000000000400816 <+25>:    mov    %eax,%edi
   0x0000000000400818 <+27>:    callq  0x4006a0 <srand@plt>
   0x000000000040081d <+32>:    callq  0x400700 <rand@plt>
   0x0000000000400822 <+37>:    mov    %eax,-0x4(%rbp)
   0x0000000000400825 <+40>:    mov    0x20187c(%rip),%rax        # 0x6020a8 <r>
   0x000000000040082c <+47>:    mov    %rax,%rdi
   0x000000000040082f <+50>:    callq  0x400650 <puts@plt>
   0x0000000000400834 <+55>:    mov    0x201865(%rip),%rax        # 0x6020a0 <d>
   0x000000000040083b <+62>:    lea    -0x8(%rbp),%rdx
   0x000000000040083f <+66>:    mov    %rdx,%rsi
   0x0000000000400842 <+69>:    mov    %rax,%rdi
   0x0000000000400845 <+72>:    mov    $0x0,%eax
   0x000000000040084a <+77>:    callq  0x4006f0 <__isoc99_scanf@plt>
   0x000000000040084f <+82>:    mov    -0x8(%rbp),%eax
   0x0000000000400852 <+85>:    cmp    %eax,-0x4(%rbp)
   0x0000000000400855 <+88>:    jne    0x40088e <password+145>
   0x0000000000400857 <+90>:    mov    0x201832(%rip),%rax        # 0x602090 <o>
   0x000000000040085e <+97>:    mov    %rax,%rdi
   0x0000000000400861 <+100>:   callq  0x4008c4 <generate_password>
   0x0000000000400866 <+105>:   mov    %rax,%rdx
   0x0000000000400869 <+108>:   mov    0x201848(%rip),%rcx        # 0x6020b8 <p>
   0x0000000000400870 <+115>:   mov    0x201821(%rip),%rax        # 0x602098 <s>
   0x0000000000400877 <+122>:   mov    %rcx,%rsi
   0x000000000040087a <+125>:   mov    %rax,%rdi
   0x000000000040087d <+128>:   mov    $0x0,%eax
=> 0x0000000000400882 <+133>:   callq  0x400680 <printf@plt>
   0x0000000000400887 <+138>:   mov    $0x1,%eax
   0x000000000040088c <+143>:   jmp    0x4008a2 <password+165>
   0x000000000040088e <+145>:   mov    0x20181b(%rip),%rax        # 0x6020b0 <f>
   0x0000000000400895 <+152>:   mov    %rax,%rdi
   0x0000000000400898 <+155>:   callq  0x400650 <puts@plt>
   0x000000000040089d <+160>:   mov    $0x0,%eax
   0x00000000004008a2 <+165>:   leaveq
   0x00000000004008a3 <+166>:   retq
End of assembler dump.
(gdb) ni
you win! the secret is:
dUJSQFAOAg==
25      in gdb.c
(gdb) quit
A debugging session is active.

        Inferior 1 [process 63200] will be killed.

Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi howto.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cat howto.txt
0.
The 0 executable gave the answer right away. I just had to run the executable and it gave the secret right away!
1.
For this one, I had to:
* run gdb
* load file "1" and make the breakpoint at 1st line.
* then i ran the program and did "disas" to understand what each register is storing.
* After some trial and errors alongwith receiving "you lose : (" message  , i figured out the register in which the return value of rand() was stored. It was eax.
* i did " p $eax" which gave me a random number 981461572(which was created by the program at that time).
* i entered that number in scanf call. After several "ni" it printed the password at generate_password() call.


Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi howto.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi howto.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi howto.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi howto.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi howto.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi howto.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$
```