```
Last login: Fri Jan 22 22:36:57 on console
Dhrumils-Air:~ Dhrumils ssh Dpate85@23.99.192.124
Dpate85@23.99.192.124's password:
Welcome to Ubuntu 14.04.3 LTS (GMU/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
      Memory usage: 6%
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 public

Dpate85@hrumil:-$ cd public

Dpate85@hrumil:-$ public$ git pull

remote: Counting objects: 110, done.

remote: Counting objects: 100% (8/8), done.

Unpacking objects: 100% (9/9), done.

remote: Total 9 (delta 4), reused 0 (delta 0)

From git. uichits.net:c361-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

files changed, 0 insertions(+), 0 deletions(-)

create mode 100755 hw2/puzzles/0

create mode 100755 hw2/puzzles/0

create mode 100755 hw2/puzzles/3

create mode 100755 hw2/puzzles/3
  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
 @DDQ7tdR?td``??/lib64/ld-linux-x86-64.so.2GNUGNUZ_???}@q?aaS¿}>??
/!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?????A?C
$ ?????)A?C
D?????eB?E?E ?E(?H0?H8?M@l8A0A(B BB??????@?@
(@
  ???o?@?@?@
   x
`?h@P@ ???o @???o???@(`f@v@?@?@?@?@?@?@?
  @

@BBCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/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

888fff !tets477707e>
                                                                                                                                      ,
?@?E?@?xN???[???o @ iP@th@h?
                      ~(@(vP@P???@????
 @?
                 ??
  @?
?D
      aD
          D??
                    ?
? ?(`(???```? ?`??0?M9?Dpate85@Dhrumil:~/public/hw2/puzzles$ clear
 Dpate85@Dhrumil:~/public/hw2/puzzles$ ls
  Dpate85@Dhrumil:~/public/hw2/puzzles$ cd ..
  Dpate85@Dhrumil:~/public/hw2$ ls
 Upateoseen.unci./
puzzles
Dpate85g0hrumil:~/public/hw2$ cp puzzles ./dpate85
cp: omitting directory 'puzzles'
Dpate85g0hrumil:~/public/hw2$ ls
  puzzles
Dpate85@Dhrumil:~/public/hw2$ cd ..
  Dpate85@Dhrumil:~/public$ ls
  hw1 hw2
Dpate85@Dhrumil:~/public$ cd
 Dpate85@Dhrumil:~s cp ./public/hw2 ./dpate85/
cp: omitting directory './public/hw2'.
Dpate85@Dhrumil:~$ cp ./public/hw2'.
Dpate85@Dhrumil:~$ cp ./public/hw2'. /dpate85/
cp: cannot stat './public/hw2'. No such file or
Dpate85@Dhrumil:~$ cp -r ./public/hw2'./dpate85/
                                                                                                  or directory
```

```
Dpate85@Dhrumil:~$ ls
  dpate85  public
Dpate85@Dhrumil:~$ cd dpate85
  Dpate85@Dhrumil:~/dpate85$ ls
  hw1 hw2 README.md
Dpate85@Dhrumil:~/dpate85$ cd hw2
Dpate85@Dhrumil:~/dpate85/hw2$ ls
  Dpate85@Dhrumil:~/dpate85/hw2$ cd puzzles
  Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
  Upateo3@Uniumit://pateos/
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@hrumil:~/dpate85/hw2/puzzles$ vi secrets.txt
Dpate85@hrumil:~/dpate85/hw2/puzzles$ vi secrets.txt
Dpate85@hrumil:~/dpate85/hw2/puzzles$ vi secrets.txt
Dpate85@hrumil:~/dpate85/hw2/puzzles$ vi howto.txt
Dpate85@hrumil:~/dpate85/hw2/puzzles$ vi howto.txt
  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!
 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:
                                                                                                                                                                                                UND puts@GLIBC_2.2.5 (2)
UND strlengGLIBE_2.2.5 (2)
UND _stack_chk_fail@GLIBC_2.4 (3)
UND _printf@GLIBC_2.2.5 (2)
                                                                                                                                                                                                UND _ libc_start_main@GLIBC_2.2.5 (2)
UND calloc@GLIBC_2.2.5 (2)
     Display information about the contents of ELF format files

Options are:

-a -all
-h -file-header
-l -program-headers
-s-segments
-S -s-section-headers
-s-sections
-groups
-t -section-deatals
-e -headers
-s-syms
-s-syms
-s-syms
-symbols
-symbols
-m-n-notes
-s-syms
-n-notes
-n-notes
-n-notes
-n-notes
-n-notes
-n-notes
-r-r-elocs
-r-r-section-info
-r-syms
-r-syms
-r-syms
-r-syms
-r-syms
-r-symbols
-r-syms
-r-symbols
-r-syms
-r-symbols
-r-syms
-r-symbols
-r-syms

DEXEC (Executable file)
Advanced Micro Devices X86-64
0x1
0x4005c0
64 (bytes into file)
4664 (bytes into file)
0x0
64 (bytes)
55 (bytes)
9

        Version:
        0x1

        Start of program headers:
        64

        Start of program headers:
        64

        Start of section headers:
        64

        Start of section header:
        64

        Size of this header:
        64

        Size of program header:
        56

        Sum ber of program headers:
        9

        Size of section headers:
        64

        Sum ber of section headers:
        28

        Section header string table index:
        27

                                                                                                                                   64 (bytes)
     Section Headers:
```

```
PROGBITS 000000000400550 00000550 00000000000 AX 0 0 16
   [13]
         [14] .fini
 There are no section groups in this file.
       Program Headers:
   Type
   PHDR
   INTERP
   LOAD
   DYNAMIC
  Section to Segment mapping:
Segment Sections...
            .in.erp ...ote.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
.init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
            .dynamic
.note.ABI-tag .note.gnu.build-id
.eh_frame_hdr
           .init_array .fini_array .jcr .dynamic .got
 Dynamic section at offset 0xe28 contains 24 entries:
  0x0
0x601000
192 (bytes)
RELA
                                              0×400468
                                             0x400468
0x400450
24 (bytes)
24 (bytes)
0x400420
   0x000000000000000 (RELASZ)
0x0000000000000000 (RELAST)
0x000000000fffffff (VERNEED)
0x000000006fffffff (VERNEEDNUM)
  0x0000000006ffffff0 (VERSYM)
0x00000000000000000 (NULL)
                                              0×400408
 Relocation section '.rela.dyn' at offset 0x450 contains 1 entries:

Offset Info Type Sym. Value Sym. Name + Addend
00000600ff8 000700000006 R_X86_64_GLOB_DAT 00000000000000 __gmon_start__ + 0
 Relocation section '.rela.plt' at offset 0x468 contains 8 entries:
The decoding of unwind sections for machine type Advanced Micro Devices X86-64 is not currently supported.
 Symbol table '.dynsym' contains 9 entries:
      0 NOTYPE WEAK DEFAULT UND _gmon_start_
0 FUNC GLOBAL DEFAULT UND getlogin_r@GLIBC_2.2.5 (2)
         000000000000000000
       8: 00000000000000000
 Version symbols section '.gnu.version' contains 9 entries:
Addr: 00000000004004000 Offset: 0x0004008 Link: 5 (.dynsym)
0000: 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*)
```

000000000000001a 000000000000000 AX

```
008: 2 (GLIBC_2.2.5)
```

```
Version needs section '.gnu.version_r' contains 1 entries:
Addr: 0x00000000000400420 Offset: 0x000420 Link: 6 (.dynstr)
000000: Version: 1 file: libc.so.6 Cnt: 2
0x0010: Name: GLIBC_2.4 Flags: none Version: 2
0x0020: Name: GLIBC_2.4.5 Flags: none Version: 2
 Displaying notes found at file offset 0x00000254 with length 0x00000020:
                                   Data size Description
0x00000010 NT_GNU_ABI_TAG (ABI version tag)
         GNU
               OS: Linux, ABI: 2.6.24
 Displaying notes found at file offset 0x00000274 with length 0x00000024:
               program inter found at first 0x800000274 With tength 0x80000024.

wher Data size Description

0x800000014 NT.GNU_BUILD_ID (unique build ID bitstring)

Build ID: 325f04855747404971ff61615357a07bdd9f94de
         GNU
 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!
 Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
 0 1 2 3 4 howto.txt secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s 1
                  | Not | Table | ".dynsym" | Contains 13 entries: | Not | Not
 Symbol table '.dynsym' contains 13 entries:
                           Symbol table '.symtab' contains 91 entries:
                                                                                                                                                                                      Vis Ndx Name
DEFAULT UND
                                                                                                                                                                                                                      8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
36 register_tm_clones
13 deregister_tm_clones
13 register_tm_clones
13 register_tm_clones
13 deregister_tm_clones
13 register_tm_clones
13 register_tm_clones
14 deregister_tm_clones
15 register_tm_clones
16 register_tm_clones
17 register_tm_clones
18 register_tm_clones
19 register_tm_clones
10 register_tm_clones
10 register_tm_clones
10 register_tm_clones
10 register_tm_clones
11 register_tm_clones
12 register_tm_clones
13 register_tm_clones
13 register_tm_clones
13 register_tm_clones
14 register_tm_clones
15 register_tm_clones
16 register_tm_clones
17 register_tm_clones
18 register_tm_clones
18 register_tm_clones
19 register_tm_clones
10 register_
                                                                                                                                                          LOCAL DEFAULT ABS
LOCAL DEFAULT ABS
LOCAL DEFAULT ABS
LOCAL DEFAULT B __init_array_end
LOCAL DEFAULT 18 __init_array_end
LOCAL DEFAULT 18 __init_array_estart
LOCAL DEFAULT 18 __init_array_estart
LOCAL DEFAULT 13 __iloc_csu_fini
WEAK DEFAULT 13 __iloc_csu_fini
WEAK DEFAULT UND puts@eGLIBC_2.2.5
GLOBAL DEFAULT 24 data_start
GLOBAL DEFAULT 24 G
GLOBAL DEFAULT 24 G
GLOBAL DEFAULT 24 g
GLOBAL DEFAULT 24 p
GLOBAL DEFAULT 24 p
GLOBAL DEFAULT 44 __fini
GLOBAL DEFAULT 14 __fini
GLOBAL DEFAULT 10 ND strlene@GLIBC_2.2.5
                                                                                                                     8 OBJECT
8 OBJECT
                               0 NOTYPE
                                                                                                                   8 OBJECT
0 FUNC
0 FUNC
                              62: 000000000000000000
                              000000000000000000
                                                                                                                    0 FUNC
                                                                                                                                                             GLOBAL DEFAULT UND __stack_chk_fail@@GLIBC_2
GLOBAL DEFAULT 24 f
                                                                                                          8 OBJECT
0 FUNC
167 FUNC
0 FUNC
0 FUNC
                  64: 000000000006020b0
                                                                                                                                                           GLOBAL DEFAULT
                                                                                                                                                            GLOBAL DEFAULT 24 f
GLOBAL DEFAULT UND printf@@GLIBC_2.2.5
GLOBAL DEFAULT UND _libc_start_main@@GLIBC_GLOBAL DEFAULT UND _and@@GLIBC_2.2.5
GLOBAL DEFAULT UND calloc@GLIBC_2.2.5
GLOBAL DEFAULT UND calloc@GLIBC_2.2.5
                  65: 000000000000000000
                  66: 00000000004007fd
                  67: 00000000000000000
                  68: 00000000000000000
                  69:
                              000000000000000000
                                                                                                                    0 FUNC
                                                                                                                                                          GLOBAL DEFAULT UND calloc@eGLIBC_2.2.
GLOBAL DEFAULT 24
GLOBAL HERAULT 24
GLOBAL HIDDEN 24
GLOBAL HIDDEN 24
GLOBAL DEFAULT 15
GLOBAL DEFAULT 25
GLOBAL DEFAULT 35
GLOBAL DEFAULT 35
GLOBAL DEFAULT 35
GLOBAL DEFAULT 43
GLOBAL DEFAULT 45
GLOBAL DEFAULT 45
GLOBAL DEFAULT 45
GLOBAL DEFAULT 42
GLOBAL DEFAULT 44
GLOBAL DEFAULT 45
GLOBAL DEFAULT 45
GLOBAL DEFAULT 45
GLOBAL DEFAULT 55
DSS_SSSSTATT
                  70:
                               00000000000602080
                                                                                                                     0 NOTYPE
                                 00000000000000000
                                                                                                                    0 NOTYPE
                                 0000000000602088
                                                                                                                    0 OBJECT
                                                                                                           4 OBJECT
0 FUNC
101 FUNC
                                 0000000000400c50
                                 00000000000000000
                                 0000000000400bd0
                                 0000000000602110
                                                                                                                   0 NOTYPE
                                 0000000000400710
                                                                                                            0 FUNC
553 FUNC
                  78:
                                 00000000004009a1
                                                                                                                                                           GLOBAL DEFAULT
GLOBAL DEFAULT
GLOBAL DEFAULT
                                 0000000000602090
                                                                                                                   8 OBJECT
8 OBJECT
                  80:
                                 0000000000602098
                                                                                                                                                          GLOBAL DEFAULT 24 S
GLOBAL DEFAULT 25 __bs_start
GLOBAL DEFAULT 25 __bs_start
GLOBAL DEFAULT 13 main
WEAK DEFAULT 13 main
WEAK DEFAULT UND _Jv_RegisterClasses
GLOBAL DEFAULT UND _Jv_RegisterClasses
GLOBAL DEFAULT UND _ITM_registerTMCloneTable
GLOBAL DEFAULT UND _ITM_registerTMCloneTable
GLOBAL DEFAULT 11 __init
                                 00000000000602100
                                                                                                                    0 NOTYPE
                  82:
                               000000000000000000
                                                                                                                 0 FUNC
32 FUNC
                                 0000000000004008a4
                                                                                                                   0 NOTYPE
0 FUNC
0 OBJECT
                                 0000000000000000000
                                 0000000000000000000
                                 000000000000602110
                                 00000000000000000
                                                                                                                     0 NOTYPE
                  88: 0000000000400620
                                                                                                                     0 FUNC
```

```
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
behelod! 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:
- ^4b
      * gdb
* gdb-minimal
  * gdb-minimal
Try: Sudo apt-get install <selected package>
Dpate85@Dhrumil:-/dpate85/hv2/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:
Journal of State Services of S
   gdb-doc gdbserver
Recommended packages:
  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!
   (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.5:81 81 in ../sysdeps/unix/syscall-template.5
    (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.5:81 81 ../sysdeps/unix/syscall-template.5: 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
   Program received signal SIGINT, Interrupt.
   (gdb) clear
   No breakpoint at this line.
     (adh) 1s
   Undefined command: "ls". Try "help".
    (qdb) exit
```

```
Undefined command: "exit". Try "help".
  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
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./1
behold! I will only tell you the secret password if you enter the random number I just generated!
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
                                               ELF64
                                               2's complement, little endian
  Data:
                                               1 (current)
                                               UNIX - System V
  OS/ABI:
  ABI Version:
                                               EXEC (Executable file)
Advanced Micro Devices X86-64
  Type:
  Machine:
  Version:
                                               0x1
0x400710
  Entry point address:
Start of program headers:
Start of section headers:
                                               64 (bytes into file)
9728 (bytes into file)
   Flags:
  Flags:
Size of this header:
Size of program headers:
Number of program headers:
Size of section headers:
Number of section headers:
                                               64 (bytes)
56 (bytes)
                                               9
64 (bytes)
  Section header string table index: 32
Section Headers:
       Address Offset
Flags Link Info Align
00000000000000000 00000000
  [Nr] Name
Size
                                Type
EntSize
                               NULL
0000000000000000000
  [ 1]
  [ 4] .gnu.hash
00000000000000001c
  [ 5] .dynsym
000000000000138
  [28]
  [29]
  [30]
  [31]
  [32]
  [33]
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
                                             VirtAddr
                                                                      PhysAddr
  PHDR
  INTERP
  LOAD
  LOAD
  DYNAMIC
```

NOTE GNU FH FRAME GNU STACK

```
        0x000000000000000
        0x0000000000000
        RW
        10

        0x0000000000001e10
        0x000000000001e10
        0x000000000001e10
        0x000000000001e10

        0x0000000000001f0
        R
        1

   Section to Segment mapping:
   Seament Sections...
     01
               .interp
               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
.init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
               .note.ABI-tag .note.gnu.build-id
     07
     08
              .init array .fini array .icr .dvnamic .got
 Dynamic section at offset 0x1e28 contains 24 entries:
   Tag Type
0x00000000000000001 (NEEDED)
                                                         Name/Value
                                                        Shared library: [libc.so.6]
  0x000000000000000 (INIT)
0x0000000000000000 (FINI)
                                                        0×400620
                                                        0x400c44
   0x00000000000000019 (INIT_ARRAY)
0x0000000000000001b (INIT_ARRAYSZ)
                                                        0x601e10
                                                        8 (bytes)
  0x000000000000001 (INII_ARRAYS2)
0x00000000000001 (FINI_ARRAYS2)
0x0000000000000001 (FINI_ARRAYS2)
0x00000000000000001 (FINI_ARRAYS2)
0x000000000000000005 (STRTAB)
0x000000000000000005 (STRTAB)
0x000000000000000005 (STRTXB)
0x00000000000000000 (STRS2)
                                                        0x601e18
                                                        8 (bytes)
                                                        0x400298
                                                         0x4003f0
                                                        0x4002b8
  156 (bytes)
                                                         24 (bytes)
                                                        0x0
0x602000
                                                         288 (bytes)
                                                         0×400500
                                                         0x4004e8
                                                         24 (bytes)
24 (bytes)
                                                        0x4004a8
                                                        0x40048c
   0x0000000000000000 (NULL)
                                                        0x0
The decoding of unwind sections for machine type Advanced Micro Devices X86-64 is not currently supported.
000000000000000000
                                        0 SECTION LOCAL
                                                              DEFAULT
      28: 000000000000000000
                                        0 SECTION LOCAL
                                                              DEFAULT
      29:
           000000000000000000
                                        0 SECTION LOCAL
                                                              DEFAULT
      30: 00000000000000000
                                        0 SECTION LOCAL
                                                              DEFAULT
      31: 00000000000000000
                                        0 SECTION LOCAL
                                                              DEFAULT
                                                                            31
                                                              DEFAULT ABS crtstuff.c
DEFAULT 20 __JCR_LIST
DEFAULT 13 deregister
      32: 00000000000000000
                                        0 FILE
                                                     LOCAL
                                       0 FILE LOCAL
0 OBJECT LOCAL
0 FUNC LOCAL
0 FUNC LOCAL
                                                                           ABS Crtstuff.C
20 __JCR_LIST__
13 deregister_tm_clones
13 register_tm_clones
13 __do_global_dtors_aux
25 completed.6973
      33: 0000000000601e20
      34: 0000000000400740
                                                            __w_ctones
__uo_global_dtors_aux
...ul 25 completed.6973

DEFAULT 19 _do_global_dtors_aux_fin
DEFAULT 13 frame_dummy
DEFAULT 18 _frame_dummy_init_array_
DEFAULT ABS db6.4.c
DEFAULT 24 encodi-
      35: 0000000000400770
      36: 00000000004007b0
                                        0 FUNC
                                                     LOCAL
      37: 0000000000602100
                                        1 OBJECT
                                                    LOCAL
LOCAL
      38: 0000000000601e18
                                        0 OBJECT
      39: 00000000004007d0
                                        0 FUNC
                                                      LOCAL
                                       0 OBJECT
0 FILE
0 FILE
      40: 0000000000601e10
                                                     LOCAL
      41: 00000000000000000
                                                     LOCAL
      42: 00000000000000000
                                                     LOCAL
                                      0 FILE
64 OBJECT
12 OBJECT
0 FILE
0 OBJECT
0 OBJECT
0 FILE
                                                              DEFAULT 24 mod_table
DEFAULT ABS SU4.C
DEFAULT 24 mod_table
DEFAULT ABS crtstuff.c
      43: 00000000006020c0
                                                     LOCAL
      44: 0000000000602100
                                                    LOCAL
      45: 00000000000000000
                                                     LOCAL
                                                                           17 __FRAME_END_
20 __JCR_END__
      46: 00000000000400eb0
                                                     LOCAL
LOCAL
                                                              DEFAULT
DEFAULT
           000000000000601e20
                                                              DEFAULT ABS
DEFAULT 18
DEFAULT 21
           0000000000000000000
                                                      LOCAL
                                                                           18 __init_array_end
21 _DYNAMIC
                                        0 NOTYPE
0 OBJECT
           000000000000601e18
                                                     LOCAL
LOCAL
           0000000000000001e28
```

18 \_\_init\_array\_start 23 GLOBAL OFFSET TABLE

00000000000601e10

52: 0000000000602000

0 NOTYPE LOCAL DEFAULT 0 OBJECT LOCAL DEFAULT

GNU RELRO

```
GLOBAL DEFAULT 13 __libc_csu_fini
WEAK DEFAULT UND _ITM_deregisterTMCloneTab
WEAK DEFAULT 24 data_start
                            000000000000000000
                                                                                                      0 NOTYPE
0 NOTYPE
                 55: 0000000000602080
                 56:
                              00000000000000000
                                                                                                       0 FUNC
                                                                                                                                         GLOBAL DEFAULT UND puts@@GLIBC_2.2.5
                              00000000006020a0
                                                                                                       8 OBJECT
                                                                                                                                         GLOBAL DEFAULT
                 58:
                              00000000006020a8
                                                                                                       8 OBJECT
                                                                                                                                         GLOBAL DEFAULT
                 59:
                              00000000000602100
                                                                                                       0 NOTYPE
                                                                                                                                         GLOBAL DEFAULT
                                                                                                                                                                                                  24 edata
                 60:
                              00000000006020b8
                                                                                                       8 OBJECT
                                                                                                                                         GLOBAL DEFAULT
                                                                                                                                                                                                  24 p
14 _fini
                                                                                                                                                                                              14 _fini
UND strlen@@GLIBC_2.2.5
UND __stack_chk_fail@@GLIBC_2
24 f
                 61:
                              00000000000400c44
                                                                                                       0 FUNC
0 FUNC
                                                                                                                                         GLOBAL DEFAULT
                              00000000000000000
                                                                                                                                         GLOBAL DEFAULT
                 63:
                              00000000000000000
                                                                                                      0 FUNC
                                                                                                                                         GLOBAL DEFAULT
                              00000000006020b0
                                                                                                      8 OBJECT
                                                                                                                                        GLOBAL DEFAULT
                                                                                                                                                                                              UND printf@@GLIBC 2.2.5
                              00000000000000000
                                                                                               0 FUNC
167 FUNC
                                                                                                                                         GLOBAL DEFAULT
                                                                                                                                                                                              UND _libc_start_main@@GLIBC_
UND srand@@GLIBC_2.2.5
UND calloc@@GLIBC_2.2.5
                 66:
                              00000000004007fd
                                                                                                                                         GLOBAL DEFAULT
                              00000000000000000
                                                                                                     0 FUNC
0 FUNC
                                                                                                                                         GLOBAL DEFAULT
                 68:
                              00000000000000000
                                                                                                                                         GLOBAL DEFAULT
                 69:
                              00000000000000000
                                                                                                      0 FUNC
                                                                                                                                         GLOBAL DEFAULT
                                                                                                                                                              DEFAULT 24 __data_start

DEFAULT UND __gmon_start__

HIDDEN 24 __dso_handle

DEFAULT 15 _IO_stdin_used
                 70:
                              0000000000602080
                                                                                                      0 NOTYPE
                                                                                                                                        GLOBAL DEFAULT
                 71:
                              00000000000000000
                                                                                                     0 NOTYPE
                                                                                                                                        WEAK DEFAULT
GLOBAL HIDDEN
                 72:
                              0000000000602088
                                                                                                     0 OBJECT
4 OBJECT
                 73:
                              0000000000400c50
                                                                                                                                        GLOBAL DEFAULT
                 74:
                              00000000000000000
                                                                                               0 FUNC
101 FUNC
                                                                                                                                         GLOBAL DEFAULT UND time@@GLIBC_2.2.5
                                                                                                                                                                                                13 __libc_csu_init
25 _end
13 _start
                 75:
                              0000000000400bd0
                                                                                                                                         GLOBAL DEFAULT
                 76:
                              0000000000602110
                                                                                                    0 NOTYPE
0 FUNC
                                                                                                                                        GLOBAL DEFAULT
                 77:
                              0000000000400710
                                                                                                                                         GLOBAL DEFAULT
                                                                                                                                                                                                 13 base64_encode
24 o
24 s
                 78:
                              00000000004009a1
                                                                                               553 FUNC
                                                                                                                                         GLOBAL DEFAULT
                                                                                                8 OBJECT
8 OBJECT
0 NOTYPE
0 FUNC
32 FUNC
                 79:
                              00000000000602090
                                                                                                                                     GLOBAL DEFAULT 24 o
GLOBAL DEFAULT 25 _bs_start
GLOBAL DEFAULT 25 _bs_start
GLOBAL DEFAULT 13 main
MEAK DEFAULT 110 _Jv_RegisterClasses
GLOBAL DEFAULT UND _Jsce99 _scanf@@GLIBC_2.7
GLOBAL HIDDEN 24 _TMC_END _
MEAK DEFAULT UND _TMC_END _
GLOBAL DEFAULT 11 _init
GLOBAL DEFAULT 14 _init
GLOBAL DEFAULT 15 _more appearance of the company o
                                                                                                                                         GLOBAL DEFAULT
                 80:
                              0000000000602098
                              00000000000602100
                               00000000000000000
                               00000000004008a4
                                                                                           32 FUNC
0 NOTYPE
0 FUNC
0 OBJECT
0 NOTYPE
0 FUNC
221 FUNC
0 FUNC
                              00000000000000000
                 85:
                              00000000000000000
                              0000000000602110
                              00000000000000000
                 88:
                              0000000000400620
00000000004008c4
                 90:
                              00000000000000000
  008: 0 (*local*)
00c: 2 (GLIBC_2.2.5)
  Version needs section '.gnu.version_r' contains 1 entries:
Addr: 0x000000000000400438 Offset: 0x000438 Link: 6 (.dynstr)
0000000: 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 0x000000010 NT_GNU_ABI_TAG (ABI version tag)

OS: Linux, ABI: 2.6.24
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: f70ffbc08652e92fab24dc3a5leb0e386114eb3d
Dpate85ghrumil:-/dpate85/hw2/puzzles5 gbd 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:
<a href="http://www.gnu.org/software/gdb/bugs/s">http://www.gnu.org/software/gdb/bugs/s</a>.
Find the GDB manual and other documentation resources online at:
<a href="http://www.gnu.org/software/gdb/documentation/s">http://www.gnu.org/software/gdb/documentation/s</a>.
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
   (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
                            in gdb.c
 vguu) s
__srandom (x=1453577417) at random.c:210
210    random.c: No such file or directory.
(gdb) s
   (gdb) s
212
                            in random.c
   (gdb) s
  \(\frac{\guera}{2}\) \text{\frac{\guera}{2}} \text{\frac{\guera}{2}}} \text{\guera}} \text{\frac{\guera}{2}}} \text{\frac{\guera}{2}}} \text{\frac{\guera}{2}}} \text{
   (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
 102
(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
                            in random r.c
   (adb) s
                            in random r.c
   (gdb) s
                            in random r.c
   (gdb) s
                            in random_r.c
 198 in random_r.c
(gdb) s
199
 (gdb) s
189
                            in random r.c
```

53: 0000000000400c40

2 FUNC

```
(gdb) s
194 in random_r.c
(gdb) s
196 in random_r.c
 196
(gdb) s
195
(gdb) s
196
(gdb) s
198
(gdb) s
199
                        in random_r.c
                        in random_r.c
                        in random_r.c
                       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
196 in random_r.c
(gdb) s
198 in random_r.c
(gdb) s
                       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
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
196 in random_r.c
(gdb) s
196 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
199 in random_r.c
(gdb) s
190 in random_r.c
(gdb) s
190 in random_r.c
(gdb) s
191 in random_r.c
(gdb) s
192 in random_r.c
(gdb) s
193 in random_r.c
(gdb) s
194 in random_r.c
(gdb) s
195 in random_r.c
(gdb) s
196 in random_r.c
(gdb) s
197 in random_r.c
(gdb) s
198 in random_r.c
(gdb) s
199 in random_r.c
(gdb) s
190 in random_r.c
(gdb) s
191 in random_r.c
(gdb) s
192 in random_r.c
(gdb) s
193 in random_r.c
(gdb) s
194 in random_r.c
(gdb) s
195 in random_r.c
(gdb) s
196 in random_r.c
(gdb) s
197 in random_r.c
(gdb) s
198 in random_r.c
(gdb) s
199 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
195
(gdb) s
196
                        in random_r.c
 (gdb) s
198
                        in random_r.c
 198
(gdb) s
199
                        in random_r.c
 199
(gdb) s
189
                        in random r.c
169
(gdb) s
194
                        in random_r.c
(gdb) s
196
                        in random_r.c
196
(gdb) s
195
                        in random_r.c
 195
(gdb) s
196
(gdb) s
                        in random_r.c
```

```
198 in random_r.c
(gdb) s
199
  (gdb) s
             in random_r.c
  (gdb) s
194
             in random_r.c
  (gdb) s
             in random_r.c
  (gdb) s
             in random r.c
 195 _.
(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
 194 ...
(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
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
(gdd) n

Breakpoint 1, password () at gdb.c:17
17 in gdb.c
(gdd) n

18 in gdb.c
(gdd) n

19 in gdb.c
(gdd) n

20 in gdb.c
(gdd) n

behold! I will only tell you the secret password if you enter the random number I just generated!
21 in gdb.c
(gdd) n

5 -
(main=0x4008a4 <main>, argc=1, s21 libc-start.c: No such file or directory. (gdb) n [Inferior 1 (process 61933) exited with code 01] (gdb) n The program is not bair.
     uur ii
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
1 libc-start.c: No such file or directory.
 (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=0x7ffffffdea560 <_dl_fini>, stack_end=0x7ffffffe688) at libc_start.c:133
133 libc_start.c: No such file or directory.
 in libc-start.c No. 137 in libc-start.c (gdb) n 133
 133 in libc-start.c (gdb) n 137 *- -
 (gdb) n
219
             in libc-start.c
 (gdb) n
137
             in libc-start.c
 219 in libc-start.c (gdb) n 220 ---
 220 in libc-start.c (gdb) n 242
 242 in libc-start.c
(gdb) n
245 s- 1
245 in libc-start.c
(gdb) n
246
250 in libc-start.c (gdb) n
 265 in libc-start.c (gdb) n
 274 in libc-start.c (gdb) n
```

```
in libc-start.c
   (gdb) n
280
                     in libc-start.c
   (gdb) n
                     in libc-start.c
  281 ...
(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
  17 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!
  will or in gdb.c (gdb) n
  n
22
  22 in gdb.c
(gdb) n
27 in gdb.c
(gdb) n
   you lose :(
28 in
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 ()
  (guo) n
__libc_start_main (main=0x4008a4 <main>, argc=1, argv=0x7ffffffe678, 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) n
[Inferior 1 (process 61939) exited with code 01]
(gdb) quit

Dpate85@hrumil:~/dpate85/hw2/puzzles$ gdb
GNU gdb (Ubuntu 7.7.1-04ubuntu5-14.04.2) 7.7.1
Copyright (C 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying" and "show warranty" for details.
This GOB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<a href="http://www.gnu.org/software/gdb/bugs/">http://www.gnu.org/software/gdb/bugs/>
Find the GOB manual and other documentation resources online at:
<a href="http://www.gnu.org/software/gdb/documentation/">http://www.gnu.org/software/gdb/documentation/></a>
For help, type "help".
Type "apropos word" to search for commands related to "word".
(gdb) fight.
Reading symbols from 1...done.
(gdb) b 1
Breakpoint pending on future shared library load? (y or [n]) n
(gdb) b
Breakpoint 1 at 0x400805: file gdb.c, line 1.
(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
 ygun) 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
in gdb.c
(gdb) n
in gdb.c
(gdb) n
        uur) ii
Libc_start_main (main=0x4008a4 <main>, argc=1, argv=0x7fffffffe678, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7ffffffe668) at libc-start.c:321
1 libc_start.c: No such file or directory.
  321
  321 libc-start.c: No Such Fisc S. I. (gdb) n
[Inferior 1 (process 61957) exited with code 01]
 [Inferior 1 (process 61957) exited with code 01] (gdpt) in The program is not being run. (gdb) in main Starting program: /home/Opate85/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
 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!
  will o in gdb.c (gdb) n
  n
22
                    in gdb.c
  27 in gdb.c (gdb) n
  you lose :(
28 in qdb.c
```

```
(gdb) n
29 in gdb.c
  (gdb) n
   main () at gdb.c:35
  (dqp) u
                    in gdb.c
  (adb) n
      libc_start_main (main=0x4008a4 <main>, argc=2, argv=0x7fffffff668, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffff658) at libc-start.c:321
  [Inferior 1 (process 61967) exited with code 01]
  (gdb) Quit
(gdb) clear
 No breakpoint at this line.
  (adb) 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
0: 000000000000000000 0 NOTYPE LOCAL DEFAULT
1: 00000000000000000 0 FUNC GLOBAL DEFAULT
2: 00000000000000000 0 FUNC GLOBAL DEFAULT
                                                                                                                                               UND
UND curl_easy_init@CURL_GNUTLS_3 (2)
                                                                                                                                              UND curl_easy_init@CURL_GNUTLS_3 (2)
UND curl_easy_perform@CURL_GNUTLS_3 (2)
UND _JV_RegisterClasses
UND curl_easy_setopt@CURL_GNUTLS_3 (2)
UND _ITM_deregisterTMCloneTab
UND __libc_start_main@GLIBC_2.2.5 (3)
UND _mon_start_
UND _ITM_registerTMCloneTable
24 _edata
25 _end
11 _init
25 _bss_start
14 _fini
2: 000000000000000000 0 FUNC GLOBAL DEFAULT UND C
3: 00000000000000000 0 FUNC GLOBAL DEFAULT UND C
4: 0000000000000000 0 FUNC GLOBAL DEFAULT UND C
5: 0000000000000000 0 FUNC GLOBAL DEFAULT UND C
7: 000000000000000 0 FUNC GLOBAL DEFAULT UND C
8: 000000000000000 0 FUNC GLOBAL DEFAULT UND C
9: 000000000000000 0 FUNC GLOBAL DEFAULT UND C
10: 00000000000000 0 FUNC GLOBAL DEFAULT UND C
11: 00000000000602050 0 FUNC GLOBAL DEFAULT 25
11: 000000000000602050 0 FUNC GLOBAL DEFAULT 25
11: 000000000000000000 0 FUNC GLOBAL DEFAULT 25
13: 0000000000000000000 0 FUNC GLOBAL DEFAULT 15
13: 00000000000000000000 0 FUNC GLOBAL DEFAULT 14
Dpate85%0hrumil:-/dpate85/hw2/puz2less readelf 2
Usage: readelf 
    options are:

                                                              out the contents of ELF format files

Equivalent to: -h -l -S -s -r -d -V -A -I
Display the ELF file header
Display the program headers
An alias for --porgram-headers
Display the sections' header
An alias for -section-headers
Display the section groups
Display the section details
Equivalent to: -h -l -S
Display the symbol table
An alias for --syms
Display the dynamic symbol table
Display the dynamic section (if present)
Display the dynamic section (if present)
Display the dynamic section (if present)
Display the dynamic specific information (if any)
Display the symbol/file index in an archive
Use the dynamic section info when displaying symbols Inames
    Options are:
              --all
--file-header
       -l --program-headers
      --segments
-S --section-headers
                --sections
       -g --section-groups
-t --section-details
-e --headers
              --syms
          -dyn-syms
        -n --notes
-r --relocs
             --unwind
--dynamic
--version-info
--archive-index
--use-dynamic
     -c --archive-lndex Use the dynamic section into when user, -
-v --hex-dump=cnumber|name> Dump the contents of section <number|name> as bytes
-p --string-dump=cnumber|name> Dump the contents of section <number|name> as strings
-R --relocated-dump=cnumber|name> Dump the contents of section <number|name> as relocated bytes

Dump the contents of section <number|name> as relocated bytes
     EXEC (Executable file)
Advanced Micro Devices X86-64
0x1
0x400680
64 (bytes into file)
0x8
64 (bytes into file)
64 (bytes)
65 (bytes)
     64 (bytes)
28
   Section Headers
```

```
There are no section groups in this file.
     Program Headers:
  PHDR
  INTERP
  LOAD
  LOAD
  DYNAMIC
  GNU_EH_FRAME
  GNU STACK
  GNU_RELRO
 .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
.init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
          .dynamic
.note.ABI-tag .note.gnu.build-id
.eh_frame_hdr
.init_array .fini_array .jcr .dynamic .got
 RELA
0x400588
0x400570
24 (bytes)
24 (bytes)
0x400530
                                      0x400514
0x0
Relocation section '.rela.dyn' at offset 0x570 contains 1 entries:

Offset Info Type Sym. Value Sym. Name + Addend
00000601ff8 000700000006 R_X86_64_GLOB_DAT 00000000000000 __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:
 Histogram for `.gnu.hash' bucket list length (total of 3 buckets):
  Length Number
0 0
1 1
2 2
                % of total Coverage
( 0.0%)
( 33.3%) 20.0%
( 66.7%) 100.0%
 Version symbols section '.gnu.version' contains 14 entries:
Addr: 00000000000400514   Offset: 0x000514   Link: 5 (.dynsym)
```

```
004:
      008:
  Displaying notes found at file offset 0x00000254 with length 0x00000020:
                                   Data size
0x00000010
                                                                   Description
NT_GNU_ABI_TAG (ABI version tag)
      GNU
         05: Linux. ABI: 2.6.24
  Displaying notes found at file offset 0x00000274 with length 0x00000024:
         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
 GNU gdb (Ubuntu 7,7.1-aubuntu5-14.04.2) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<a href="http://www.gnu.org/software/gdb/bugs/s-">http://www.gnu.org/software/gdb/bugs/s-</a>
Find the GDB manual and other documentation resources online at:
<a href="http://www.gnu.org/software/gdb/documentation/">http://www.gnu.org/software/gdb/documentation/</a>
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) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
   (gdb) info registers
The program has no registers now.
   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
rbx
rcx
rdx
rsi
rdi
rbp
rsp
r10
r11
r12
r13
r14
r15
rip
eflags
cs
ss
ds
es
fs
                             0x0 0
0x7fffffffe688
0x7fffffffe678
                            # 0x6020a8 <r>
                                                                                                                        # 0x6020a0 <d>
                                                                                             _isoc99_scanf@plt>
                                                                                                                        # 0x602090 <n>
                                                                        # 0x6020b8 
# 0x602098 <s>
                                                                                                                        # 0x6020b0 <f>
  End of assembler dump.
(gdb) ni
18 in gdb.c
                in gdb.c
 tion password:

push %rbp

mov %rsp,%rbp

sub $0x10,%rsp

movl $0x0,%ex8(%rbp)

mov $0x0,%eddi

callq 0x4006d0 <time@plt>
                                                                       %eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
        0x0000000000040081d <+32>:
0x0000000000040081d <+32>:
0x00000000000400822 <+37>:
0x00000000000400825 <+40>:
                                                            callq
                                                            mov
mov
                                                                        %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                        # 0x6020a8 <r>
        0x0000000000040082c <+47>:
0x0000000000040082f <+50>:
                                                            mov %rax,%rdi
callq 0x400650 <puts@plt>
```

```
0x0000000000400835 <+62>:
0x00000000000400835 <+66>:
0x000000000000400842 <+69>:
0x000000000000400845 <+72>:
                                                                        -0x8(%rbp),%rdx
%rdx,%rsi
                                                                        %rax.%rdi
                                                             callo
              0x0000000000040084a <+77>:
                                                                        0x4006f0 <
                                                                                         __isoc99_scanf@plt>
                                                                        -0x8(%rbp),%eax
%eax,-0x4(%rbp)
              0x0000000000040084f <+82>:
              0x00000000000400852 <+85>:
              0x00000000000400855 <+88>:
0x00000000000400857 <+90>:
                                                                        0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                  # 0x602090 <o>
              0x000000000040085e <+97>:
0x00000000000400861 <+100>:
                                                             mov
callq
                                                                        %rax,%rdi
0x4008c4 <generate_password>
              0x00000000000400866 <+105>:
                                                             mov
                                                                        %rax.%rdx
                                                                        %rax,%rux
0x201848(%rip).%rcx
              0x00000000000400869 <+108>:
                                                                                                                   # 0x6020b8 
# 0x602098 <s>
              0x00000000000400870 <+115>:
                                                                        0x201821(%rip).%rax
              0x00000000000400877 <+122>:
                                                                        %rcx.%rsi
              0x0000000000040087a <+125>:
                                                                        %rax.%rdi
              0x0000000000040087d <+128>:
                                                                        $0x0.%eax
                                                                        0x400680 <printf@plt>
              0x00000000000400882 <+133>:
                                                             calla
              0x00000000000400887 <+138>:
                                                                        $0x1.%eax
             0x0000000000088/ <+1;38:
0x000000000040088c <+143:
0x000000000040088c <+145:
0x000000000400895 <+152:
0x0000000000400893 <+156:
0x000000000400883 <+165:
0x00000000400833 <+166:
                                                                       0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                             jmp
mov
                                                                                                                  # 0x6020b0 <f>
                                                                       %rax,%rdi
0x400650 <puts@plt>
callq
                                                                        $0x0,%eax
                                                             leaveg
                                                                                                                  # 0x6020a8 <r>
                                                                                                                  # 0x6020a0 <d>
                                                                                         _isoc99_scanf@plt>
                                                                       %rax,%rdi
0x4008c4 <generate_password>
%rax,%rdx
0x201848(%rip),%rcx #
0x201821(%rip),%rax #
                                                                                                                  # 0x6020b0 <f>
                                                            # 0x6020a8 <r>
                                                                                                                  # 0x6020a0 <d>
                                                                                          _isoc99_scanf@plt>
                                                                                                                  # 0x602090 <n>
                                                                        0x2018321%:1p,,......
%rax,%rdi
0x4008c4 <generate_password>
                                                                                                                  # 0x6020b8 
# 0x602098 <s>
              0x00000000000000077 <+125>
              0x0000000000040087d <+128>:
                                                                        $0x0,%eax
0x400680 <printf@plt>
              0x0000000000040087 <+128>:
0x0000000000400887 <+138>:
0x0000000000040088C <+143>:
0x0000000000040088C <+145>:
                                                             mov
jmp
mov
mov
                                                                        $0x1.%eax
                                                                        $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                  # 0x6020b0 <f>
              0x00000000000400895 <+152>:
                                                                       %rax,%rdi
0x400650 <puts@plt>
              0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                             calla
                                                             mov
leaveq
                                                                        $0x0.%eax
         End of assembler dump. (gdb) ni
          0x00000000000400818
                                           18
                                                             in adb.c
         issword:

%rbp

%rsp,%rbp

$0x10,%rsp

$0x0,-0x8(%rbp)

$0x0,%edi

0x4006d0 <time@plt>
                                                                       %eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
              0x00000000000400816 <+25>:
0x00000000000400818 <+27>:
                                                             mov
callq
              0x000000000040081d <+32>:
0x0000000000040082d <+32>:
0x00000000000400822 <+37>:
0x00000000000400825 <+40>:
                                                             callo
                                                             mov
                                                                        %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                  # 0x6020a8 <r>
              0x0000000000040082c <+47>:
0x0000000000040082f <+50>:
                                                             mov %rax,%rdi
callq 0x400650 <puts@plt>
```

0x00000000000400834 <+55>:

0x201865(%rip).%rax

# 0x6020a0 <d>

```
0x00000000000400834 <+55>:
                                                                 0x201865(%rip).%rax
                                                                                                        # 0x6020a0 <d>
            0x0000000000400835 <+62>:
0x00000000000400835 <+66>:
0x000000000000400842 <+69>:
0x000000000000400845 <+72>:
                                                                 -0x8(%rbp),%rdx
%rdx,%rsi
                                                                 %rax.%rdi
                                                                 $0x0.%eax
                                                       callo
            0x0000000000040084a <+77>:
                                                                 0x4006f0 <
                                                                                 __isoc99_scanf@plt>
                                                                 -0x8(%rbp),%eax
%eax,-0x4(%rbp)
            0x0000000000040084f <+82>:
            0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                       # 0x602090 <o>
                                                                 %rax,%rdi
0x4008c4 <generate_password>
                                                       mov
callq
                                                       mov
                                                                 %rax.%rdx
                                                                 %rax,%rux
0x201848(%rip).%rcx
                                                                                                        # 0x6020b8 
# 0x602098 <s>
            0x00000000000400870 <+115>:
                                                                 0x201821(%rip).%rax
            0x00000000000400877 <+122>:
                                                                 %rcx.%rsi
            0x0000000000040087a <+125>:
                                                                 %rax.%rdi
           0x0000000000000400873 <-1255:
0x0000000000000400874 <-1288:
0x0000000000004008872 <-1338:
0x000000000004008872 <-1338:
0x0000000000004008872 <-1345:
0x0000000000004008882 <-14455:
0x00000000000004008895 <-1555:
0x0000000000004008939 <-1555:
0x000000000004008939 <-1555:
0x0000000000004008939 <-1565:
0x00000000000400833 <-1565:
0x00000000000400833 <-1565:
                                                                 $0x0.%eax
                                                       calla
                                                                 0x400680 <printf@plt>
                                                       mov
                                                                 $0x1.%eax
                                                                0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                       jmp
mov
                                                                                                        # 0x6020b0 <f>
                                                       mov
callq
                                                                %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                       leaveg
       End of assembler dump.
                                                                                                        # 0x6020a8 <r>
                                                                                                        # 0x6020a0 <d>
                                                                                 _isoc99_scanf@plt>
                                                                                                        # 0x602090 <o>
                                                                %rax,%rdi
0x4008c4 <generate_password>
%rax,%rdx
0x201848(%rip),%rcx #
0x201821(%rip),%rax #
                                                                                                        # 0x6020b0 <f>
                                                      # 0x6020a8 <r>
                                                                                                        # 0x6020a0 <d>
                                                                                 _isoc99_scanf@plt>
                                                                                                        # 0x602090 <n>
                                                                 # 0x6020b8 
# 0x602098 <s>
                                                                0X201821(%rip),%rax
%rcx,%rsi
%rax,%rdi
$0x0,%eax
0x400680 <printf@plt>
                                                      mov
jmp
mov
mov
                                                                 $0x1.%eax
                                                                 $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                        # 0x6020b0 <f>
                                                                %rax,%rdi
0x400650 <puts@plt>
                                                      callq
                                                      mov
leaveq
                                                                $0x0.%eax
       in gdb.c
       (gdb) disas
Dump of assembler code for function password:
           %rbp
%rsp,%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                     push
mov
sub
movl
                                                      mov $0x0,%edi
callq 0x4006d0 <time@plt>
```

%eax,%edi

```
0x00000000000400818 <+27>:
                                                                                                                     0x4006a0 <srand@plt>
0x400700 <rand@plt>
             0x0000000000400818 <+2/>
0x0000000000040081d <+2/>
0x000000000000000822 <+37>
0x0000000000000400825 <+40>
0x00000000000040082c <+47>
0x00000000000040082f <+50>:
                                                                                                  callo
                                                                                                                       %eax.-0x4(%rbp)
                                                                                                                       0x20187c(%rip),%rax
                                                                                                                                                                                                   # 0x6020a8 <r>
                                                                                                                     %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                  calla
               0x00000000000400834 <+55>:
                                                                                                  mov
lea
                                                                                                                                                                                                   # 0x6020a0 <d>
              0x000000000040083b <+62>:
0x0000000000040083f <+66>:
                                                                                                                       %rdx.%rsi
              0x00000000000400842 <+69>:
0x00000000000400845 <+72>:
                                                                                                                       %rax.%rdi
                                                                                                  mov
callq
                                                                                                                       $0x0.%eax
              0x0000000000040084a <+77>:
0x00000000000040084f <+82>:
                                                                                                                      0x4006f0 <__isoc99_scanf@plt>
                                                                                                                       -0x8(%rbp),%eax
%eax,-0x4(%rbp)
              0x0000000000400852 <+85>:
0x00000000000400855 <+88>:
0x000000000000400857 <+90>:
                                                                                                  cmp
jne
                                                                                                                       0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                   # 0x602090 <o>
              0x0000000000400857 <-+90>:
0x0000000000400855 <-+97>:
0x00000000000400861 <-100>:
0x00000000000400866 <-105>:
0x00000000000400869 <+108>:
0x00000000000400870 <-115>:
0x00000000000400877 <-122>:
                                                                                                                      %rax,%rdi
0x4008c4 <generate_password>
                                                                                                  calla
                                                                                                  mov
                                                                                                                       %rax.%rdx
                                                                                                  mov
                                                                                                                       0x201848(%rip).%rcx
                                                                                                                                                                                                     # 0x6020b8 
# 0x602098 <s>
                                                                                                  mov
                                                                                                                       0x201821(%rip),%rax
                                                                                                  mov
                                                                                                                       %rcx,%rsi
              0x0000000000040087a <+125>:
0x0000000000040087d <+128>:
0x00000000000400882 <+133>:
                                                                                                  mov
                                                                                                                       %rax,%rdi
                                                                                                                      $0x0,%eax
0x400680 <printf@plt>
                                                                                                  callq
              0x00000000400882 <+1;338:
0x000000000400887 <+1;38:
0x00000000000400880 <+1;45:
0x0000000000400880 <+1;55:
0x00000000000400895 <+1;55:
0x00000000000400893 <+1;55:
0x0000000000400833 <+1;55:
0x000000000000400833 <+1;55:
                                                                                                  mov
                                                                                                                       $0x1,%eax
                                                                                                                      0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                  jmp
mov
                                                                                                                                                                                                   # 0x6020b0 <f>
                                                                                                                     %rax,%rdi
0x400650 <puts@plt>
                                                                                                  callq
                                                                                                  mov
leaveq
                                                                                                                      $0x0,%eax
      End of assembler dump.
       (gdb) ni
0x0000000000040082c
                                                                 20
                                                                                                  in qdb.c
       (gdb) ni
0x0000000000040082f 20
                                                                                                 in qdb.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
ssword:
%rtp
%rsp,%rtp
$6x10,%rsp
$6x0,-0x8(%rbp)
$6x0,%edi
0x400660 <time@plt>
%eax,%edi
0x400700 <rand@plt>
%eax,0x4(%rbp)
0x20187c(%rip),%rax
%rax,%rdi
%rax,%rax
                                                                                                                                                                                                   # 0x6020a8 <r>
                                                                                                                     %x20167C(%1p),%rdx
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
%rax,%rdi
%nax,%rdi
                                                                                                                                                                                                   # 0x6020a0 <d>
                                                                                                                     #rax, %rax

                                                                                                                                                                                                   # 0x602090 <o>
                                                                                                                                                                                                   # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                   # 0x6020b0 <f>
                                                                                                                     %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
    # 0x6020a8 <r>
                                                                                                                                                                                                   # 0x6020a0 <d>
                                                                                                                                                       isoc99 scanf@plt>
                                                                                                                      0X4000T0 <___1S0C99_SCAN1
-0X8(%rbp),%eax
%eax,-0X4(%rbp)
0X40088e <password+145>
0X201832(%rip),%rax
                                                                                                                                                                                                   # 0x602090 <o>
                                                                                                                      %rax,%rdi
0x4008c4 <generate_password>
                                                                                                  mov
mov
mov
mov
mov
                                                                                                                                                                                                    # 0x6020b8 
# 0x602098 <s>
              0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                                                       0x201821(%rip),%rax
                                                                                                                       %rcx,%rsi
%rax,%rdi
              0x0000000000040087a <+125>:
              0x0000000000040087d <+128>:
                                                                                                                      $0x0,%eax
0x400680 <printf@plt>
                                                                                                  calla
              0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                  mov
jmp
mov
                                                                                                                       $0x1.%eax
                                                                                                                      0x4008a2 <password+165>
0x20181b(%rip),%rax
               0x0000000000040088c <+143>:
               0x000000000040088e
                                                                     <+145>:
                                                                                                                                                                                                   # 0x6020b0 <f>
               0x00000000000400895 <+152>:
                                                                                                                     %rax,%rdi
0x400650 <puts@plt>
                                                                                                  calla
               0x00000000000400898 <+155>:
              0x0000000000440896 <+155>.
0x0000000000044089d <+160>:
0x00000000000440882 <+165>:
0x00000000000440883 <+166>:
                                                                                                                      $0x0.%eax
                                                                                                  leaved
     End of assembler dump. (gdb) ni
0x0000000000040083f
                                                                  21
                                                                                                  in adb.c
      (gdb) disas
Dump of assembler code for function password:
              0x000000000004007fd <+0>:
0x000000000004007fe <+1>:
                                                                                                              %rbp
%rsp,%rbp
```

```
0x00000000000400801 <+4>:
                                                                                                                 $0x10.%rsp
             0x0000000000400801 <+4>:
0x0000000000400805 <+8>:
0x00000000000040080c <+15>:
0x000000000000400811 <+20>:
0x00000000000400811 <+25>:
0x00000000000400813 <+27>:
0x00000000000400814 <+32>:
                                                                                                                 $0x0,-0x8(%rbp)
$0x0,%edi
                                                                                              movl
                                                                                              callq
                                                                                                                 0x4006d0 <time@plt>
                                                                                                                 %eax.%edi
                                                                                              calla
                                                                                                                 0x4006a0 <srand@plt>
0x400700 <rand@plt>
           callo
                                                                                                                 %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                              mov
                                                                                                                                                                                          # 0x6020a8 <r>
                                                                                                                 %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                              callo
                                                                                              mov
lea
                                                                                                                                                                                          # 0x6020a0 <d>
                                                                                                                 %rdx.%rsi
                                                                                              mov
                                                                                                                 %rax.%rdi
                                                                                                                 $0x0.%eax
            isoc99 scanf@plt>
                                                                                              callo
                                                                                                                 0x4006f0 <
                                                                                                                 0x4000T0 <___1soc99_scant
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                              mov
                                                                                              cmp
jne
                                                                                                                                                                                          # 0x602090 <o>
                                                                                                                 %rax,%rdi
                                                                                                                 0x4008c4 <generate_password>
                                                                                              callq
                                                                                              mov
                                                                                                                 %rax,%rdx
0x201848(%rip),%rcx
                                                                                              mov
                                                                                                                                                                                           # 0x6020b8 
              0x0000000000400870 <+115>:
0x0000000000400877 <+122>:
                                                                                                                 0x201821(%rip),%rax
                                                                                                                                                                                          # 0x602098 <s>
                                                                                                                 %rcx,%rsi
              0x000000000040087a <+125>:
                                                                                                                 %rax,%rdi
                                                                                                                 $0x0,%eax
0x400680 <printf@plt>
              0x000000000040087d <+128>:
                                                                                              callq
              0x00000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                                 $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                             mov
jmp
mov
              0x000000000400887 <+1385:
0x000000000400886 <+1435:
0x000000000400886 <+1455:
0x000000000400898 <+1555:
0x0000000000400898 <+1555:
0x0000000000400893 <+1655:
0x000000000400833 <+1665:
0x000000000400833 <+1665:
                                                                                                                                                                                          # 0x6020b0 <f>
                                                                                                                 %rax,%rdi
0x400650 <puts@plt>
                                                                                              callq
                                                                                              mov
leaveq
                                                                                                                 $0x0,%eax
End of assembler dump.
       (gdb) ni
0x0000000000400842 21
                                                                                              in qdb.c
                                                                                                              ssword:
%rtp
%rsp,%rtp
$6x10,%rsp
$6x0,-0x8(%rbp)
$6x0,%edi
0x400660 <time@plt>
%eax,%edi
0x400700 <rand@plt>
%eax,0x4(%rbp)
0x20187c(%rip),%rax
%rax,%rdi
%rax,%rax
                                                                                                              %eax,—0x4(%rbp)
%eax,—0x4(%rbp)
%20187C(%rip),%rax # 0
%rax,%rdi
%x400650 <puts@plt>
%x201865(%rip),%rax # 0
%x201865(%rip),%rax # 0
%x201865(%rip),%rax
%rdx,%rsi
%rax,%rdi
%x400676 <__isoc99_scanf@plt>
—0x3(%rbp),%eax
%eax,—0x4(%rbp)
%x400880 <password+145>
%x201832(%rip),%rax # 0
%x201821(%rip),%rax # 0
%x200820(%rip),%rax # 0
%x201821(%rip),%rax # 0
%x200820(%rip),%rax # 0
%x200820(%r
                                                                                                                                                                                          # 0x6020a8 <r>
                                                                                                                                                                                          # 0x6020a0 <d>
                                                                                                                                                                                          # 0x602090 <o>
                                                                                                                                                                                          # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                          # 0x6020b0 <f>
   # 0x6020a8 <r>
                                                                                                                                                                                          # 0x6020a0 <d>
                                                                                                                                                isoc99 scanf@plt>
                                                                                                                 0X4000T0 <___1S0C99_SCAN1
-0X8(%rbp),%eax
%eax,-0X4(%rbp)
0X40088e <password+145>
0X201832(%rip),%rax
                                                                                                                                                                                          # 0x602090 <o>
                                                                                                                 %rax,%rdi
0x4008c4 <generate_password>
                                                                                             mov
mov
mov
mov
mov
                                                                                                                                                                                           # 0x6020b8 
# 0x602098 <s>
              0x00000000000400870 <+115>:
                                                                                                                 0x201821(%rip),%rax
                                                                                                                %rcx,%rsi
%rax,%rdi
$0x0,%eax
0x400680 <printf@plt>
              0x00000000000400877 <+122>:
              0x0000000000040087a <+125>:
              0x0000000000040087d <+128>:
                                                                                              calla
              0x00000000000400882 <+133>:
                                                                                              mov
jmp
mov
              0x00000000000400887 <+138>:
                                                                                                                 $0x1.%eax
                                                                                                                 $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
              0x0000000000040088c <+143>:
              0x000000000040088e
                                                                  <+145>:
                                                                                                                                                                                          # 0x6020b0 <f>
              0x00000000000400895 <+152>:
                                                                                                                %rax,%rdi
0x400650 <puts@plt>
                                                                                              calla
              0x00000000000400898 <+155>:
              0x0000000000440896 <+155>.
0x0000000000044089d <+160>:
0x00000000000440882 <+165>:
0x00000000000440883 <+166>:
                                                                                                                 $0x0.%eax
                                                                                              leaved
     End of assembler dump.
(gdb) ni
0x0000000000040084a
                                                               21
                                                                                             in adb.c
      (gdb) disas
Dump of assembler code for function password:
              0x000000000004007fd <+0>:
0x000000000004007fe <+1>:
                                                                                                         %rbp
%rsp,%rbp
```

```
0x00000000000400801 <+4>:
                                                                                                                                     $0x10.%rsp
                 0x0000000000400801 <+4>:
0x0000000000400805 <+8>:
0x00000000000040080c <+15>:
0x000000000000400811 <+20>:
0x00000000000400811 <+25>:
0x00000000000400813 <+27>:
0x00000000000400814 <+32>:
                                                                                                                                    $0x0,-0x8(%rbp)
$0x0,%edi
                                                                                                              movl
                                                                                                              callq
                                                                                                                                     0x4006d0 <time@plt>
                                                                                                                                     %eax.%edi
                                                                                                              calla
                                                                                                                                    0x4006a0 srand@plt>
0x400700 <rand@plt>
                0x00000000040011 <-325-

0x000000000040822 <-475-

0x000000000408255 <-440-

0x00000000000408025 <-475-

0x0000000000000408027 <-500-

0x000000000000408023 <-555-

0x0000000000400033 <-555-

0x0000000000400033 <-656-

0x0000000000400040812 <-669-

0x0000000000400040815 <-775-

0x000000000000000040815 <-775-

0x0000000000000000040815 <-775-
                                                                                                                                    %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                        # 0x6020a8 <r>
                                                                                                                                    %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                              callo
                                                                                                              mov
lea
                                                                                                                                                                                                                        # 0x6020a0 <d>
                                                                                                                                     %rdx.%rsi
                                                                                                              mov
                                                                                                                                     %rax.%rdi
                                                                                                                                     $0x0.%eax
               isoc99 scanf@plt>
                                                                                                              callo
                                                                                                                                     0x4006f0 <
                                                                                                                                    0x4000T0 <___1soc99_scant
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                              mov
                                                                                                              cmp
jne
                                                                                                                                                                                                                        # 0x602090 <o>
                                                                                                                                     %rax,%rdi
                                                                                                                                     0x4008c4 <generate_password>
                                                                                                              callq
                                                                                                              mov
                                                                                                                                     %rax,%rdx
0x201848(%rip),%rcx
                                                                                                              mov
                                                                                                                                                                                                                         # 0x6020b8 
                  0x0000000000400870 <+115>:
0x0000000000400877 <+122>:
                                                                                                                                     0x201821(%rip),%rax
                                                                                                                                                                                                                        # 0x602098 <s>
                                                                                                                                     %rcx,%rsi
%rax,%rdi
                   0x000000000040087a <+125>:
                                                                                                                                    $0x0,%eax
0x400680 <printf@plt>
                 0x000000000400874 <-128:
0x00000000000400882 <-133:
0x000000000000400887 <-138:
0x00000000000000400886 <-145:
0x0000000000000400885 <-152:
0x0000000000000400898 <-152:
0x000000000004000989 <-152:
0x0000000000004000989 <-165:
0x000000000000400833 <-165:
0x0000000000000000033 <-166:
0x00000000000000000033 <-166:
                   0x000000000040087d <+128>:
                                                                                                              callq
                                                                                                                                    $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                              jmp
mov
                                                                                                                                                                                                                        # 0x6020b0 <f>
                                                                                                                                    %rax,%rdi
0x400650 <puts@plt>
                                                                                                              callq
                                                                                                              mov
leaveq
                                                                                                                                    $0x0,%eax
        End of assembler dump.
(gdb) ni
88
in qdb.c
                                                                                                                                # 0x6020a8 <r>
                                                                                                                                                                                                                        # 0x6020a0 <d>
                                                                                                                                                                                                                        # 0x602090 <o>
                                                                                                                                                                                                                        # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                        # 0x6020b0 <f>
      | In a same of the content of the co
                                                                                                                                                                                                                        # 0x6020a8 <r>
                                                                                                                                                                                                                        # 0x6020a0 <d>
                                                                                                                                                                       isoc99 scanf@plt>
                                                                                                                                                                                                                        # 0x602090 <o>
                                                                                                                                    %rax,%rdi
0x4008c4 <generate_password>
                                                                                                             mov
mov
mov
mov
mov
callq
                                                                                                                                                                                                                        # 0x6020b8 
# 0x602098 <s>
                  0x00000000000400870 <+115>:
                                                                                                                                     0x201821(%rip),%rax
                  0x00000000000400877 <+122>:
                                                                                                                                     %rcx,%rsi
%rax,%rdi
                  0x0000000000040087a <+125>:
                  0x0000000000040087d <+128>:
                                                                                                                                    $0x0,%eax
0x400680 <printf@plt>
                  0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                             mov
jmp
mov
                                                                                                                                     $0x1.%eax
                                                                                                                                    $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                  0x000000000040088c <+143>:
0x0000000000040088e <+145>:
                                                                                                                                                                                                                        # 0x6020b0 <f>
                   0x00000000000400895 <+152>:
                                                                                                                                   %rax,%rdi
0x400650 <puts@plt>
                  0x0000000000440893 <+152>:
0x00000000000440898 <+155>:
0x00000000000440894 <+160>:
0x0000000000440882 <+165>:
                                                                                                              callo
                                                                                                                                    $0x0.%eax
                                                                                                              mov
leaveq
                  0x0000000000004008a3 <+166>:
        exemple of assembler dump.

(gdb) i r eax'

Invalid register `eax''

(gdb) i r eax
       eax 0x58
(gdb) x/d 0x58
                                                                                   88
```

```
0x58: Cannot access memory at address 0x58 (gdb) x/d (0x58 - 0x4) 0x54: Cannot access memory at address 0x54 (gdb) ni
     (gdb) ni
0x00000000000400855 22
     (adb) disas
   (gdb) disas
Dump of assembler code for function password:
          push
mov
sub
                                                                                                                                         %rsp.%rbp
                                                                                                                                          $0x10,%rsp
$0x0,-0x8(%rbp)
                                                                                                                  movl
                                                                                                                                           $0x0,%edi
                                                                                                                  callq
                                                                                                                                         0x4006d0 <time@plt>
                                                                                                                  mov
callq
                                                                                                                                           %eax.%edi
                                                                                                                                         callo
                                                                                                                  mov
                                                                                                                                          %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                                    # 0x6020a8 <r>
                                                                                                                                         %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                  calla
                                                                                                                                                                                                                                     # 0x6020a0 <d>
                                                                                                                  mov
lea
                                                                                                                  mov
                                                                                                                                           %rdx,%rsi
                                                                                                                  mov
                                                                                                                                           %rax,%rdi
           $0x0,%eax
                                                                                                                                         0x4006f0 <_isoc99_scanf@plt>

-0x8(%rbp),%eax

%eax,-0x4(%rbp)

0x40088e <password+145>

0x201832(%rip),%rax # 6
                                                                                                                  callq
                                                                                                                 mov
cmp
jne
mov
                                                                                                                                                                                                                                    # 0x602090 <o>
                                                                                                                                          %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                  callq
                                                                                                                  mov
mov
                                                                                                                                          %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                                                                                                                                                     # 0x6020b8 
# 0x602098 <s>
                                                                                                                                           %rcx,%rsi
                                                                                                                  mov
                                                                                                                                           %rax,%rdi
                                                                                                                  mov
callq
                                                                                                                                          $0x0,%eax
0x400680 <printf@plt>
                                                                                                                 mov
jmp
mov
                                                                                                                                          $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                                                                                     # 0x6020b0 <f>
                                                                                                                                       %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                                                                                  mov
callq
                                                                                                                  mov
leaveq
  0x0000000000000000003 <+156>: 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)
0x7ffffffffe57c: 395572009
(qdb) ni
| Section | Sect
                                                                                                                                                                                                                                     # 0x6020a8 <r>
                                                                                                                                                                                                                                     # 0x6020a0 <d>
                                                                                                                                                                                                                                  # 0x602090 <n>
                                                                                                                                                                                                                                    # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                                     # 0x6020h0 <f>
   0x00000000004008as <+100
End of assembler dump.
(gdb) ni
0x0000000000400898 27
 in adb.c
                                                                                                                                       issword:

%rbp

%rsp,%rbp

$0x10,%rsp

$0x0,-0x8(%rbp)

$0x0,%edi

0x4006d0 <time@plt>
                                                                                                                                        0x400600 <time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                                 # 0x6020a8 <r>
                                                                                                                                         %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                                                                                                                     # 0x6020a0 <d>
                                                                                                                                           %rdx,%rsi
%rax,%rdi
                                                                                                                                           $0x0.%eax
                                                                                                                                         $0x0,%eax
0x4006f0 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax # 6
                                                                                                                 mov
cmp
jne
mov
               0x00000000000400855 <+88>:
0x00000000000400857 <+90>:
                                                                                                                                                                                                                                    # 0x602090 <o>
             0x000000000400457 <+90>:
0x0000000000400859 <+97>:
0x00000000000400861 <+100>:
0x000000000000400866 <+105>:
0x000000000000400869 <+105>:
0x00000000000400870 <+115>:
                                                                                                                                          %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                  callo
                                                                                                                                           %rax,%rux
0x201848(%rip),%rcx
                                                                                                                                                                                                                              # 0x6020b8 
# 0x602098 <s>
                                                                                                                                          0x201821(%rip),%rax
```

```
%rcx.%rsi
                                                                                   %rcx,%isi
%rax,%rdi
$0x0,%eax
0x400680 <printf@plt>
                                                                     callq
                                                                                    $0x1.%eax
                                                                                   0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                          # 0x6020b0 <f>
                                                                     mov
callq
                                                                                    %rax,%rdi
                                                                                   0x400650 <puts@plt>
                                                                     mov
leaveq
                                                                                   $0x0.%eax
   End of assembler dump.
   (adb) ni
   you lose :(
   28 in gdb.c
(gdb) quit
    A debugging session is active.
                  Inferior 1 [process 62019] will be killed.
  Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 1
 Dpate85@Dhrumil:~dpate85/hw2/puzzles$ gdb 1
GMU gdb (Ubuntu 7.7.1-@ubuntu5-14.04.2) 7.7.1
Copyright (c) 2014 Free Software Foundation, Inc.
License GPLv3+: GMU GPL version 3 or later <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying" and "show warranty" for details.
This GOB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<a href="http://www.gnu.org/software/gdb/bugs/>"http://www.gnu.org/software/gdb/bugs/>"find the GOB manual and other documentation resources online at:
<a href="http://www.gnu.org/software/gdb/documentation/">http://www.gnu.org/software/gdb/documentation/</a>
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) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
   (gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1
                                                                                 # 0x6020a8 <r>
                                                                                                                                          # 0x6020a0 <d>
                                                                                                                                          # 0x602090 <o>
                                                                                                                                          # 0x6020b8 
# 0x602098 <s>
                                                                                                                                          # 0x6020b0 <f>
                                                                                                                                          # 0x6020a8 <r>
        # 0x6020a0 <d>
                                                                                                          isoc99 scanf@plt>
                                                                                   0x4006f0 < __150099_360...

-0x8(%rbp),%eax

%eax,-0x4(%rbp)

0x40088e <password+145>

0x201832(%rip),%rax
                                                                     mov
cmp
jne
mov
mov
                                                                                                                                          # 0x602090 <o>
                                                                                   %rax,%rdi
0x4008c4 <generate_password>
                                                                     calla
                                                                    mov
mov
mov
mov
mov
                                                                                    %rax.%rdx
                                                                                    0x201848(%rip).%rcx
                                                                                                                                          # 0x6020b8 
# 0x602098 <s>
         0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                    0x201821(%rip),%rax
                                                                                    %rcx,%rsi
%rax,%rdi
         0x000000000040087a <+125>:
0x00000000000040087d <+128>:
0x00000000000400882 <+133>:
0x000000000000400887 <+138>:
                                                                                   $0x0,%eax
0x400680 <printf@plt>
                                                                     calla
                                                                     mov
jmp
mov
                                                                                    $0x1.%eax
                                                                                   0x4008a2 <password+165>
0x20181b(%rip),%rax
          0x0000000000040088c <+143>:
          0x0000000000040088e <+145>:
                                                                                                                                          # 0x6020b0 <f>
                                                                                 %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
          0x00000000000400895 <+152>:
          0×00000000000400898 <+155>:
                                                                     callq
         0x00000000004400896 <+155>:
0x00000000000440089d <+160>:
0x0000000000044008a2 <+165>:
0x0000000000044008a3 <+166>:
                                                                     leaved
  End of assembler dump.
   (gdb) ni
0x0000000000400811
                                                   18
                                                                    in qdb.c
```

```
(adb) disas
  %rbp
%rsp,%rbp
$0x10,%rsp
                                                      $0x0,-0x8(%rbp)
$0x0,%edi
     0x4006d0 <time@plt>
                                                      %eax.%edi
                                             calla
                                                      0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                             callo
                                                      %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                             mov
                                                                                         # 0x6020a8 <r>
                                                      %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                             callo
                                             mov
lea
                                                                                         # 0x6020a0 <d>
                                             mov
                                                      %rdx.%rsi
                                             mov
                                                      %rax.%rdi
                                                      $0x0.%eax
                                             callq
                                                      0x4006f0 <__isoc99_scanf@plt>
                                             mov
                                                      -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                             cmp
jne
                                                      0x40088e <password+145>
0x201832(%rip),%rax
                                                                                         # 0x602090 <o>
                                             mov
      0x0000000000400857 <+190>:
0x000000000000400856 <+197>:
0x000000000000400866 <+100>:
0x00000000000400866 <+1105>:
0x00000000000400869 <+108>:
0x00000000000400870 <+115>:
0x00000000000400877 <+112>:
                                                      %rax,%rdi
                                             callq
                                                      0x4008c4 <generate_password>
                                             mov
                                                      %rax,%rdx
                                                      0x201848(%rip),%rcx
                                             mov
                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                      0x201821(%rip),%rax
      mov
                                                      %rcx,%rsi
%rax,%rdi
                                             mov
                                                      $0x0,%eax
0x400680 <printf@plt>
                                             callq
                                                      $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                             mov
                                             jmp
mov
                                                                                         # 0x6020b0 <f>
                                                      %rax,%rdi
0x400650 <puts@plt>
                                             callq
                                             mov
leaveq
                                                      $0x0,%eax
 End of assembler dump.
   (gdb) ni
0x0000000000400816 18
                                             in qdb.c
                                                    # 0x6020a8 <r>
                                                                                          # 0x6020a0 <d>
                                                                                         # 0x602090 <o>
                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                         # 0x6020b0 <f>
# 0x6020a8 <r>
                                                                                         # 0x6020a0 <d>
      isoc99 scanf@plt>
                                             mov
cmp
jne
mov
mov
                                                      -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                      0x40088e <password+145>
0x201832(%rip),%rax
                                                                                         # 0x602090 <o>
                                                      %rax,%rdi
0x4008c4 <generate_password>
                                             callo
                                             mov
mov
mov
mov
mov
                                                      %rax.%rdx
                                                      %rax,%rux
0x201848(%rip).%rcx
                                                                                          # 0x6020b8 
# 0x602098 <s>
       0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                      0x201821(%rip),%rax
                                                      %rcx,%rsi
%rax,%rdi
       0x0000000000040087a <+125>:
       0x0000000000040087d <+128>:
                                                      $0x0.%eax
                                             calla
                                                      0x400680 <printf@plt>
       0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
                                             mov
jmp
mov
                                                      $0x1.%eax
                                                      0x4008a2 <password+165>
0x20181b(%rip),%rax
       0x0000000000040088c <+143>:
       0x0000000000040088e <+145>:
                                                                                         # 0x6020b0 <f>
       0x00000000000400895 <+152>:
                                                      %rax,%rdi
0x400650 <puts@plt>
      0x0000000000400898 <+155>:
0x0000000000040089d <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                             callo
                                                      $0x0.%eax
                                             leaven
  End of assembler dump.
(gdb) ni
19 in gdb.c
```

```
(adb) disas
 %rbp
%rsp,%rbp
$0x10,%rsp
                                                       $0x0,-0x8(%rbp)
$0x0,%edi
    0x4006d0 <time@plt>
                                                       %eax.%edi
                                             calla
                                                       0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                             callo
                                             mov
                                                       %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                           # 0x6020a8 <r>
                                                       %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                             callo
                                                                                           # 0x6020a0 <d>
                                             mov
lea
                                                       %rdx.%rsi
                                             mov
                                                       %rax.%rdi
                                                       $0x0.%eax
                                             callq
                                                       0x4006f0 <__isoc99_scanf@plt>
                                             mov
                                                       -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                             cmp
jne
                                                       0x40088e <password+145>
0x201832(%rip),%rax
                                                                                           # 0x602090 <o>
                                             mov
     0x0000000000400857 <+190>:
0x000000000000400856 <+197>:
0x000000000000400866 <+100>:
0x000000000000400866 <+1105>:
0x00000000000400869 <+108>:
0x00000000000400870 <+115>:
0x000000000000400877 <+112>:
                                                       %rax,%rdi
                                             callq
                                                       0x4008c4 <qenerate password>
                                             mov
mov
                                                       %rax,%rdx
                                                       0x201848(%rip),%rcx
                                                                                           # 0x6020b8 
# 0x602098 <s>
                                                       0x201821(%rip),%rax
     %rcx,%rsi
%rax,%rdi
                                             mov
                                                       $0x0,%eax
0x400680 <printf@plt>
                                             callq
                                                       $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                             mov
jmp
mov
                                                                                           # 0x6020b0 <f>
                                                       %rax,%rdi
0x400650 <puts@plt>
                                             callq
                                             mov
leaveq
                                                       $0x0,%eax
End of assembler dump.
  (gdb) ni
0x0000000000400822 19
                                             in qdb.c
                                                     # 0x6020a8 <r>
                                                                                            # 0x6020a0 <d>
                                                                                           # 0x602090 <o>
                                                                                           # 0x6020b8 
# 0x602098 <s>
                                                                                           # 0x6020b0 <f>
                                                                                           # 0x6020a8 <r>
                                                                                           # 0x6020a0 <d>
     isoc99 scanf@plt>
                                                       -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                             mov
cmp
jne
mov
mov
                                                       0x40088e <password+145>
0x201832(%rip),%rax
                                                                                           # 0x602090 <o>
                                                       %rax,%rdi
0x4008c4 <generate_password>
                                             callo
                                             mov
mov
mov
mov
mov
                                                       %rax.%rdx
                                                       %rax,%rux
0x201848(%rip).%rcx
                                                                                            # 0x6020b8 
# 0x602098 <s>
      0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                       0x201821(%rip),%rax
                                                       %rcx,%rsi
%rax,%rdi
      0x0000000000040087a <+125>:
      0x0000000000040087d <+128>:
                                                       $0x0,%eax
0x400680 <printf@plt>
                                             calla
      0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
                                             mov
jmp
mov
                                                       $0x1.%eax
                                                       $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
      0x0000000000040088c <+143>:
      0x000000000040088e
                               <+145>:
                                                                                           # 0x6020b0 <f>
                                                      %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
      0x00000000000400895 <+152>:
      0×00000000000400898 <+155>:
                                             callo
     0x00000000004400896 <+155>:
0x00000000000440089d <+160>:
0x0000000000044008a2 <+165>:
0x0000000000044008a3 <+166>:
                                             leaved
 End of assembler dump.
 (gdb) ni
0x000000000040082c
                                 20
                                             in qdb.c
```

```
%rbp
%rsp,%rbp
$0x10,%rsp
                                                              $0x0,-0x8(%rbp)
$0x0,%edi
     0x4006d0 <time@plt>
                                                               %eax.%edi
                                                    calla
                                                              0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                    callo
                                                               %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                       # 0x6020a8 <r>
                                                    mov
                                                              %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                    callo
                                                                                                       # 0x6020a0 <d>
                                                    mov
lea
                                                    mov
                                                               %rdx.%rsi
                                                    mov
                                                               %rax.%rdi
                                                               $0x0.%eax
                                                    callq
                                                              0x4006f0 <__isoc99_scanf@plt>
                                                    mov
                                                               -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                    cmp
jne
                                                               0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                       # 0x602090 <o>
                                                    mov
       0x0000000000400857 <+190>:
0x000000000000400856 <+197>:
0x000000000000400866 <+100>:
0x000000000000400866 <+1105>:
0x00000000000400869 <+108>:
0x00000000000400870 <+115>:
0x000000000000400877 <+112>:
                                                               %rax,%rdi
                                                    callq
                                                               0x4008c4 <generate_password>
                                                               %rax,%rdx
                                                               0x201848(%rip),%rcx
                                                    mov
                                                                                                       # 0x6020b8 
# 0x602098 <s>
                                                               0x201821(%rip),%rax
       %rcx,%rsi
%rax,%rdi
                                                    mov
                                                              $0x0,%eax
0x400680 <printf@plt>
                                                    callq
                                                              $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                    mov
                                                    jmp
mov
                                                                                                       # 0x6020b0 <f>
                                                              %rax,%rdi
0x400650 <puts@plt>
                                                    callq
                                                    mov
leaveq
                                                              $0x0,%eax
End of assembler dump.
   (gdb) ni
0x000000000040082f 20
                                                    mov
mov
mov
mov
mov
       0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                               %rcx,%rsi
%rax,%rdi
       0x0000000000040087a <+125>:
       0x000000000044087a <+125>:
0x0000000000044087d <+128>:
0x00000000000440882 <+133>:
0x00000000000440887 <+138>:
                                                              $0x0,%eax
0x400680 <printf@plt>
                                                    calla
                                                   mov
jmp
mov
                                                               $0x1.%eax
                                                              $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
       0x000000000040088c <+143>:
0x0000000000040088e <+145>:
                                                                                                       # 0x6020b0 <f>
       0X00000000400886 <+145>:
0X0000000000400898 <+155>:
0X00000000000400894 <+160>:
0X00000000000400894 <+165>:
0X00000000000400833 <+165>:
                                                              %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                    callo
                                                    leaved
  End of assembler dump. (qdb) ni
```

(adb) disas

```
(adb) ni
           0x0000000000040083f 21
                                                                                                                            in adb.c
           (gdb) disas
                | In the content of t
                          of assembler code for function password:
                                                                                                                                                      %rbp
%rsp,%rbp
                                                                                                                              sub
                                                                                                                                                       $0x10.%rsc
                                                                                                                               movl
                                                                                                                                                        $0x0,-0x8(%rbp)
                                                                                                                                                        $0x0,%edi
                                                                                                                                                      0x4006d0 <time@plt>
                                                                                                                              callq
                                                                                                                              mov
callq
                                                                                                                                                        %eax.%edi
                                                                                                                                                       0x4006a0 srand@plt>
0x400700 <rand@plt>
                                                                                                                              callo
                                                                                                                              mov
                                                                                                                                                        %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                              mov
                                                                                                                                                      %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                              calla
                                                                                                                                                                                                                                                       # 0x6020a0 <d>
                                                                                                                              mov
lea
                                                                                                                              mov
                                                                                                                                                        %rdx,%rsi
                                                                                                                              mov
                                                                                                                                                        %rax,%rdi
                                                                                                                              mov
callq
                                                                                                                                                        $0x0,%eax
                                                                                                                                                       0x4006f0 <__isoc99_scanf@plt>
                                                                                                                                                        -0x8(%rbp),%eax
                  0x000000000400841 <-822:
0x000000000400852 <-865:
0x000000000400855 <-888:
0x0000000000400855 <-977:
0x00000000000400856 <-195:
0x00000000000400856 <-105:
0x00000000000400856 <-105:
0x000000000004008576 <-1105:
0x00000000000400877 <-1125:
0x000000000000400877 <-1125:
                                                                                                                              mov
                                                                                                                              cmp
jne
                                                                                                                                                        %eax,-0x4(%rbp)
                                                                                                                                                       0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                                      # 0x602090 <o>
                                                                                                                                                        %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                              callq
                                                                                                                              mov
mov
                                                                                                                                                        %rax,%rdx
                                                                                                                                                        0x201848(%rip),%rcx
                                                                                                                                                                                                                                                        # 0x6020b8 
# 0x602098 <s>
                                                                                                                              mov
                                                                                                                                                        0x201821(%rip),%rax
                   mov
                                                                                                                                                        %rcx,%rsi
                                                                                                                              mov
                                                                                                                                                        %rax,%rdi
                                                                                                                                                        $0x0,%eax
0x400680 <printf@plt>
                                                                                                                              callq
                                                                                                                              mov
jmp
mov
                                                                                                                                                       $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                                                                                                       # 0x6020b0 <f>
                                                                                                                              mov
callq
                                                                                                                                                      %rax,%rdi
0x400650 <puts@plt>
                                                                                                                                                       $0x0,%eax
                                                                                                                              mov
leaveq
         End of assembler dump.
(gdb) ni
0x00000000000400842 21
in gdb.c
                                                                                                                                                   3ssword:
%rbp
%rsp,%rbp
$ssvord:
%rbp
%rsp,%rbp
$80x10,%rsp
$80x10,%rsp
$80x10,%rsp
$80x10,%rsp
$80x0,-0x8(%rbp)
$80x0,wedi
0x4006600 <ri>6xeax,%edi
0x4006600 <radeplt>
0x4007600 <radeplt>
0x20187C(%rip),%rax # 0
%rax,%rdi
0x201855(%rip),%rax # 0
%rax,%rdi
0x201865(%rip),%rax # 0
%rax,%rdi
$80x0,%eax
0x400676 <_isoc99_scanf@plt>
-0x8(%rbp),%eax
%rax,%rdi
$80x0,%eax
0x400676 <_isoc99_scanf@plt>
-0x8(%rbp),%eax
%rax,%rdi
$80x0,%eax
0x201848(%rip),%rax # 0
%rax,%rdi
%rax,%rdi
$80x0,%eax
0x201848(%rip),%rax # 0
%rxx,%rdi
$80x0,%eax
0x4006680 <pri>6xex0,%rdi
$80x0,%eax
0x400669 <pri>6xex0,%rdi
$80x0,%eax
0x4006680 <pri>6xex0,%rdi
$80x0,%eax
0x4006580 <pri>6xex0,%rdi
$80x0,%eax
0x4006580 <pri>6xex0,%rdi
$80x0,%eax
$80x0,%eax
$80x0,%eax
$80x0,%eax
$80x0,%eax
$80x0,%eax
                                                                                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                                                                                                                                                       # 0x6020a0 <d>
                                                                                                                                                                                                                                                      # 0x602090 <o>
                                                                                                                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                                                       # 0x6020h0 <f>
       assword:
%rbp
%rsp,%rbp
$0x0,%rsp
$0x0,%rsp
$0x0,%edi
$0x4006d0 etime@plt>
%eax,%edi
$0x4006d0 erand@plt>
%eax,%edi
$0x4006d0 erand@plt>
%eax,%edi
$0x4006d0 erand@plt>
%eax,%edi
$0x40050 erand@plt>
%eax,%edi
$0x20187c(%rip),%rax
%rax,%rdi
$0x201855(%rip),%rax
%rdi
$0x0,%rsi
%rax,%rdi
$0x0,%eax
                                                                                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                                                                                                                                                       # 0x6020a0 <d>
                                                                                                                                                      $000,%eax
0x4006f0 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax # #
                                                                                                                                                                                                                                                       # 0x602090 <o>
                                                                                                                                                       %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                              mov
mov
mov
mov
mov
                                                                                                                                                        %rax,%rdx
0x201848(%rip),%rcx
                                                                                                                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                     0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                                                                                        0x201821(%rip),%rax
                                                                                                                                                        %rcx,%rsi
%rax,%rdi
                     0x0000000000040087a <+125>:
                     0x0000000000040087d <+128>:
                                                                                                                                                        $0x0.%eax
                     0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                                              calla
                                                                                                                                                        0x400680 <printf@plt>
                                                                                                                                                        $0x1.%eax
                                                                                                                                                       0x4008a2 <password+165>
0x20181b(%rip),%rax
                     0x0000000000040088c <+143>:
0x0000000000040088e <+145>:
                                                                                                                              j mp
mov
                                                                                                                                                                                                                                                       # 0x6020h0 <f>
                    0x00000000004400886 <+145>:
0x0000000000004400895 <+152>:
0x0000000000004400898 <+155>:
0x00000000000440089d <+160>:
                                                                                                                                                      %rax,%rdi
0x400650 <puts@plt>
                                                                                                                              callo
                                                                                                                                                       $0x0.%eax
                    0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                                                                              leaveg
```

0x000000000040083b

21

in adb.c

```
(adb) ni
   0x0000000000040084a 21
                                                        in adb.c
   (adb) disas
      of assembler code for function password:
                                                                    %rbp
%rsp,%rbp
                                                                    $0x10,%rsp
                                                         sub
                                                                    $0x0,-0x8(%rbp)
$0x0,%edi
                                                         movl
                                                        callq
                                                                    0x4006d0 <time@plt>
                                                         mov
callq
                                                                     %eax.%edi
                                                                    0x4006a0 srand@plt>
0x400700 <rand@plt>
                                                         callo
                                                         mov
                                                                     %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                 # 0x6020a8 <r>
                                                         mov
                                                                    %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                         calla
                                                                                                                 # 0x6020a0 <d>
                                                         mov
lea
                                                         mov
                                                                     %rdx,%rsi
                                                         mov
                                                                     %rax,%rdi
                                                         mov
callq
                                                                     $0x0,%eax
      0x000000000040084a <+77>:
0x0000000000040084f <+82>:
                                                                    0x4006f0 <__isoc99_scanf@plt>
      0x000000000400841 <-822:
0x000000000400852 <-865:
0x000000000400855 <-888:
0x0000000000400855 <-977:
0x00000000000400856 <-195:
0x00000000000400856 <-105:
0x00000000000400856 <-105:
0x000000000004008576 <-1105:
0x00000000000400877 <-1125:
0x000000000000400877 <-1125:
                                                         mov
                                                                     -0x8(%rbp),%eax
                                                         cmp
jne
                                                                     %eax,-0x4(%rbp)
                                                                    0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                 # 0x602090 <o>
                                                                     %rax,%rdi
0x4008c4 <generate_password>
                                                         callq
                                                         mov
mov
                                                                     0x201848(%rip),%rcx
                                                                                                                  # 0x6020b8 
# 0x602098 <s>
                                                         mov
                                                                     0x201821(%rip),%rax
       mov
                                                                     %rcx,%rsi
                                                         mov
                                                                     %rax,%rdi
                                                                     $0x0,%eax
0x400680 <printf@plt>
                                                         callq
                                                        mov
jmp
mov
                                                                    $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                 # 0x6020b0 <f>
                                                         mov
callq
                                                                    %rax,%rdi
0x400650 <puts@plt>
                                                                    $0x0,%eax
                                                         mov
leaveq
End of assembler dump.
(gdb) ni
395572009
                                                                  # 0x6020a8 <r>
                                                                                                                  # 0x6020a0 <d>
                                                                                                                 # 0x602090 <o>
                                                                                                                 # 0x6020b8 
# 0x602098 <s>
                                                                                                                 # 0x6020h0 <f>
# 0x6020a8 <r>
                                                        mov
lea
mov
mov
mov
callq
                                                                                                                 # 0x6020a0 <d>
      0x00000000400034 <-55>
0x000000000400335 <-55>
0x000000000400335 <-65>
0x00000000000400337 <-65>
0x000000000000400837 <-75>
0x000000000000000400849 <-77>
0x0000000000000000400844 <-77>
0x0000000000000400855 <-85>
0x00000000000400055 <-85>
0x00000000000400055 <-85>
0x0000000000000000055 <-90>
                                                                    %rax,%rdi
$0x0,%eax
0x4006f0 <__isoc99_scanf@plt>
                                                         mov
cmp
jne
mov
mov
                                                                     -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                     0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                 # 0x602090 <o>
       0X0000000000400857 <+90>:

0X0000000000040085e <+97>:

0X000000000000400861 <+100>:

0X00000000000400866 <+105>:

0X00000000000400869 <+108>:
                                                                     %rax,%rdi
0x4008c4 <generate_password>
                                                         calla
                                                         mov
mov
mov
mov
mov
                                                                     %rax.%rdx
                                                                     %rax,%rux
0x201848(%rip).%rcx
                                                                                                                  # 0x6020b8 
# 0x602098 <s>
        0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                     0x201821(%rip).%rax
                                                                     %rcx,%rsi
%rax,%rdi
        0x0000000000040087a <+125>:
        0x000000000040087d <+128>:
0x00000000000400882 <+133>:
                                                                    $0x0,%eax
0x400680 <printf@plt>
                                                         calla
                                                         mov
jmp
mov
                                                                    $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
       0×000000000000400887 <+138>:
        0×00000000000040088c <+143>:
       0x0000000000040088c <+145>:
0x00000000000040088c <+145>:
0x000000000000400895 <+155>:
                                                                                                                 # 0x6020h0 <f>
                                                                   %rax,%rdi
0x400650 <puts@plt>
                                                         callo
       0x0000000000040089d <+160>:
0x000000000004008a2 <+165>:
                                                                    $0x0,%eax
```

leaveg

End of assembler dump.

```
End of assembler dump.
   (adb) ni
   0x00000000000400855
                                                    in adb.c
   (adb) disas
         of assembler code for function password:
      %rbp
%rsp,%rbp
$0x10,%rsp
                                                     sub
                                                                $0x0,-0x8(%rbp)
$0x0,%edi
                                                     movl
    calla
                                                                0x4006d0 <time@plt>
                                                                %eax.%edi
                                                     calla
                                                                0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                     callo
                                                     mov
                                                                %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                         # 0x6020a8 <r>
                                                     mov
                                                               %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                     callo
                                                     mov
lea
                                                                                                         # 0x6020a0 <d>
                                                     mov
                                                                %rdx,%rsi
                                                     mov
                                                                %rax,%rdi
                                                                $0x0,%eax
                                                     callq
                                                                0x4006f0 <__isoc99_scanf@plt>
                                                    mov
cmp
jne
                                                                -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                         # 0x602090 <o>
                                                                %rax,%rdi
0x4008c4 <generate_password>
                                                     callq
                                                     mov
mov
                                                                %rax,%rdx
0x201848(%rip),%rcx
                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                     mov
                                                                0x201821(%rip),%rax
                                                     mov
                                                                %rcx,%rsi
%rax,%rdi
                                                     mov
                                                     mov
callq
                                                                $0x0,%eax
0x400680 <printf@plt>
                                                                $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                     mov
                                                     jmp
mov
                                                                                                         # 0x6020b0 <f>
                                                     mov
callq
                                                               %rax,%rdi
0x400650 <puts@plt>
                                                                $0x0,%eax
                                                     mov
leaveq
End of assembler dump.
(gdb) ni
              in gdb.c
                                                              # 0x6020a8 <r>
                                                                                                         # 0x6020a0 <d>
                                                                                                         # 0x602090 <o>
                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                         # 0x6020h0 <f>
# 0x6020a8 <r>
                                                    mov
lea
mov
mov
mov
callq
                                                                                                         # 0x6020a0 <d>
      0x000000004008334 <-55>
0x00000000004008335 <-56>
0x00000000004008337 <-66>
0x0000000000004008347 <-66>
0x0000000000000400842 <-69>
0x0000000000000400844 <-77>
0x0000000000000400844 <-77>
0x000000000000400845 <-85>
0x000000000000400855 <-88>
0x00000000000400855 <-98>
0x00000000000400855 <-98>
0x000000000000400855 <-98>
0x00000000000400855 <-99>
                                                               %rax,%rdi
$0x0,%eax
0x4006f0 <__isoc99_scanf@plt>
                                                    mov
cmp
jne
mov
mov
                                                                -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                         # 0x602090 <o>
       0x000000000040085; <+97>:
0x00000000000400861 <+100>:
0x00000000000400866 <+105>:
0x00000000000400869 <+108>:
                                                                %rax,%rdi
0x4008c4 <generate_password>
                                                     calla
                                                    mov
mov
mov
mov
mov
                                                                %rax.%rdx
                                                                %rax,%rux
0x201848(%rip).%rcx
                                                                                                          # 0x6020b8 
# 0x602098 <s>
       0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                0x201821(%rip).%rax
                                                                %rcx,%rsi
%rax,%rdi
       0x0000000000040087a <+125>:
       0x000000000040087d <+128>:
0x00000000000400882 <+133>:
                                                                $0x0,%eax
0x400680 <printf@plt>
                                                     calla
                                                     mov
jmp
mov
                                                               $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
       0×00000000000400887 <+138>:
       0×00000000000040088c <+143>:
       0x0000000000040088c <+145>:
0x00000000000040088c <+145>:
0x000000000000400895 <+155>:
                                                                                                         # 0x6020h0 <f>
                                                               %rax,%rdi
0x400650 <puts@plt>
                                                     callo
       0x0000000000040089d <+160>:
0x000000000004008a2 <+165>:
                                                                $0x0,%eax
                                                     leaveg
```

0x000000000004008a3 <+166>: retq

```
End of assembler dump.
   (adb) ni
   0x00000000000400898 27
       (adb) disas
            of assembler code for function password:
                                                                                     %rbp
%rsp,%rbp
$0x10,%rsp
                                                                                     $0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                        movl
                                                                       callq
                                                                                       %eax.%edi
                                                                       calla
                                                                                     0x4006a0 srand@plt>
0x400700 <rand@plt>
                                                                       callo
                                                                                      %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                       mov
                                                                                                                                               # 0x6020a8 <r>
                                                                                     %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                       calla
                                                                       mov
lea
                                                                                                                                               # 0x6020a0 <d>
                                                                       mov
                                                                                       %rdx,%rsi
                                                                       mov
                                                                                       %rax,%rdi
                                                                       mov
callq
                                                                                       $0x0,%eax
                                                                                      0x4006f0 <__isoc99_scanf@plt>
                                                                       mov
                                                                                       -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                                      0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                               # 0x602090 <o>
                                                                                       %rax,%rdi
0x4008c4 <generate_password>
                                                                       callq
                                                                       mov
                                                                                       %rax,%rdx
0x201848(%rip),%rcx
                                                                       mov
                                                                                                                                               # 0x6020b8 
# 0x602098 <s>
                                                                                       0x201821(%rip),%rax
                                                                                       %rcx,%rsi
%rax,%rdi
                                                                       mov
                                                                       mov
callq
                                                                                      $0x0,%eax
0x400680 <printf@plt>
                                                                       mov
jmp
mov
                                                                                      $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                               # 0x6020b0 <f>
                                                                       mov
callq
                                                                                     %rax,%rdi
0x400650 <puts@plt>
                                                                                      $0x0,%eax
                                                                       mov
leaveq
   End of assembler dump.
  (gdb) ni
you lose :(
28 in
  you tose :(
28 in gdb.c
(gdb) quit
A debugging session is active.
                  Inferior 1 [process 62125] will be killed.
Inferior 1 [process 62125] will be killed.

Quit anyway? (y or n) y
ppate85ghrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (Ubuntu 7.7.1-8ubuntu5-14.04.2) 7.7.1
GNYI gdb (Ubuntu 7.7.1-8ubuntu5-14.04.2) 7.7.1
Copyright (C 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
This is free software: you are free to change and redistribute it.
There is NO WARRANITY, to the extent permitted by law. Type "show copying" and "show warranity" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<a href="http://www.gnu.org/software/gdb/bugs/-">http://www.gnu.org/software/gdb/bugs/-</a>
Find the GDB manual and other documentation resources online at:
<a href="http://www.gnu.org/software/gdb/documentation/">http://www.gnu.org/software/gdb/documentation/>
Type "apropos word" to search for commands related to "word"...
Reading symbols from 1...done.
(gdb) disas
No frame selected.
(gdb) b
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
# 0x6020a8 <r>
                                                                                                                                               # 0x6020a0 <d>
                                                                                                               _isoc99_scanf@plt>
                                                                                                                                               # 0x602090 <n>
                                                                                      %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                               # 0x6020b8 
# 0x602098 <s>
       mov
jmp
mov
                                                                                       $0x1.%eax
                                                                                      0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                               # 0x6020b0 <f>
                                                                                     %rax,%rdi
0x400650 <puts@plt>
                                                                       calla
                                                                                     $0x0.%eax
                                                                       mov
leaveq
  End of assembler dump.
   (gdb) ni
18
                   in gdb.c
  (gdb) disas
Dump of assembler code for function password:
       %rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                                      push
mov
sub
movl
                                                                       mov $0x0,%edi
callq 0x4006d0 <time@plt>
                                                                                      %eax,%edi
```

0x000000000004008a3 <+166>: retq

```
0x00000000000400818 <+27>:
                                                                                                                                                        0x4006a0 <srand@plt>
0x400700 <rand@plt>
                         0x000000000400818 <+2/>: 0x0000000000400814 <+2/>: 0x00000000000400822 <+37>: 0x000000000000400825 <+40>: 0x00000000000400825 <+47>: 0x000000000000400825 <+50>: <+50>:
                                                                                                                                                          %eax.-0x4(%rbp)
                                                                                                                                                          0x20187c(%rip),%rax
                                                                                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                                                        %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                 calla
                          0x00000000000400834 <+55>
                                                                                                                                 mov
lea
                                                                                                                                                                                                                                                       # 0x6020a0 <d>
                          0x000000000040083b <+62>:
0x000000000040083f <+66>:
                                                                                                                                                          %rdx.%rsi
                          0x00000000000400842 <+69>:
0x00000000000400845 <+72>:
                        0x0000000000400845 <-77>:
0x000000000040084a <-77>:
0x0000000000040084a <-77>:
0x00000000000400852 <-885>:
0x000000000000400857 <-882-:
0x000000000000400857 <-995>:
0x000000000000400856 <-997>:
0x000000000000400856 <-195>:
0x00000000000400856 <-1105>:
0x00000000000400856 <-1105>:
0x00000000000400873 <-125>:
0x0000000000000400877 <-1225>:
0x0000000000000400877 <-125>:
                                                                                                                                 mov
callq
                                                                                                                                                          $0x0.%eax
                                                                                                                                                        0x4006f0 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                                                                                                         0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                                      # 0x602090 <o>
                                                                                                                                                         %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                 calla
                                                                                                                                 mov
                                                                                                                                                          %rax.%rdx
                                                                                                                                 mov
                                                                                                                                                          0x201848(%rip).%rcx
                                                                                                                                                                                                                                                        # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                          0x201821(%rip),%rax
                                                                                                                                                          %rcx,%rsi
                          0x0000000000040087a <+125>:
0x0000000000040087d <+128>:
0x00000000000400882 <+133>:
                                                                                                                                 mov
                                                                                                                                                          %rax,%rdi
                                                                                                                                                          $0x0,%eax
                                                                                                                                 callq
                                                                                                                                                         0x400680 <printf@plt>
                         0x000000000400882 <+133>:
0x000000000400887 <+138>:
0x00000000000400886 <+143>:
0x0000000000400886 <+145>:
0x000000000400889 <+155>:
0x000000000400893 <+155>:
0x000000000400893 <+156>:
0x000000000400833 <+166>:
0x00000000000400833 <+166>:
0x000000000000400833 <+166>:
0x000000000000400833 <+166>:
                                                                                                                                                         $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                 mov
                                                                                                                                 jmp
mov
                                                                                                                                                                                                                                                       # 0x6020b0 <f>
                                                                                                                                                        %rax,%rdi
0x400650 <puts@plt>
                                                                                                                                 callq
                                                                                                                                 mov
leaveq
                                                                                                                                                         $0x0,%eax
## BASEMBLER | Jan | | Jan
                End of assembler dump.
                 (gdb) ni
0x00000000000400811 18
                                                                                                                                                       %rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                                                                        %eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                                                        %rax,%rsi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
                                                                                                                                                                                                                                                       # 0x6020a0 <d>
                                                                                                                                                          %rax,%rdi
                                                                                                                                                        %10x,%101
$0x0,%eax
0x4006f0 <__isoc99_scant
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
%raw %rdi
                                                                                                                                                                                                  _isoc99_scanf@plt>
                                                                                                                                                                                                                                                       # 0x602090 <o>
                                                                                                                                                      0x201832(%rip),%rax #
%rax,%rdi
0x4008c4 <generate_password>
%rax,%rdx
0x201848(%rip),%rcx #
0x201821(%rip),%rax #
%rcx,%rsi
5000,%eax
0x400630 cprintf@plt>
50x1,%eax
0x400630 cprintf@plt>
50x1,%eax
0x400630 cprintf@plt>
50x0,%rdi
50x0,%eax
0x400630 cprintf@plt>
50x0,%eax
                                                                                                                                                                                                                                                      # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                                                       # 0x6020b0 <f>
             # 0x6020a8 <r>
                                                                                                                                                                                                                                                       # 0x6020a0 <d>
                                                                                                                                                                                                  isoc99 scanf@plt>
                                                                                                                                                                                                                                                       # 0x602090 <n>
                                                                                                                                                         %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                mov
callq
mov
mov
mov
mov
mov
callq
                                                                                                                                                         %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                           0x00000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                                                                                          %rcx,%rsi
%rax,%rdi
                           0x0000000000040087a <+125>:
                           0x0000000000040087d <+128>:
                                                                                                                                                         $0x0,%eax
0x400680 <printf@plt>
                          0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
0x0000000000040088c <+143>:
0x0000000000040088e <+145>:
                                                                                                                                mov
jmp
mov
                                                                                                                                                          $0x1.%eax
                                                                                                                                                         $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                                                                                                       # 0x6020b0 <f>
                           0x00000000000400895 <+152>:
                                                                                                                                                        %rax,%rdi
0x400650 <puts@plt>
                          0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                                                                                 calla
                                                                                                                                                         $0x0.%eax
                                                                                                                                 leaved
                End of assembler dump.
                 (adb) ni
                (gdb) n1
0x00000000000400818 18
                                                                                                                                in adb.c
               %rbp
%rsp,%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
```

```
0x00000000000400811 <+20>:
                                                                                                                            callq
                                                                                                                                                 0x4006d0 <time@plt>
                           0x0000000000400811 <+20>:
0x00000000000400816 <+25>:
0x000000000000400818 <+27>:
0x000000000000400814 <+32>:
0x00000000000400822 <+37>:
0x00000000000400825 <+40>:
                                                                                                                                                  %eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                                            mov
callq
                                                                                                                                                    %eax.-0x4(%rbp)
                                                                                                                                                    0x20187c(%rip),%rax
                                                                                                                                                                                                                                          # 0x6020a8 <r>
                             0x0000000000040082c <+47>:
0x0000000000040082f <+50>:
0x00000000000400834 <+55>:
                                                                                                                                                   %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                            calla
                                                                                                                            mov
lea
                                                                                                                                                                                                                                          # 0x6020a0 <d>
                             0x00000000040083b <+62>:
0x0000000000040083f <+66>:
0x0000000000040084z <+66>:
0x0000000000040084z <+72>:
                                                                                                                            mov
mov
                                                                                                                                                    %rdx.%rsi
                                                                                                                                                    %rax.%rdi
                                                                                                                            mov
callq
                                                                                                                                                    $0x0.%eax
                            0x000000000400845 <+7/>
0x00000000000400846 <+77>:
0x0000000000040084f <+82>:
0x00000000000400852 <+85>:
0x00000000000400855 <+88>:
0x00000000000400857 <+90>:
                                                                                                                                                   0x4006f0 <__isoc99_scanf@plt>
                                                                                                                            mov
                                                                                                                                                    -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                                                                            cmp
jne
                                                                                                                                                    0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                          # 0x602090 <o>
                            0x000000000400857 <+90>:
0x0000000000400855 <+97>:
0x0000000000400856 <+97>:
0x000000000000006666 <+105>:
0x00000000000000000400859 <+105>:
0x000000000000000070 <+115>:
0x000000000000000070 <+115>:
0x0000000000000000070 <+125>:
0x000000000000000070 <+125>:
                                                                                                                                                    %rax.%rdi
                                                                                                                            calla
                                                                                                                                                    0x4008c4 <generate password>
                                                                                                                            mov
                                                                                                                                                    %rax,%rdx
                                                                                                                                                    0x201848(%rip),%rcx
                                                                                                                            mov
                                                                                                                                                                                                                                            # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                    0x201821(%rip),%rax
                                                                                                                                                    %rcx,%rsi
                                                                                                                            mov
                                                                                                                                                    %rax,%rdi
                           $0x0,%eax
0x400680 <printf@plt>
                                                                                                                            callq
                                                                                                                                                    $0x1,%eax
                                                                                                                                                   0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                            jmp
mov
                                                                                                                                                                                                                                          # 0x6020b0 <f>
                                                                                                                                                  %rax,%rdi
0x400650 <puts@plt>
                                                                                                                            callq
mov
leaveq
                                                                                                                                                   $0x0,%eax
                   End of assembler dump.
                                                                                                                                                                                                                                          # 0x6020a8 <r>
                                                                                                                                                                                                                                          # 0x6020a0 <d>
                                                                                                                                                                                         _isoc99_scanf@plt>
                                                                                                                                               0x70832\(\partial\) # # % rax,\(\partial\) # % rax\(\partial\) # % rax\(\partial\) # % rax\(\partial\) # % rax\(\partial\) # 0x20832\(\partial\) # rax\(\partial\) # rax\(\par
                                                                                                                                                                                                                                          # 0x602090 <o>
                                                                                                                                                                                                                                          # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                                          # 0x6020b0 <f>
                                                                                                                                                                                                                                          # 0x6020a8 <r>
                                                                                                                                                                                                                                          # 0x6020a0 <d>
                                                                                                                                                                                        _isoc99_scanf@plt>
                                                                                                                                                                                                                                          # 0x602090 <n>
                                                                                                                                                    %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                           mov
callq
mov
mov
mov
mov
mov
callq
                                                                                                                                                                                                                                           # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                    %rcx,%rsi
%rax,%rdi
                             0x0000000000040087a <+125>:
                            0x000000000044087a <-125>:
0x000000000044087d <+128>:
0x00000000000400882 <+133>:
0x0000000000400887 <+138>:
0x000000000040088c <+143>:
0x0000000000040088c <+145>:
                                                                                                                                                   $0x0,%eax
0x400680 <printf@plt>
                                                                                                                           mov
jmp
mov
                                                                                                                                                    $0x1.%eax
                                                                                                                                                   $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                                                                                          # 0x6020b0 <f>
                             0x00000000000400895 <+152>:
                                                                                                                                                  %rax,%rdi
0x400650 <puts@plt>
                             0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                                                                            calla
                                                                                                                            mov
leaveq
                                                                                                                                                   $0x0.%eax
                 426386943
                    (gdb) p/x rbp
No symbol "rbp" in current context.
                    (adh) ni
                                             in gdb.c
                   (qdb) disas
```

```
Dump of assembler code for function password:

0.08080808080804007fd <+0>: push
0.08080808080804007fe <+1>: mov
0.08080808080804007fe <+1>: mov
0.080808080808040807fe <+1>: mov
0.0808080808080408081 <+4>: su
0.0808080808080408081 <+1>: mov
0.0808080808080408081 <+2>: mov
0.0808080808080408081 <+2>: callq
0.0808080808080408081 <+2>: callq
0.0808080808080408081 <+2>: callq
0.08080808080808081 <+3>: callq
0.08080808080808081 <+3>: callq
0.08080808080808081 <+3>: callq
0.08080808080808081 <+3>: callq
0.080808080808081 <+3>: callq
0.080808080808081 <+3>: callq
0.080808080808081 <+3>: callq
0.080808080808081 <+3>: callq
0.0808080808080881 <+3>: callq
0.08080808080808081 <+3>: callq
0.0808080808080840835 <+4>: callq
0.0808080808080840835 <+6>: callq
0.080808080808080840835 <+6>: callq
0.08080808080808080840835 <+6>: callq
0.08080808080808080840835 <+60 : callq
0.080808080808080840835 <+6 : callq
0.08080808080808080840835 <+6 : callq
0.08080808080808080840835 <+6 : callq
0.080808080808080840835 <+6 : callq
0.080808080808080808485 <+6 : callq
0.0808080808080808485 <+6 : callq
0.08080808080808485 <+6 : callq
0.08080808080808485 <+6 : callq
0.080808080808485 <+6 : callq
0.080808080808485 <+6 : callq
0.080808080808485 <+6 : callq
0.0808080808485 <+6 : callq
0.080808080808485 <+6 : callq
0.0808080808485 <+6 : callq
0.0808080808485 <+6 : callq
0.080808080808485 <+6 : callq
0.0808080885 <+6 : callq
0.08080808
                                                                                                                         %rbp
%rsp,%rbp
                                                                                                                         $0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                                                                                         0x4006d0 <time@plt>
                                                                                                                          %eax.%edi
                                                                                                                         0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                                          %eax.-0x4(%rbp)
                                                                                                                          0x20187c(%rip),%rax
                                                                                                                                                                                                          # 0x6020a8 <r>
                                                                                                                         %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                                                                                          # 0x6020a0 <d>
                                                                                                                          %rdx.%rsi
                                                                                                                          %rax.%rdi
                                                                                                                          $0x0.%eax
            0x0000000000400845 <+//>
0x0000000000040084f <+82>:

0x00000000000040084f <+82>:

0x000000000000400855 <+85>:

0x00000000000400855 <+88>:

0x000000000000400857 <+90>:

0x000000000000400856 <+97>:
                                                                                                     calla
                                                                                                                         0x4006f0 <__isoc99_scanf@plt>
                                                                                                     mov
                                                                                                                          -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                                                     cmp
jne
                                                                                                                         0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                          # 0x602090 <o>
                                                                                                     mov
                                                                                                                          %rax,%rdi
            0x00000000000400861 <+100>:
0x00000000000400866 <+105>:
0x00000000000400869 <+108>:
                                                                                                     callq
                                                                                                                         0x4008c4 <generate_password>
                                                                                                                          %rax,%rdx
                                                                                                                          0x201848(%rip),%rcx
                                                                                                     mov
                                                                                                                                                                                                           # 0x6020b8 
# 0x602098 <s>
             0x00000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                                                          0x201821(%rip),%rax
                                                                                                     mov
                                                                                                                          %rcx,%rsi
             0x000000000040087a <+125>
                                                                                                     mov
                                                                                                                          %rax,%rdi
             0x000000000040087d <+128>:
                                                                                                                          $0x0,%eax
0x400680 <printf@plt>
            0x000000000400874 <-128:
0x00000000000400882 <-133:
0x000000000000400887 <-138:
0x00000000000000400886 <-145:
0x0000000000000400885 <-152:
0x0000000000000400898 <-152:
0x000000000004000989 <-152:
0x0000000000004000989 <-165:
0x000000000000400833 <-165:
0x0000000000000000033 <-166:
0x00000000000000000033 <-166:
                                                                                                     callq
                                                                                                                         0x400000 -p.1...

$0x1,%eax

0x4008a2 <password+165>

0x20181b(%rip),%rax
                                                                                                     mov
                                                                                                     jmp
mov
                                                                                                                                                                                                          # 0x6020b0 <f>
                                                                                                     mov
callq
                                                                                                                         %rax,%rdi
0x400650 <puts@plt>
                                                                                                                         $0x0,%eax
                                                                                                     leaveg
                                                                                                     retq
End of assembler dump. (gdb) ni
     0x0000000000040082c
                                                                                                     in qdb.c
                                                                                                                      # 0x6020a8 <r>
                                                                                                                                                                                                          # 0x6020a0 <d>
                                                                                                                                                                                                          # 0x602090 <o>
                                                                                                                                                                                                          # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                          # 0x6020b0 <f>
 ISSWORD:
%rbp
%rsp,%rbp
$0x10,%rsp
$0x10,%rsp
$0x0,0x8(%rbp)
$0x0,0x6d
0x400600 <time@plt>
%eax,%ed1
0x4006a0 <rand@plt>
%eax,0x4(%rbp)
$0x20187(%rip),%rax
%rax,%rdi
0x20187(%rip),%rax
%rax,%rdi
$0x20187(%rip),%rax
%rdi
$0x0,%eax
0x400676 <_iisoc99_scanf-
0x8(%rbp),%eax
%eax,0x4(%rbp)
0x40088e <password+145>
0x2018185(%rip),%rax
%rax,%rdi
$0x0,%eax
$0x400676 <_iisoc99_scanf-
0x8(%rbp),%eax
%rax,%rdi
$0x40088e <password+145>
0x201832(%rip),%rax
%rax,%rdi
$0x40064 <quentate passw
                                                                                                                                                                                                          # 0x6020a8 <r>
                                                                                                                                                                                                          # 0x6020a0 <d>
                                                                                                                                                            _isoc99_scanf@plt>
                                                                                                                                                                                                          # 0x602090 <o>
                                                                                                                         %rax,%rdi
0x4008c4 <generate_password>
                                                                                                     mov
mov
mov
mov
mov
                                                                                                                          %rax,%rdx
0x201848(%rip),%rcx
                                                                                                                                                                                                           # 0x6020b8 
# 0x602098 <s>
            0x00000000000400870 <+115>:
                                                                                                                          0x201821(%rip),%rax
            0x00000000000400877 <+122>:
                                                                                                                          %rcx,%rsi
%rax,%rdi
            0x0000000000040087a <+125>:
             0x0000000000040087d <+128>:
                                                                                                                          $0x0,%eax
0x400680 <printf@plt>
                                                                                                     calla
             0x00000000000400882 <+133>:
                                                                                                    mov
jmp
mov
             0x00000000000400887 <+138>:
                                                                                                                          $0x1,%eax
                                                                                                                         0x4008a2 <password+165>
0x20181b(%rip),%rax
             0x0000000000040088c <+143>:
             0x0000000000040088e <+145>:
                                                                                                                                                                                                          # 0x6020b0 <f>
             0x0000000000400895 <+152>:
0x00000000000400898 <+155>:
                                                                                                                         %rax,%rdi
0x400650 <puts@plt>
                                                                                                     calla
            0x0000000000440896 <+153>.
0x0000000000044089d <+160>:
0x00000000000440882 <+165>:
0x00000000000440883 <+166>:
                                                                                                                         $0x0,%eax
                                                                                                     leaved
   End of assembler dump.
    tiguo, il
behold! I will only tell you the secret password if you enter the random number I just generated!
21 in qdb.c
```

```
(adb) disas
   %rbp
%rsp,%rbp
$0x10,%rsp
                                                            $0x0,-0x8(%rbp)
$0x0,%edi
      0x4006d0 <time@plt>
                                                            %eax.%edi
                                                  calla
                                                            0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                  callo
                                                            %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                  mov
                                                                                                  # 0x6020a8 <r>
                                                            %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                  calla
                                                                                                  # 0x6020a0 <d>
                                                  mov
lea
                                                            %rdx.%rsi
                                                  mov
                                                            %rax.%rdi
                                                            $0x0.%eax
                                                  callq
                                                            0x4006f0 <__isoc99_scanf@plt>
                                                  mov
                                                            -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                  cmp
jne
                                                            0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                  # 0x602090 <o>
                                                  mov
        0x0000000000400857 <+190>:
0x000000000000400856 <+197>:
0x000000000000400866 <+100>:
0x000000000000400866 <+1105>:
0x00000000000400869 <+108>:
0x00000000000400870 <+115>:
0x000000000000400877 <+112>:
                                                            %rax,%rdi
                                                  callq
                                                            0x4008c4 <qenerate password>
                                                            %rax,%rdx
                                                            0x201848(%rip),%rcx
                                                  mov
                                                                                                  # 0x6020b8 
# 0x602098 <s>
                                                            0x201821(%rip),%rax
        %rcx,%rsi
%rax,%rdi
                                                            $0x0,%eax
0x400680 <printf@plt>
                                                  callq
                                                            $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                  mov
jmp
mov
                                                                                                  # 0x6020b0 <f>
                                                           %rax,%rdi
0x400650 <puts@plt>
                                                  callq
                                                  mov
leaveq
                                                            $0x0,%eax
ssword:
%rtp
%rsp,%rtp
$6x10,%rsp
$6x0,-0x8(%rbp)
$6x0,%edi
0x400660 <time@plt>
%eax,%edi
0x400700 <rand@plt>
%eax,0x4(%rbp)
0x20187c(%rip),%rax
%rax,%rdi
%rax,%rax
                                                           # 0x6020a8 <r>
                                                                                                  # 0x6020a0 <d>
                                                                                                  # 0x602090 <o>
                                                                                                  # 0x6020b8 
# 0x602098 <s>
                                                                                                  # 0x6020b0 <f>
   # 0x6020a8 <r>
                                                                                                  # 0x6020a0 <d>
                                                                            isoc99 scanf@plt>
                                                            0x4000T0 <___1soc99_scant
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                  # 0x602090 <o>
                                                            %rax,%rdi
0x4008c4 <generate_password>
                                                  mov
mov
mov
mov
mov
                                                                                                  # 0x6020b8 
# 0x602098 <s>
         0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                            0x201821(%rip),%rax
                                                            %rcx,%rsi
%rax,%rdi
         0x0000000000040087a <+125>:
         0x0000000000040087d <+128>:
                                                            $0x0,%eax
0x400680 <printf@plt>
         0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                  calla
                                                  mov
jmp
mov
                                                            $0x1.%eax
                                                            $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
         0x0000000000040088c <+143>:
                                                                                                  # 0x6020b0 <f>
         0x000000000040088e
                                   <+145>:
         0x00000000000400895 <+152>:
                                                           %rax,%rdi
0x400650 <puts@plt>
         0x0000000000400898 <+155>:
0x0000000000040089d <+160>:
                                                  calla
                                                            $0x0.%eax
        0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                  leaveq
retq
    End of assembler dump.
    (adh) ni
    0×00000000000040083f
                                  21
                                                 in adb.c
    (gdb) disas
Dump of assembler code for function password:
```

```
0x000000000004007fd <+0>:
                                                                                                                                                                                       %rbp
                                 0x0000000004007fd <+0>:
0x000000000004007fe <+1>:
0x00000000000400801 <+4>:
0x00000000000400805 <+8>:
0x0000000000040080c <+15>:
0x00000000000400811 <+20>:
                                                                                                                                                                                       %rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                                                                                                                            sub
                                                                                                                                                            mov
callq
                                                                                                                                                                                         0x4006d0 <time@plt>
                                  0x00000000000400816 <+25>
                                                                                                                                                                                          %eax.%edi
                                 %eax,%ed1
0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                                                                            callq
callq
                                                                                                                                                            mov
                                                                                                                                                                                          %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                                                                                                        # 0x6020a8 <r>
                                                                                                                                                                                         %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                                            callo
                                                                                                                                                                                                                                                                                                        # 0x6020a0 <d>
                                                                                                                                                            mov
lea
                                0x00000000040835 <+62>:
0x0000000000040835 <+66>:
0x00000000000400845 <+66>:
0x00000000000400842 <+69>:
0x00000000000400845 <+72>:
                                                                                                                                                                                          %rdx.%rsi
                                                                                                                                                            mov
                                                                                                                                                                                          %rax.%rdi
                                                                                                                                                                                          $0x0.%eax
                                 0x000000000040084a ++72-
0x0000000000040084f ++82-
0x00000000000040085f +885-
0x000000000000400855 ++885-
0x000000000000400857 +900-:
                                                                                                                                                            callo
                                                                                                                                                                                         0x4006f0 < isoc99 scanf@plt>
                                                                                                                                                                                         -0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                            mov
                                                                                                                                                            cmp
jne
                                                                                                                                                                                                                                                                                                        # 0x602090 <o>
                                 0x0000000000400857 <+1905:
0x000000000040085e <+9775:
0x000000000000400861 <+1005:
0x00000000000400866 <+1055:
0x00000000000400869 <+1085:
0x00000000000400870 <+11255:
0x000000000000400877 <+12255:
                                                                                                                                                                                          %rax,%rdi
                                                                                                                                                            callq
                                                                                                                                                                                          0x4008c4 <generate_password>
                                                                                                                                                            mov
                                                                                                                                                                                          %rax,%rdx
                                                                                                                                                                                          0x201848(%rip),%rcx
                                                                                                                                                                                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                          0x201821(%rip),%rax
                                                                                                                                                                                          %rcx,%rsi
%rax,%rdi
                                   0x000000000040087a <+125>:
                                   0x000000000040087d <+128>:
                                                                                                                                                                                          $0x0,%eax
0x400680 <printf@plt>
                                   0x00000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                                                                            callq
                                                                                                                                                           mov
jmp
mov
                                                                                                                                                                                         $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                  0x000000000400887 <+1385:
0x000000000400886 <+1435:
0x000000000400886 <+1455:
0x000000000400898 <+1555:
0x0000000000400898 <+1555:
0x0000000000400893 <+1655:
0x000000000400833 <+1665:
0x000000000400833 <+1665:
                                                                                                                                                                                                                                                                                                        # 0x6020b0 <f>
                                                                                                                                                                                       %rax,%rdi
0x400650 <puts@plt>
                                                                                                                                                            callq
                                                                                                                                                            mov
leaveq
                                                                                                                                                                                         $0x0,%eax
End of assembler dump.
(gdb) ni
0x00000000000400842
                                                                                                                                                            in qdb.c
                                                                                                                                                                                     ssword:
%rtp
%rsp,%rtp
$6x10,%rsp
$6x0,-0x8(%rbp)
$6x0,%edi
0x400660 <time@plt>
%eax,%edi
0x400700 <rand@plt>
%eax,0x4(%rbp)
0x20187c(%rip),%rax
%rax,%rdi
%rax,%rax
                                                                                                                                                                                     %eax,—0x4(%rbp)
%eax,—0x4(%rbp)
%prax,%rdi
%rax,%rdi
%x400650 <puts@plt>
%x20185(%rip),%rax # %
%x400650 <puts@plt>
%x201865(%rip),%rax # %
%rdx,%rsi
%rax,%rdi
%x400676 <__isoc99_scanf@plt>
-0x3(%rbp),%eax
%eax,—0x4(%rbp)
%x400868 <password+145>
%x201832(%rip),%rax # %
%rax,%rdi
%x400676 <puts@plt>
%x400676 <puts@plt>
%x400676 <puts@plt>
%x400676 <puts@plt>
%x400676 <puts@plt>
%x400688 <puts@plt>
%xx400688 <puts@plt>
%x
                                                                                                                                                                                                                                                                                                        # 0x6020a8 <r>
                                                                                                                                                                                                                                                                                                         # 0x6020a0 <d>
                                                                                                                                                                                                                                                                                                        # 0x602090 <o>
                                                                                                                                                                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                                                                                                        # 0x6020b0 <f>
                                                                                                                                                                                   assword:
%rhp
%rsp,%rbp
%rsp,%rbp
$9x0,-0x8(%rbp)
$9x0,-0x8(%rbp)
$9x0,-0x8(%rbp)
$9x0,-0x8(%rbp)
$9x0,-0x8(%rbp)
$0x0,-0x8(%rbp)
$0x409700 crand@plt>
%eax,-0x4(%rbp)
%eax,-0x4(%rbp)
%eax,-0x4(%rbp)
%rax,%rdi
$0x201855(%rip),%rax
%rdx,%rdi
$vx0,x,4rdi
$vx0,x,4rdi
$vx0,x,4rdi
$vx0,x,6rdi
$vx0,x
                                                                                                                                                                                                                                                                                                        # 0x6020a8 <r>
                                                                                                                                                                                                                                                                                                        # 0x6020a0 <d>
                                                                                                                                                                                                                                        isoc99 scanf@plt>
                                                                                                                                                                                         0X4000T0 <___1S0C99_SCAN1
-0X8(%rbp),%eax
%eax,-0X4(%rbp)
0X40088e <password+145>
0X201832(%rip),%rax
                                                                                                                                                                                                                                                                                                        # 0x602090 <o>
                                  0x000000000040085; <+97>:
0x00000000000400861 <+100>:
0x00000000000400866 <+105>:
0x00000000000400869 <+108>:
                                                                                                                                                                                         %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                                           mov
mov
mov
mov
mov
                                                                                                                                                                                          %rax.%rdx
                                                                                                                                                                                          %rax,%rux
0x201848(%rip).%rcx
                                                                                                                                                                                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                   0x0000000000400870 <+115>:
                                                                                                                                                                                          0x201821(%rip),%rax
                                   0x00000000000400877 <+122>:
                                                                                                                                                                                          %rcx,%rsi
%rax,%rdi
                                   0x0000000000040087a <+125>:
                                  0x0000000000040087d <+128>:
                                                                                                                                                                                         $0x0,%eax
0x400680 <printf@plt>
                                                                                                                                                            calla
                                   0x0000000000400882 <+133>:
                                                                                                                                                            mov
jmp
mov
                                   0x00000000000400887 <+138>:
                                                                                                                                                                                          $0x1.%eax
                                                                                                                                                                                         $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                   0x0000000000040088c <+143>:
                                   0x000000000040088e
                                                                                                                 <+145>:
                                                                                                                                                                                                                                                                                                        # 0x6020b0 <f>
                                   0x00000000000400895 <+152>:
                                                                                                                                                                                       %rax,%rdi
0x400650 <puts@plt>
                                                                                                                                                            calla
                                   0x00000000000400898 <+155>:
                                  0x0000000000440896 <+153>.
0x0000000000044089d <+160>:
0x00000000000440882 <+165>:
0x00000000000440883 <+166>:
                                                                                                                                                                                         $0x0.%eax
                                                                                                                                                            leaved
                     End of assembler dump. (gdb) ni
0x00000000000400845
                                                                                                             21
                                                                                                                                                           in adb.c
                      (gdb) disas
Dump of assembler code for function password:
                                  0x000000000004007fd <+0>:
0x000000000004007fe <+1>:
                                                                                                                                                                           n %rbp
%rsp,%rbp
```

```
0x00000000000400801 <+4>:
                                                                                                                          $0x10.%rsp
                                                                                                                         $0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                     movl
                                                                                                     callq
                                                                                                                           %eax.%edi
                                                                                                     calla
                                                                                                                          0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                     callo
                                                                                                                          %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                     mov
                                                                                                                                                                                                           # 0x6020a8 <r>
                                                                                                                          %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                     callo
                                                                                                                                                                                                          # 0x6020a0 <d>
                                                                                                     mov
lea
                                                                                                                           %rdx.%rsi
                                                                                                     mov
                                                                                                                           %rax.%rdi
                                                                                                                           $0x0.%eax
                                                                                                     calla
                                                                                                                          0x4006f0 < isoc99 scanf@plt>
                                                                                                                          0x4000T0 <___1soc99_scant
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                     mov
                                                                                                     cmp
jne
                                                                                                                                                                                                           # 0x602090 <o>
                                                                                                                           %rax,%rdi
                                                                                                                           0x4008c4 <generate_password>
                                                                                                     callq
                                                                                                     mov
                                                                                                                           %rax,%rdx
0x201848(%rip),%rcx
                                                                                                     mov
                                                                                                                                                                                                           # 0x6020b8 
                                                                                                                                                                                                           # 0x602098 <s>
             0x0000000000400870 <+115>:
0x0000000000400877 <+122>:
                                                                                                                           0x201821(%rip),%rax
                                                                                                                           %rcx,%rsi
%rax,%rdi
  0x0000000000040087a <+125>:
                                                                                                                          $0x0,%eax
0x400680 <printf@plt>
                                                                                                     callq
                                                                                                                          $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                    mov
jmp
mov
                                                                                                                                                                                                           # 0x6020b0 <f>
                                                                                                                         %rax,%rdi
0x400650 <puts@plt>
                                                                                                     callq
                                                                                                     mov
leaveq
                                                                                                                          $0x0,%eax
   (gdb) p/d $rax
$4 = 4197491
(gdb) p/d $rax
$4 = 4197491
(gdb) ni
0x00000000000040084a
                                                                    21
                                                                                                    in gdb.c
assword:
% rbp
% rsp,% rbp
% rsp,% rbp
$8x0, % rsp
$8x
                                                                                                                                                                                                           # 0x6020a8 <r>
                                                                                                                                                                                                           # 0x6020a0 <d>
                                                                                                                                                                                                           # 0x602090 <o>
                                                                                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                           # 0x6020h0 <f>
                                                                                                                        ssword:
%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                                        # 0x6020a8 <r>
                                                                                                                                                                                                           # 0x6020a0 <d>
                                                                                                                           %eax,-0x4(%rbp)
                                                                                                                          0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                          # 0x602090 <o>
                                                                                                                           %rax,%rdi
0x4008c4 <generate_password>
                                                                                                    mov
mov
mov
mov
                                                                                                                           0x201848(%rip),%rcx
             0x00000000000400869 <+108>:
                                                                                                                                                                                                           # 0x6020b8 
# 0x602098 <s>
             0x00000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                                                           0x201821(%rip),%rax
                                                                                                                           %rcx,%rsi
%rax,%rdi
             0x0000000000040087a <+125>:
0x0000000000040087d <+128>:
                                                                                                                           $0x0.%eax
             0x00000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                     callq
                                                                                                                         0x400680 <printf@plt>
$0x1,%eax
```

```
0x4008a2 <password+165>
0x20181b(%rip),%rax
            0x000000000040088c <+143>:
            0x000000000040088c <+143>:
0x000000000040088e <+145>:
0x0000000000400895 <+155>:
0x00000000000400898 <+155>:
0x00000000000400894 <+160>:
0x00000000000400832 <+166>:
0x00000000000400833 <+166>:
                                                                                                                        # 0x6020b0 <f>
                                                                         %rax,%rdi
0x400650 <puts@plt>
                                                              callq
                                                                          $0x0.%eax
                                                              leaved
       End of assembler dump.
        (odb) p/x $eax
(gdb) p/d $eax
       (adb) ni
        22 in gdb.c
(gdb) disas
                                                                                                                        # 0x6020a8 <r>
                                                                                                                        # 0x6020a0 <d>
                                                                                                                        # 0x602090 <o>
                                                                                                                        # 0x6020b8 
# 0x602098 <s>
                                                                                                                        # 0x6020b0 <f>
                                                                                                                        # 0x6020a8 <r>
                                                                                                                        # 0x6020a0 <d>
                                                                                                                        # 0x602090 <o>
                                                                                                                        # 0x6020b8 
# 0x602098 <s>
                                                                                                                        # 0x6020h0 <f>
       End of assembler dump. (gdb) p/d $eax $10 = 0
       $10 = 0
(gdb) p/x $eax
$11 = 0x0
(gdb) ni
        0x00000000000400855 22
                                                              in adb.c
        (gdb) disas
Dump of assembler code for function password:
           issword:

%rbp

%rsp,%rbp

$0x10,%rsp

$0x0,-0x8(%rbp)

$0x0,%edi

0x4006d0 <time@plt>
                                                              push
mov
sub
                                                              movl
mov
callq
                                                                         0x4006d0 <time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                              mov
callq
callq
                                                              mov
                                                                                                                        # 0x6020a8 <r>
                                                                          0x20187c(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
%rax,%rdi
                                                              calla
                                                              mov
lea
mov
mov
            0x00000000000400834 <+55>
                                                                                                                        # 0x6020a0 <d>
            0x0000000040083b <+62>:
0x000000000040083f <+66>:
0x0000000000040084z <+69>:
0x00000000000400845 <+72>:
            0x0000000000040084a <+77>:
0x00000000000040084f <+82>:
                                                              callq
                                                                          0x4006f0 <__iso
-0x8(%rbp),%eax
                                                                                              isoc99 scanf@plt>
```

```
0x00000000000400852 <+85>:
                                                                                                                                                                                             %eax.-0x4(%rbp)
                            0X000000000400855 <+85>:

0X0000000000400855 <+88>:

0X000000000000400857 <+90>:

0X0000000000040085e <+97>:

0X000000000000400861 <+100>:

0X00000000000400866 <+105>:
                                                                                                                                                                                            0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                                                                                               # 0x602090 <o>
                                                                                                                                                              callo
                                                                                                                                                                                             0x4008c4 <generate_password>
                                                                                                                                                                                             %rax.%rdx
                                                                                                                                                                                             0x201848(%rip).%rcx
                                0x00000000000400869 <+108>:
                                                                                                                                                                                                                                                                                                                 # 0x6020b8 
# 0x602098 <s>
                                0x00000000000400870 <+115>:
                                                                                                                                                                                             0x201821(%rip),%rax
                                0x00000000000400877 <+122>:
                                                                                                                                                                                             %rcx,%rsi
                                0x0000000000040087a <+125>:
                                                                                                                                                                                             %rax.%rdi
                                0x0000000000040087d <+128>:
                                                                                                                                                              mov
callq
                                                                                                                                                                                             $0x0.%eax
                                0x00000000000400882 <+133>:
                                                                                                                                                                                            0x400680 <printf@plt>
                                0x00000000000400887 <+138>:
                                                                                                                                                                                             $0x1.%eax
                                                                                                                                                                                            0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                              jmp
mov
                                0x0000000000040088c <+143>:
                               0x000000000040088c <+143>:
0x000000000040088e <+145>:
0x0000000000400895 <+155>:
0x00000000000400898 <+155>:
0x00000000000400894 <+160>:
0x00000000000400832 <+166>:
0x00000000000400833 <+166>:
                                                                                                                                                                                                                                                                                                               # 0x6020b0 <f>
                                                                                                                                                                                           %rax,%rdi
0x400650 <puts@plt>
                                                                                                                                                              calla
                                                                                                                                                              mov
leaveq
                                                                                                                                                                                            $0x0.%eax
                   End of assembler dump.
                  (gdb) p/x $eax
$12 = 0x0
(gdb) p/d $eax
$13 = 0
                  $13 = 0
(gdb) p/d ( $rbp - 0x4 )
$14 = 140737488348540
(gdb) p/x ( $rbp - 0x4 )
$15 = 0x7fffffffe57c
| Total | Tota
                   (gdb) p/d 0x7ffffffffe57c
$16 = 140737488348540
                                                                                                                                                                                           ssword:
%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                                                                                                           %cax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                                                                                                               # 0x6020a8 <r>
                                                                                                                                                                                           %x20167C(%1f),%fdx
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
%rax,%rdi
                                                                                                                                                                                                                                                                                                               # 0x6020a0 <d>
                                                                                                                                                                                           $0x0,%eax
0x4006f0 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                                                                                                                                             %eax,-0x4(%rup)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                                                                                               # 0x602090 <o>
                                                                                                                                                                                             %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                                                                             %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                                                                                                                                                                                                                               # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                           0x201021(%11),%1dx
%rcx,%rdi
%rax,%rdi
$0x0,%eax
0x400680 <printf@plt>
$0x1,%eax
0x400802 <password+165>
0x20181b(%rip),%rax
%rax.%rdi
%rax.%rdi
                                                                                                                                                                                                                                                                                                               # 0x6020b0 <f>
                                                                                                                                                                                           %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
              | Company | Comp
                                                                                                                                                                                                                                                                                                               # 0x6020a8 <r>
                                                                                                                                                                                                                                                                                                               # 0x6020a0 <d>
                                                                                                                                                                                                                                              _isoc99_scanf@plt>
                                                                                                                                                                                                                                                                                                               # 0x602090 <0>
                                                                                                                                                                                            0x2018321%:1p,,......
%rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                                                                                                                                                                                                 # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                           0X201821(%rip),%rax
%rcx,%rsi
%rax,%rdi
$0x0,%eax
0x400680 <printf@plt>
                                 0x00000000000400882 <+133>:
0x000000000000400887 <+138>:
                                                                                                                                                              calla
                                                                                                                                                              mov
jmp
mov
mov
                                                                                                                                                                                             $0x1.%eax
                                                                                                                                                                                            $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                               0x0000000000040088c <+143>:
0x0000000000040088e <+145>:
                                                                                                                                                                                                                                                                                                               # 0x6020b0 <f>
                                0x00000000000400895 <+152>:
                                                                                                                                                                                          %rax,%rdi
0x400650 <puts@plt>
                                0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                                                                                                              calla
                                                                                                                                                                                            $0x0.%eax
                                                                                                                                                              mov
leaveq
                   End of assembler dump.
                     (gdb) ni
0x0000000000400895 27
                                                                                                                                                             in adb.c
                  ssword:
%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                                                                                                                                                           0x4006d0 <time@plt>
                                                                                                                                                              callo
                                0x0000000000400811 <+20>:
0x00000000000400816 <+25>:
                                                                                                                                                                                           0x4006d0 <time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                              mov
callq
                               0x000000000400816 <+27>:
0x00000000000400818 <+27>:
0x0000000000000400814 <+32>:
0x00000000000400822 <+37>:
0x00000000000400825 <+40>:
0x0000000000040082c <+47>:
                                                                                                                                                              callo
                                                                                                                                                              mov
mov
mov
                                                                                                                                                                                                                                                                                                               # 0x6020a8 <r>
                                                                                                                                                                                             %rax,%rdi
```

```
0x000000000040082f <+50>:
0x00000000000400834 <+55>:
0x00000000000400835 <+62>:
0x000000000040083f <+66>:
0x0000000000400842 <+69>:
0x00000000000400845 <+72>:
                                                                                    0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                         callo
                                                                         mov
lea
                                                                                                                                         # 0x6020a0 <d>
                                                                                      %rdx.%rsi
                                                                                       %rax.%rdi
                                                                                      $0x0.%eax
                                                                         callo
                 0x000000000040084a <+77>:
0x0000000000040084f <+82>:
                                                                                      0x4006f0 <
                                                                                                           _isoc99_scanf@plt>
                                                                                      -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                         # 0x602090 <o>
                                                                         mov
callq
                                                                                      %rax,%rdi
0x4008c4 <generate_password>
                                                                                      %rax.%rdx
                                                                         mov
                                                                                      0x201848(%rip).%rcx
                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                 0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                      0x201821(%rip),%rax
                                                                                      %rcx.%rsi
                 0x0000000000040087a <+125>:
                                                                                      %rax.%rdi
               0X00000000040874 <-112>:
0X0000000000408874 <-128>:
0X0000000000408882 <+138>:
0X0000000000408887 <+138>:
0X00000000000400888 <+145>:
0X000000000000400888 <+145>:
0X00000000000408898 <+155>:
0X0000000000408899 <+155>:
                                                                                      $0x0.%eax
                                                                         calla
                                                                                      0x400680 <printf@plt>
                                                                         mov
                                                                                      $0x1,%eax
                                                                                      0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                         jmp
mov
                                                                                                                                         # 0x6020b0 <f>
                                                                                     %rax,%rdi
0x400650 <puts@plt>
callq
                 0x000000000040089d <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                         mov
leaveq
                                                                                     $0x0,%eax
                                                                                                                                         # 0x6020a8 <r>
                                                                                                                                         # 0x6020a0 <d>
                                                                                     $0x0,%eax
0x4006f0 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                                                                                         # 0x602090 <o>
                                                                                      %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                                                         # 0x6020b0 <f>
                                                                                                                                         # 0x6020a8 <r>
                                                                                                                                         # 0x6020a0 <d>
                                                                                                            _isoc99_scanf@plt>
                                                                                                                                         # 0x602090 <n>
                                                                                      # 0x6020b8 
# 0x602098 <s>
                9x909090000040874 <125>

9x909090000000040874 <125>

9x9090900000000408785 <133>

9x909090000000400882 <133>

9x909090000000400887 <143>

9x9090900000000400885 <155>

9x90900000000400885 <155>

9x909000000000400885 <155>

9x909000000000400883 <166>

9x90900000000400883 <1665>

9x909000000000400883 <1665>

9x9090000000000400883 <1665>
                                                                        mov
jmp
mov
                                                                                      0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                         # 0x6020b0 <f>
                                                                                     %rax,%rdi
0x400650 <puts@plt>
                                                                         calla
                                                                                     $0x0.%eax
                                                                         mov
leaveq
           End of assembler dump.
            (gdb) ni
29 i
                          in gdb.c
           ssword:
%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                0x000000000400805 <+85:

0x0000000000040080c <+15>:

0x000000000000400811 <+20>:

0x00000000000400816 <+27>:

0x00000000000400818 <+27>:

0x0000000000040081d <+32>:
                                                                         mov
callq
                                                                                     %eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                         mov
callq
                                                                         callo
                 0x00000000000400822 <+37>:
0x00000000000400825 <+40>:
                                                                                      %eax,-0x4(%rbp)
0x20187c(%rip),%rax
```

# 0x6020a8 <r>

```
%rax.%rdi
                                                                                                                                  0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                             callq
                                                                                                                                                                                                                           # 0x6020a0 <d>
                                                                                                                                    %rdx.%rsi
            0x0000000000400845 <-77>:
0x000000000040084a <-77>:
0x0000000000040084a <-77>:
0x00000000000400852 <-885>:
0x000000000000400857 <-882-:
0x000000000000400857 <-995>:
0x000000000000400856 <-997>:
0x000000000000400856 <-195>:
0x00000000000400856 <-1105>:
0x00000000000400856 <-1105>:
0x00000000000400873 <-125>:
0x0000000000000400877 <-1225>:
0x0000000000000400877 <-125>:
                                                                                                             mov
callq
                                                                                                                                    0x4006f0 <
                                                                                                                                                                       __isoc99_scanf@plt>
                                                                                                                                    -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                                                                                   0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                          # 0x602090 <o>
                                                                                                                                   %rax,%rdi
0x4008c4 <generate_password>
                                                                                                             mov
callq
                                                                                                                                    %rax.%rdx
                                                                                                                                    %rax,%rux
0x201848(%rip).%rcx
                                                                                                             mov
                                                                                                                                                                                                                           # 0x6020b8 
# 0x602098 <s>
                                                                                                                                    0x201821(%rip).%rax
                                                                                                                                    %rcx.%rsi
           0x0000000000400877 <-1225-
0x00000000000400873 <-1255-
0x00000000000400870 <-1285-
0x00000000000400882 <-1385-
0x00000000000400883 <-1385-
0x00000000000400883 <-1435-
0x00000000000400885 <-1435-
0x00000000000400885 <-1455-
0x000000000000400883 <-1655-
0x00000000000400883 <-1665-
0x00000000000400833 <-1665-
0x000000000000400833 <-1665-
0x00000000000400833 <-1665-
0x000000000000400833 <-1665-
0x000000000000400833 <-1665-
                                                                                                                                    %rax.%rdi
                                                                                                                                    $0x0.%eax
                                                                                                             callq
                                                                                                                                   0x400680 <printf@plt>
                                                                                                                                    $0x1,%eax
                                                                                                                                   0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                             jmp
mov
                                                                                                                                                                                                                           # 0x6020b0 <f>
                                                                                                                                    %rax,%rdi
                                                                                                                                  0x400650 <puts@plt>
                                                                                                             callq
                                                                                                                                   $0x0,%eax
                                                                                                             leaveg
End of assembler dump.
     0x000000000004008a3 29
                                                                                                             in qdb.c
                                                                                                                                 %rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                                                   %cax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                           # 0x6020a8 <r>
                                                                                                                                   %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                                                                                                           # 0x6020a0 <d>
                                                                                                                                    %rdx,%rsi
                                                                                                                                    %rax,%rdi
                                                                                                                                   %104,%101
$0x0,%eax
0x4006f0 <__isoc99_scan
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
%rax %rdif
                                                                                                                                                                        _isoc99_scanf@plt>
                                                                                                                                 0x201832(%rip),%rax #
%rax,%rdi
0x4008c4 <generate_password>
%rax,%rdi
0x201848(%rip),%rcx #
0x201821(%rip),%rax #
%rcx,%rdi
50%0,%eax
0x400630 cprintf@plt>
50%1,%eax
0x400630 cprintf@plt>
50%1,%eax
0x400630 cprintf@plt>
50%1,%eax
0x400630 cprintf@plt>
50%0,%eax
                                                                                                                                                                                                                           # 0x6020b0 <f>
                            Inferior 1 [process 62210] will be killed.
Inferior 1 [process 62210] will be killed.

Quit anyway? (y or n) y
ppate85@hrumi1:-/dpate85/hw2/puzzles5 gdb 1
GNU gdb (Ubuntu 7.7.1-0ubuntu5-14.04.2) 7.7.1
COpyright (C) 2914 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
License GPLv3+: GNU GPL version 3 or later <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
This is GB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<a href="http://www.gnu.org/software/gdb/bugs/>-find the GBD manual and other documentation resources online at:</a>
<a href="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) r
Fearking program: /home/Dnate85/dpate85/hw2/ouzzles/1</a>
   (gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/1
issword:
%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                                                 0x400600 ctime@plt>
weax, %edi
0x4006a0 crand@plt>
0x400700 crand@plt>
0x20187c(%rip), %rax
%rax, %rdi
0x400650 cputs@plt>
0x201865(%rip), %rax
-0x8(%rbp), %rdx
%rdx, %rsi
%rax, %rdi
50x0, %eax
0x4006f0 < isoc99 ss</pre>
                                                                                                                                                                                                                           # 0x6020a8 <r>
                                                                                                                                                                                                                           # 0x6020a0 <d>
             0x000000000040845 <+7/2:

0x00000000000400846 <+77>:

0x0000000000040084f <+82>:

0x00000000000400852 <+85>:

0x00000000000400855 <+88>:

0x000000000000400857 <+90>:
                                                                                                                                  $0x4006f0 <__isoc99_scant
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                             callo
                                                                                                                                                                         isoc99 scanf@plt>
                                                                                                            mov
cmp
jne
mov
                                                                                                                                                                                                                         # 0x602090 <o>
              0x0000000000040085e <+97>:
0x00000000000400861 <+100>:
                                                                                                                                 %rax,%rdi
0x4008c4 <qenerate password>
                                                                                                            callq
```

```
0x00000000000400866 <+105>:
             0x0000000000400869 <+103>:
0x00000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                                                              0x201848(%rip).%rcx
                                                                                                                                                                                                                    # 0x6020b8 
# 0x602098 <s>
                                                                                                                               0x201821(%rip),%rax
              0x0000000000040087a <+125>:
             0x0000000000040087d <+128>:
                                                                                                         callo
             0x00000000000400882 <+133>:
                                                                                                                               0x400680 <printf@plt>
                                                                                                        mov
jmp
mov
             0x00000000000400887 <+138>:
                                                                                                                               $0x1.%eax
            0x00000000400887 <+1385:
0x000000000400886 <+1435:
0x0000000000400886 <+1455:
0x00000000000400888 <+1555:
0x0000000000400889 <+1555:
0x000000000400889 <+1565:
0x00000000400883 <+1665:
0x000000000400883 <+1665:
                                                                                                                              0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                                                                  # 0x6020b0 <f>
                                                                                                                             %rax,%rdi
0x400650 <puts@plt>
                                                                                                         mov
callq
                                                                                                         mov
leaveq
                                                                                                                              $0x0.%eax
   End of assembler dump.
| The color of the
     (adb) ni
                            in gdb.c
     (gdb) disas
                                                                                                                              %rsp,%rbp
                                                                                                                               $0x10,%rsp
                                                                                                                               $0x0,-0x8(%rbp)
$0x0,%edi
                                                                                                                             0x4006d0 <time@plt>
                                                                                                                                %eax,%edi
                                                                                                                              0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                                               %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                  # 0x6020a8 <r>
                                                                                                                              %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                                                                                                  # 0x6020a0 <d>
                                                                                                                               %rdx,%rsi
                                                                                                                               %rax,%rdi
                                                                                                                               $0x0,%eax
0x4006f0 <
                                                                                                                                                                 isoc99 scanf@plt>
                                                                                                                              0x4006f0 <___1soc99_scant
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                  # 0x602090 <o>
                                                                                                                               %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                              %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                                                                                                                                  # 0x6020b8 
# 0x602098 <s>
                                                                                                                               %rcx,%rsi
%rax,%rdi
                                                                                                                              $0x0,%eax
0x400680 <printf@plt>
                                                                                                                              $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                                                                  # 0x6020b0 <f>
                                                                                                                             %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
# 0x6020a8 <r>
                                                                                                                                                                                                                   # 0x6020a0 <d>
                                                                                                                                                                                                                  # 0x602090 <o>
                                                                                                                                                                                                                  # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                  # 0x6020h0 <f>
                                                                                                                            wxzul81D(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                                                                         mov
leaved
              0x000000000004008a2 <+165>:
0x0000000000004008a3 <+166>:
   in adb.c
     (adb) ni
     0x00000000000400818
                                                                                                       in adb.c
     (gdb) ni
19 i
                            in gdb.c
     (adb) ni
     0x00000000000400822 19
                                                                                                       in adb.c
     (gdb) ni
20 i
                            in gdb.c
     (qdb) disas
  ssword:
%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                                            0x4006d0 <timeoplt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rrr>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
%rax,%rdi
0x400550 <puts@plt>
0x201805(%rip),%rax
-0x8(%rbp),%rax
           0x00000000000400818 <+27>:
0x000000000000400814 <+32>:
0x000000000000400822 <+37>:
0x000000000000400825 <+40>:
0x00000000000400825 <+47>:
0x000000000000400826 <+5>:
0x00000000000440824 <+55>:
                                                                                                         callq
                                                                                                         mov
mov
mov
                                                                                                                                                                                                                  # 0x6020a8 <r>
                                                                                                         callo
                                                                                                                                                                                                                  # 0x6020a0 <d>
```

0x0000000000040083b <+62>:

```
0x0000000000400842 <+69>:
0x00000000000400845 <+72>:
0x000000000000400844 <+77>:
0x0000000000040084f <+82>:
                                                                                               %rax,%rdi
$0x0,%eax
                                                                                callo
                                                                                               0x4006f0 <
                                                                                                                     __isoc99_scanf@plt>
                                                                                                -0x8(%rbp).%eax
                                                                                               %eax.-0x4(%rbp)
                   0x00000000000400852 <+85>:
                                                                                               0x40088e <password+145>
0x201832(%rip),%rax
                   0x00000000000400855 <+88>:
                   0x00000000000400857 <+90>:
                                                                                                                                                      # 0x602090 <o>
                                                                                               %rax,%rdi
0x4008c4 <generate_password>
                   0x000000000040085e <+97>:
0x00000000000400861 <+100>:
                                                                                mov
callq
                   0x0000000000400866 <+105>:
0x00000000000400869 <+108>:
                                                                                mov
                                                                                               %rax.%rdx
                                                                                               %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                   0x00000000000400870 <+115>:
                   0x00000000000400877 <+122>:
                                                                                               %rcx.%rsi
                   0x0000000000040087a <+125>:
                                                                                               %rax.%rdi
                   0x0000000000040087d <+128>:
                                                                                               $0x0.%eax
                  0x000000000000400874 <-1285:
0x00000000000400882 <-1133:
0x0000000000400883 <-1345:
0x00000000000000000886 <-1435:
0x00000000000000000885 <-1455:
0x0000000000000000000888 <-1455:
0x000000000000000000888 <-1655:
0x000000000000000000888 <-1665:
0x00000000000000000838 <-1665:
0x00000000000000000383 <-1666:
                                                                                calla
                                                                                               0x400680 <printf@plt>
                                                                                               $0x1.%eax
                                                                                              0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                jmp
mov
                                                                                                                                                       # 0x6020b0 <f>
                                                                                               %rax,%rdi
                                                                                              0x400650 <puts@plt>
                                                                                callq
                                                                                mov
leaveq
                                                                                               $0x0,%eax
End of assembler dump.
             (gdb) p/d $eax
$1 = 242262210
             (gdb) p/d ( $rbp - 0x4 )
$2 = 140737488348540
                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                                                       # 0x6020a0 <d>
                                                                                                                       _isoc99_scanf@plt>
                                                                                                                                                       # 0x602090 <o>
                                                                                             0x201332(%rip),%rax #
%rax,%rdi
0x4008c4 <generate_password>
%rax,%rdx
0x201348(%rip),%rcx #
0x201348(%rip),%rax #
%rcx,%rsi
%rax,%rdi
$x00,%eax
0x400630 <pririff@plt>
$0x1,%eax
0x400630 <pririff@plt>
$0x1,%eax
0x400630 <pririff@plt>
$0x20131b(%rip),%rax #
%rax,%rdi
$0x20131b(%rip),%rax #
%rax,%rdi
$0x400650 <pririff@plt>
$0x0,0%eax
                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                       # 0x6020b0 <f>
                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                                                       # 0x6020a0 <d>
                                                                                                                       _isoc99_scanf@plt>
                                                                                                                                                       # 0x602090 <n>
                                                                                               0x2018321%:1p,,......
%rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                  9.00000000000400873 <-12.55-
9.000000000000400874 <-12.58-
9.0000000000004008872 <-12.58-
9.0000000000004008872 <-13.58-
9.0000000000004008872 <-13.58-
9.0000000000004008882 <-14.55-
9.0000000000004008882 <-14.55-
9.0000000000004008883 <-15.55-
9.00000000000004008883 <-15.55-
9.00000000000004008833 <-15.56-
9.00000000000004008833 <-15.56-
9.00000000000000400833 <-15.56-
9.00000000000000400833 <-15.56-
9.000000000000000400833 <-15.56-
9.00000000000000400833 <-15.56-
9.000000000000000000000000003
                                                                                mov
jmp
mov
mov
                                                                                               $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                       # 0x6020b0 <f>
                                                                                              %rax,%rdi
0x400650 <puts@plt>
                                                                                calla
                                                                                mov
leaveq
                                                                                              $0x0.%eax
            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
             21 in gdb.c
(gdb) i r
             rax
rbx
                                            0x62
                                                             98
                                            0x7fffff7b00870
                                                                               140737348896880
            rcx
rdx
rsi
rdi
rbp
rsp
r8
                                            0x7fffff7dd59e0
0x7fffff7ff5000
                                                                                140737351866848
140737354092544
                                            0x1 1
0x7ffffffffe580
                                                                                0x7fffffffe580
                                            0x7ffffffffe570
0xffffffff
                                                                                0x7ffffffffe570
4294967295
```

0x0000000000040083f <+66>:

%rdx.%rsi

```
r9
r10
r11
r12
r13
r14
r15
rip
eflags
cs
ss
ds
es
fs
                                                0x22
                                                0x246
                                                0x400710 4196112
                                                0x7ffffffffe670
                                                                                              140737488348784
                                                0x400834 0x400834 <password+55>
                                                0x246
                                                                           [ PF ZF IF ]
                                                0x33
                                                                          51
43
                                                0x2b
   gs
(gdb) ni
                                                0×0
                                                                         21
   0x0000000000040083b
                                                                                                  in adb.c
   (adb) disas
  Dump of assembler code for function password:
push
mov
                                                                                                                        %rbp
                                                                                                                       %rsp,%rbp
$0x10,%rsp
                                                                                                   sub
                                                                                                                       $0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                   movl
                                                                                                   mov
callq
                                                                                                   mov
callq
                                                                                                                        %eax,%edi
                                                                                                                        0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                   callq
                                                                                                                        %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                   mov
mov
                                                                                                                                                                                                        # 0x6020a8 <r>
                                                                                                                       %x2016/C(%1f),%fdx
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
                                                                                                   callq
                                                                                                                                                                                                        # 0x6020a0 <d>
                                                                                                   mov
lea
                                                                                                   mov
                                                                                                   mov
                                                                                                                         %rax,%rdi
                                                                                                                      %rax,%rd1
$0x0,%eax
0x4006f0 <_isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax # (
                                                                                                   mov
callq
                                                                                                   mov
                                                                                                   cmp
jne
                                                                                                                                                                                                        # 0x602090 <o>
                                                                                                   mov
                                                                                                   mov
callq
                                                                                                                        %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                        %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                   mov
mov
                                                                                                                                                                                                        # 0x6020b8 
# 0x602098 <s>
                                                                                                   mov
                                                                                                   mov
                                                                                                                         %rcx,%rsi
                                                                                                   mov
                                                                                                                         %rax,%rdi
                                                                                                   mov
callq
                                                                                                                        $0x0,%eax
0x400680 <printf@plt>
                                                                                                                        $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                  mov
jmp
mov
                                                                                                                                                                                                        # 0x6020b0 <f>
                                                                                                                      %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                                                                   mov
callq
                                                                                                   mov
leaveq
retq
                                             0x400c73 4197491
0x0 0
0x7ffff7b00870 140737348896880
0x7ffff7b00810 140737351866848
0x7ffff7f500 10 140737354092540
0x7fffffff500 10 140737354092540
0x7fffffff580 0x7fffffff570
0x10 0x7ffffffff570 0x7fffffff6570
0x646 582
0x409710 4196112
0x7fffffff6570 140737488348784
0x0 0
0x40083b 0x40083b <password+62>
0x246 [PF ZF IF]
0x33 51
0x20 0
0x40 0
0x0 0

                                                0x400c73 4197491
# 0x6020a8 <r>
                                                                                                                                                                                                        # 0x6020a0 <d>
                                                                                                                                                          _isoc99_scanf@plt>
                                                                                                                                                                                                        # 0x602090 <o>
                                                                                                                        %rax,%rdi
0x4008c4 <generate_password>
                                                                                                  mov
callq
mov
mov
mov
mov
mov
callq
                                                                                                                       %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                                                                                                                        # 0x6020b8 
# 0x602098 <s>
            0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                                                         %rcx,%rsi
%rax,%rdi
            0x0000000000040087a <+125>:
            0×000000000040087d <+128>:
                                                                                                                        $0x0,%eax
0x400680 <printf@plt>
            0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                  mov
jmp
mov
                                                                                                                         $0x1,%eax
                                                                                                                        0x4008a2 <password+165>
0x20181b(%rip),%rax
            0x000000000040088c <+143>:
0x0000000000040088e <+145>:
                                                                                                                                                                                                        # 0x6020b0 <f>
            0X000000000400836 <+145>:
0X0000000000400898 <+155>:
0X000000000000400894 <+165>:
0X000000000000400834 <+165>:
0X00000000000400833 <+166>:
                                                                                                                     %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                                                                   calla
                                                                                                   leaved
  End of assembler dump.
   (gdb) ni
0x000000000040083f
                                                                 21
                                                                                                  in adb.c
  %rbp
%rsp,%rbp
$0x10,%rsp
```

```
$0x0,%edi
0x4006d0 <time@plt>
                                                callq
                                                          %eax.%edi
                                                calla
                                                          0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                          %eax.-0x4(%rbp)
                                                          0x20187c(%rip),%rax
                                                                                                 # 0x6020a8 <r>
                                                          %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                calla
                                                mov
lea
                                                                                                 # 0x6020a0 <d>
                                                          %rdx.%rsi
                                                mov
                                                          %rax.%rdi
     mov
callq
                                                          $0x0.%eax
                                                          0x4006f0 <__isoc99_scanf@plt>
                                                          -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                mov
                                                cmp
jne
                                                          0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                 # 0x602090 <o>
                                                          %rax,%rdi
0x4008c4 <generate_password>
                                                callq
                                                mov
                                                          %rax,%rdx
                                                          0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                mov
                                                                                                 # 0x6020b8 
# 0x602098 <s>
                                                mov
                                                          %rcx,%rsi
                                                          %rax,%rdi
                                                          $0x0,%eax
0x400680 <printf@plt>
                                                callq
                                                          jmp
mov
                                                                                                 # 0x6020b0 <f>
                                                mov
callq
                                                          %rax,%rdi
0x400650 <puts@plt>
                                                mov
leaveq
                                                          $0x0,%eax
 End of assembler dump. (gdb) i r
                       0x400c73 4197491
 rax
rbx
rbx
rcx
rdx
rsi
rdi
rbp
rsp
r8
r9
r10
r11
r12
r13
r14
r15
rip
eflags
cs
ss
ds
                       0x0 0
0x7fffff7b00870
                                                140737348896880
                       0x7ffffffffe578
0x7fffff7ff5000
                                                140737488348536
140737354092544
                       0x1 1
0x7fffffffe580
                       0x7ffffffffe570
0xffffffff
                                                4294967295
                       0x246 582
0x400710 4196112
0x7fffffffe670 140737488348784
                      # 0x6020a8 <r>
                                                                                                 # 0x6020a0 <d>
                                                                                                 # 0x602090 <o>
                                                                                                 # 0x6020b8 
# 0x602098 <s>
                                                                                                 # 0x6020h0 <f>
 0x000000000004008as <+100
End of assembler dump.
(gdb) ni
0x00000000000400842 21
                                                in adb.c
  in adb.c
  (gdb) ni
0x0000000000040084a
                               21
                                               in gdb.c
  (gdb) ni
ni
%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                          0x4006d0 <time@plt>
                                                          0x400600 <Time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                 # 0x6020a8 <r>
                                                          0X2018/C(%rip),%rax
%rax,%rdi
0X400650 <puts@plt>
0X201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
      0x000000000040082c <+47>:
0x0000000000040082f <+50>:
0x00000000000400834 <+55>:
                                                callo
                                                mov
lea
mov
mov
                                                                                                 # 0x6020a0 <d>
     0x0000000040083b <+62>:
0x000000000040083f <+66>:
0x00000000000400842 <+69>:
0x00000000000400845 <+72>:
                                                          %rax,%rdi
$0x0,%eax
```

0x00000000000400805 <+8>:

\$0x0.-0x8(%rbp)

```
-0x8(%rbp).%eax
                                                                                                          -0x8(%rop), %eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                 # 0x602090 <o>
                                                                                            mov
callq
                                                                                                           %rax,%rdi
                                                                                                           %14008c4 <generate_password>
                                                                                                           %rax.%rdx
                                                                                                           0x201848(%rip).%rcx
                                                                                                                                                                 # 0x6020b8 
# 0x602098 <s>
                                0x00000000000400870 <+115>:
                                                                                                           0x201821(%rip),%rax
                                0x00000000000400877 <+122>:
                                                                                                           %rcx,%rsi
%rax,%rdi
                                0x0000000000040087a <+125>:
                                0x0000000000040087d <+128>:
                                                                                            mov
callq
                                                                                                           $0x0.%eax
                                0x00000000000400882 <+133>:
                                                                                                          0x400680 <printf@plt>
                                0x00000000000400887 <+138>:
                                                                                                           $0x1.%eax
                                                                                                          0x4008a2 <password+165>
0x20181b(%rip),%rax
                                0x0000000000040088c <+143>:
                                                                                            jmp
mov
                               0x000000000040088c <+143>:
0x000000000040088e <+145>:
0x0000000000400895 <+155>:
0x00000000000400898 <+155>:
0x0000000000400894 <+166>:
0x0000000000400832 <+166>:
0x00000000000400833 <+166>:
                                                                                                                                                                 # 0x6020b0 <f>
                                                                                                          %rax,%rdi
0x400650 <puts@plt>
                                                                                            calla
                                                                                                          $0x0.%eax
                                                                                            leaveq
                          End of assembler dump.
                          (gdb) ni
0x0000000000400852
                                                                        22
                                                                                           in gdb.c
                          (gdb) ni
0x00000000000400855 22
                                                                                          in qdb.c
                          (gdb) ni
27
                         27 in gdb.c
(gdb) quit
                          A debugging session is active.
                                        Inferior 1 [process 62493] will be killed.
                       Inferior 1 [process 62493] will be killed.

Quit anyway? (y or n) y
ppate85@hrumil:~/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 <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
License GPLv3+: GNU GPL version 3 or later <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
This is GB was configured as "x86_64-linux-gnu". Type "show copying" and "show warranty" for details.
This GBB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<a href="http://www.gnu.org/software/gdb/dbugs/>-find the GBB manual and other documentation resources online at:</a>
<a href="http://www.gnu.org/software/gdb/dbcumentation/>-
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.
The process is not being run.
                         The program is not being run. (gdb) ni
                                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
0x00000000000400816 18 in gdb.c
(gdb) ni
# 0x6020a8 <r>
                                                                                                                                                                 # 0x6020a0 <d>
                                                                                                                                  _isoc99_scanf@plt>
                                                                                                                                                                 # 0x602090 <n>
                                                                                                          %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                                                 # 0x6020b8 
# 0x602098 <s>
                               0x0000000000400877 <-12/2>:
0x0000000000400873 <-12/5>:
0x00000000000400874 <-12/6>:
0x000000000000400882 <-13/3>:
0x00000000000400882 <-13/3>:
0x00000000000400882 <-14/3>:
0x00000000000400886 <-14/3>:
                                                                                           mov
jmp
mov
mov
                                                                                                          0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                 # 0x6020b0 <f>
                                0x00000000000400895 <+152>:
                                                                                                        %rax,%rdi
0x400650 <puts@plt>
                                                                                            calla
                                0x00000000000400898 <+155>:
                                0x0000000000440896 <+153>.
0x0000000000044089d <+160>:
0x00000000000440882 <+165>:
0x00000000000440883 <+166>:
                                                                                                          $0x0.%eax
                                                                                            leaved
                          End of assembler dump.
                          (gdb) ni
0x0000000000040082c
                                                                         20
                                                                                           in adb.c
                          (adb) ni
                          0x0000000000040082f
                                                                        20
                                                                                           in qdb.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
                          21 in gdb.c
(qdb) disas
                         Dump of assembler code for function password:
0x000000000004007fd <+0>: push %rbp
```

0x0000000000040084a <+77>:

callo

0x4006f0 < isoc99 scanf@plt>

```
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                0x000000000004007fe <+1>:
               0x0000000004007Fe <+15:

0x000000000000400801 <+4>:

0x000000000000400805 <+8>:

0x0000000000040080c <+15>:

0x00000000000400811 <+20>:

0x00000000000400816 <+25>:
                                                                                                        movl
                                                                                                       calla
                                                                                                                           0x4006d0 <time@plt>
                                                                                                                            %eax.%edi
                                                                                                       calla
                                                                                                                           0x4006a0 srand@plt>
0x400700 <rand@plt>
             0x00000000400018 <-27>
0x000000000400014 <-27>
0x0000000000400014 <-37>
0x0000000000400012 <-37>
0x0000000000400012 <-47>
0x0000000000400012 <-47>
0x0000000000400012 <-47>
0x0000000000400012 <-47>
0x000000000400012 <-47>
0x000000000400013 <-55>
0x000000000400013 <-55>
0x000000000400013 <-55>
0x000000000400013 <-55>
0x000000000400013 <-55>
0x000000000400013 <-55>
0x0000000000400013 <-55>
0x0000000000400013 <-55>
0x0000000000400013 <-55>
0x0000000000400013 <-55>
0x0000000000400013 <-75>
0x00000000000000000000015 <-77>
                0x00000000000400818 <+27>:
                                                                                                       callo
                                                                                                                            %eax.-0x4(%rbp)
                                                                                                                            0x20187c(%rip),%rax
                                                                                                                                                                                                           # 0x6020a8 <r>
                                                                                                                           %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                       calla
                                                                                                       mov
lea
                                                                                                                                                                                                           # 0x6020a0 <d>
                                                                                                                            %rdx.%rsi
                                                                                                       mov
                                                                                                                            %rax.%rdi
                                                                                                                            $0x0.%eax
               0x00000000400845 <+72>:
0x000000000400844 <+77>:
0x000000000400844 <+82>:
0x0000000000400845 <+85>:
0x00000000000400855 <+85>:
0x00000000000400855 <+90>:
0x0000000000400855 <+997>:
0x0000000000400856 <+105>:
0x0000000000400856 <+105>:
0x00000000000400856 <+105>:
                                                                                                       calla
                                                                                                                           0x4006f0 < isoc99 scanf@plt>
                                                                                                       mov
                                                                                                                            -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                                                       cmp
jne
                                                                                                                            0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                           # 0x602090 <o>
                                                                                                       mov
callq
                                                                                                                            %rax,%rdi
                                                                                                                            0x4008c4 <generate_password>
                                                                                                       mov
                                                                                                                            %rax,%rdx
                0x0000000000440860 <+103>:
0x00000000000440869 <+108>:
0x00000000000440870 <+115>:
0x00000000000440877 <+122>:
                                                                                                                            0x201848(%rip),%rcx
                                                                                                       mov
                                                                                                                                                                                                            # 0x6020b8 
                                                                                                                            0x201821(%rip),%rax
                                                                                                                                                                                                            # 0x602098 <s>
                                                                                                                            %rcx,%rsi
               0x000000000040087a <+125>:
                                                                                                                            %rax,%rdi
                                                                                                                            $0x0,%eax
                                                                                                       callq
                                                                                                                            0x400680 <printf@plt>
                                                                                                                           0x400000 -p.1...

$0x1,%eax

0x4008a2 <password+165>

0x20181b(%rip),%rax
                                                                                                       jmp
mov
                                                                                                                                                                                                           # 0x6020b0 <f>
                                                                                                       mov
callq
                                                                                                                           %rax,%rdi
0x400650 <puts@plt>
                                                                                                       mov
leaveq
                                                                                                                           $0x0,%eax
End of assembler dump.
        (gdb) ni
0x000000000040083b 21
                                                                                                       in qdb.c
                                                                                                                        # 0x6020a8 <r>
                                                                                                                                                                                                           # 0x6020a0 <d>
                                                                                                                                                                                                           # 0x602090 <o>
                                                                                                                                                                                                           # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                           # 0x6020b0 <f>
     | In a days | In a
                                                                                                                                                                                                           # 0x6020a8 <r>
                                                                                                                                                                                                           # 0x6020a0 <d>
                                                                                                                                                              isoc99 scanf@plt>
                                                                                                                                                                                                           # 0x602090 <o>
                                                                                                                           %rax,%rdi
0x4008c4 <generate_password>
                                                                                                      mov
mov
mov
mov
mov
callq
                                                                                                                                                                                                            # 0x6020b8 
# 0x602098 <s>
                 0x0000000000400870 <+115>:
                                                                                                                            0x201821(%rip),%rax
                 0x00000000000400877 <+122>:
                                                                                                                            %rcx,%rsi
%rax,%rdi
                0x0000000000040087a <+125>:
                0x0000000000040087d <+128>:
                                                                                                                           $0x0,%eax
0x400680 <printf@plt>
                 0x00000000000400882 <+133>:
                                                                                                      mov
jmp
mov
                 0x00000000000400887 <+138>:
                                                                                                                            $0x1.%eax
                                                                                                                           $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                 0x0000000000040088c <+143>:
                                                                                                                                                                                                           # 0x6020b0 <f>
                 0x000000000040088e
                                                                        <+145>:
                 0x00000000000400895 <+152>:
                                                                                                                           %rax,%rdi
0x400650 <puts@plt>
                                                                                                       calla
                 0x00000000000400898 <+155>:
                0X0000000000440898 <+155>:

0X0000000000044089d <+160>:

0X0000000000440882 <+165>:

0X0000000000440883 <+166>:
                                                                                                                           $0x0.%eax
                                                                                                       leaved
                                                                                                       reta
      End of assembler dump.
(gdb) ni
0x0000000000400842
                                                                       21
                                                                                                     in adb.c
        (odb) disas
               np of assembler code for function password:
0x00000000004007fd <+0>: push %rbp
```

```
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
        0x000000000004007fe <+1>:
       0x0000000004007Fe <+15:

0x000000000000400801 <+45:

0x00000000000400805 <+85:

0x0000000000040080c <+15>:

0x00000000000400811 <+205:

0x00000000000040816 <+255:
                                                    movl
                                                   calla
                                                              0x4006d0 <time@plt>
                                                              %eax.%edi
                                                   calla
                                                              0x4006a0 srand@plt>
0x400700 <rand@plt>
      0x00000000000400818 <+27>:
                                                   callo
                                                              %eax.-0x4(%rbp)
                                                              0x20187c(%rip),%rax
                                                                                                      # 0x6020a8 <r>
                                                             %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                   calla
                                                   mov
lea
                                                                                                      # 0x6020a0 <d>
                                                              %rdx.%rsi
                                                   mov
                                                              %rax.%rdi
                                                              $0x0.%eax
       0x00000000400845 <+72>:
0x000000000400844 <+77>:
0x000000000400844 <+82>:
0x0000000000400847 <+82>:
0x00000000000400855 <+85>:
0x00000000000400855 <+89>:
0x0000000000400855 <+99>:
0x000000000400856 <+105>:
0x0000000000400856 <+105>:
0x00000000000400856 <+105>:
                                                   calla
                                                              0x4006f0 < isoc99 scanf@plt>
                                                   mov
                                                              -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                   cmp
jne
                                                              0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                      # 0x602090 <o>
                                                   mov
callq
                                                              %rax,%rdi
                                                              0x4008c4 <generate_password>
                                                   mov
                                                              %rax,%rdx
        0x0000000000440860 <+103>:
0x00000000000440869 <+108>:
0x00000000000440870 <+115>:
0x00000000000440877 <+122>:
                                                              0x201848(%rip),%rcx
                                                                                                      # 0x6020b8 
                                                   mov
                                                              0x201821(%rip),%rax
                                                                                                      # 0x602098 <s>
                                                              %rcx,%rsi
       0x000000000040087a <+125>:
                                                              %rax,%rdi
                                                              $0x0,%eax
                                                   callq
                                                              0x400680 <printf@plt>
                                                              0x400000 -p.1...

$0x1,%eax

0x4008a2 <password+165>

0x20181b(%rip),%rax
                                                   jmp
mov
                                                                                                      # 0x6020b0 <f>
                                                   mov
callq
                                                             %rax,%rdi
0x400650 <puts@plt>
                                                   mov
leaveq
                                                              $0x0,%eax
End of assembler dump.
    (gdb) ni
0x0000000000400845 21
                                                   in qdb.c
                                                            # 0x6020a8 <r>
                                                                                                      # 0x6020a0 <d>
                                                                                                      # 0x602090 <o>
                                                                                                      # 0x6020b8 
# 0x602098 <s>
                                                                                                      # 0x6020b0 <f>
  # 0x6020a8 <r>
                                                                                                      # 0x6020a0 <d>
                                                                               isoc99 scanf@plt>
                                                                                                      # 0x602090 <o>
                                                              %rax,%rdi
0x4008c4 <generate_password>
                                                   mov
mov
mov
mov
mov
callq
                                                                                                      # 0x6020b8 
# 0x602098 <s>
        0x00000000000400870 <+115>:
                                                              0x201821(%rip),%rax
        0x00000000000400877 <+122>:
                                                              %rcx,%rsi
%rax,%rdi
        0x0000000000040087a <+125>:
        0x0000000000040087d <+128>:
                                                              $0x0,%eax
0x400680 <printf@plt>
        0x00000000000400882 <+133>:
                                                   mov
jmp
mov
        0x00000000000400887 <+138>:
                                                              $0x1.%eax
                                                              90x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
        0x0000000000040088c <+143>:
                                                                                                      # 0x6020b0 <f>
        0x0000000000040088e <+145>:
        0x00000000000400895 <+152>:
                                                             %rax,%rdi
0x400650 <puts@plt>
        0x0000000000440893 <+152>:
0x00000000000440898 <+155>:
0x00000000000440894 <+160>:
0x0000000000440882 <+165>:
                                                   callo
                                                              $0x0.%eax
                                                   mov
leaveq
        0x0000000000004008a3 <+166>:
                                                   reta
   0x00000000000440883
End of assembler dump.
(gdb) i r
rax 0x0
rbx 0x0
rcx 0x7ffff
rdx 0x7ffff
                          0x7fffff7b00870
0x7ffffffffe578
                                                   140737348896880
```

140737488348536

```
0x7fffffffe578 140737488348536
0x400c73 4197491
0x7fffffffe580 0x7fffffffe580
      rsi
rdi
rbp
rsp
r8
r9
r10
r11
r12
r13
r14
r15
rip
eflags
cs
ss
ds
                                                                                                                                                                            0x7ffffffffe580
0x7ffffffffe570
                                                                                       0x7ffffffffe570
                                                                                                                                                                                  4294967295
                                                                                       0x22
                                                                                       0x40084a 0x40084a <password+77>
                                                                                                                                   [ PF ZF IF ]
51
43
                                                                                       0x246
                                                                                       0x33
                                                                                       0x2b
       es
fs
       gs
(gdb) disas
                                                                                       0×0
    %rsp,%rbp
$0x10,%rsp
                                                                                                                                                                                                                      $0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                                                                                                  movl
                                                                                                                                                                                 mov
callq
                                                                                                                                                                                  mov
callq
                                                                                                                                                                                                                         %eax,%edi
                                                                                                                                                                                                                       0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                                                                                                  callq
                                                                                                                                                                                                                       %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                  mov
                                                                                                                                                                                                                                                                                                                                                                     # 0x6020a8 <r>
                                                                                                                                                                                  mov
                                                                                                                                                                                                                       %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                                                                  callq
                                                                                                                                                                                                                                                                                                                                                                     # 0x6020a0 <d>
                                                                                                                                                                                  mov
lea
                                                                                                                                                                                                                         %rdx,%rsi
                                                                                                                                                                                  mov
                                                                                                                                                                                                                         %rax,%rdi
                                                                                                                                                                                  mov
callq
                                                                                                                                                                                                                         $0x0,%eax
0x4006f0 <
                                                                                                                                                                                                                                                                                   isoc99 scanf@plt>
                                                                                                                                                                                                                       -0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                 mov
cmp
jne
                                                                                                                                                                                                                                                                                                                                                                     # 0x602090 <o>
                                                                                                                                                                                  mov
callq
                                                                                                                                                                                                                         %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                                                                                                       %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                                                                                                  mov
mov
                                                                                                                                                                                                                         %rcx,%rsi
%rax,%rdi
                                                                                                                                                                                                                      $0x0,%eax
0x400680 <printf@plt>
$0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                                  mov
callq
                                                                                                                                                                                 mov
jmp
mov
                                                                                                                                                                                                                                                                                                                                                                     # 0x6020b0 <f>
                                                                                                                                                                                                                      %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                                                                                                                                                  mov
callq
| The content of the 
                                                                                                                                                                                                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                                                                                                                                                                                                                                                                     # 0x6020a0 <d>
                                                                                                                                                                                                                                                                                                                                                                     # 0x602090 <o>
                                                                                                                                                                                                                                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                                                                                                                                                                     # 0x6020h0 <f>
      | Ggd) n1 | gdb.c | Cgd) n1 | gdb.c | Cgd) n1 | Ggd 
                                                                                                                                                                                 in adb.c
                                                                                                                                                                                                                   %rbp
%rsp,%rbp
%0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                                                                                                                                                                                      0x4006d0 <time@plt>
                                                                                                                                                                                                                    0x4000d0 <tilme@ptt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                                                                                                                                                                     # 0x6020a8 <r>
                                                                                                                                                                                                                      %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                                                                                                                                                                                                                                                     # 0x6020a0 <d>
                   0x00000000040083b <-662:
0x000000000040083f <-665:
0x00000000000040083f <-659:
0x000000000000400845 <-772:
0x000000000000400846 <-7775:
0x000000000000040085f <-825:
0x00000000000400855 <-885:
                                                                                                                                                                                                                    -0x8(%rbp),%rdx
%rdx,%rdi
%rax,%rdi
$0x0,%eax
0x4006f0 <__isoc99_scan1
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
                                                                                                                                                                                  mov
mov
                                                                                                                                                                                  callo
                                                                                                                                                                                                                                                                                    isoc99 scanf@plt>
                                                                                                                                                                                 mov
cmp
jne
```

```
0x0000000000400857 <+90>:
                                                                    0x201832(%rip),%rax
                                                                                                               # 0x602090 <o>
           0x000000000040085; <+97>:
0x00000000000400861 <+100>:
0x00000000000400866 <+105>:
0x00000000000400869 <+108>:
                                                                    %rax,%rdi
0x4008c4 <generate_password>
                                                         callo
                                                                     %rax.%rdx
                                                                     0x201848(%rip).%rcx
                                                                                                               # 0x6020b8 
# 0x602098 <s>
           0x00000000000400870 <+115>:
                                                                     0x201821(%rip),%rax
           0x00000000000400877 <+122>:
                                                                     %rcx.%rsi
           0x0000000000040087a <+125>:
           0x0000000000040087d <+128>:
                                                         mov
callq
                                                                     $0x0.%eax
           0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                    0x400680 <printf@plt>
                                                         mov
jmp
mov
                                                                     $0x1.%eax
                                                                    0x4008a2 <password+165>
0x20181b(%rip),%rax
           0x0000000000040088c <+143>:
                                                                                                               # 0x6020b0 <f>
           0x0000000000040088e <+145>:
           0x00000000000400895 <+152>:
                                                                    %rax,%rdi
0x400650 <puts@plt>
           0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                         callo
                                                         mov
leaveq
                                                                    $0x0.%eax
End of assembler dump.
      (adb) ni
       0x00000000000400855 22
                                                         in gdb.c
                                                                                                               # 0x6020a8 <r>
                                                                                                               # 0x6020a0 <d>
                                                                                                               # 0x602090 <o>
                                                                                                               # 0x6020b8 
# 0x602098 <s>
                                                                                                               # 0x6020b0 <f>
                                                                                                               # 0x6020a8 <r>
                                                                                                               # 0x6020a0 <d>
                                                                                                               # 0x602090 <n>
                                                                                                               # 0x6020b8 
# 0x602098 <s>
                                                                                                               # 0x6020h0 <f>
      End of assembler dump.
(gdb) ni
0x0000000000400895 27
     in adb.c
                                                                   %rbp
%rsp,%rbp
%0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                                    0x4006d0 <time@plt>
                                                                   0x4000d0 <tilme@ptt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                               # 0x6020a8 <r>
                                                                    %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                               # 0x6020a0 <d>
          0x00000000040083b <+62>:
0x00000000040083f <+66>:
0x00000000040083f <+66>:
0x0000000000040083f <+72>:
0x00000000000400845 <+72>:
0x000000000000400846 <+77>:
0x000000000000400855 <+85>:
0x00000000000400855 <+88>:
                                                         mov
mov
                                                                     %rdx,%rsi
%rax,%rdi
                                                                    %rax,%rd1

$0x0,%eax

0x4006f0 <__isoc99_scan

-0x8(%rbp),%eax

%eax,-0x4(%rbp)

0x40088e <password+145>
                                                         callo
                                                                                       isoc99 scanf@plt>
                                                         mov
cmp
jne
```

```
0x0000000000400857 <+90>:
0x0000000000040085e <+97>:
0x000000000000400861 <+100>:
0x00000000000400866 <+105>:
0x00000000000400869 <+108>:
                                                                                                       0x201832(%rip),%rax
                                                                                                       %rax,%rdi
0x4008c4 <generate_password>
                                                                                      callo
                                                                                                        %rax.%rdx
                                                                                                        0x201848(%rip).%rcx
                                                                                                                                                                            # 0x6020b8 
# 0x602098 <s>
           0x00000000000400870 <+115>:
                                                                                                        0x201821(%rip),%rax
           0x00000000000400877 <+122>:
                                                                                                        %rcx,%rsi
%rax,%rdi
           0x0000000000040087a <+125>:
        mov
callq
                                                                                                        $0x0.%eax
                                                                                                       0x400680 <printf@plt>
                                                                                                        $0x1.%eax
                                                                                                       0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                      jmp
mov
                                                                                                                                                                            # 0x6020b0 <f>
                                                                                                      %rax,%rdi
0x400650 <puts@plt>
                                                                                      calla
                                                                                      mov
leaveq
                                                                                                       $0x0.%eax
End of assembler dump.
   (adb) ni
   0x0000000000400898
                                                          27
                                                                                     in gdb.c
                                                                                                       %rbp
%rsp,%rbp
                                                                                                       $0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                                                      callq 0x4006d0 <time@plt>
                                                                                                     0x400000 <1mcepts
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                            # 0x6020a8 <r>
                                                                                                       %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                                                            # 0x6020a0 <d>
                                                                                                        %rdx,%rsi
                                                                                                        %rax,%rdi
                                                                                                       %rax,%rd1
$0x0,%eax
0x4006f0 <__isoc99_scant
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                    isoc99 scanf@plt>
                                                                                                                                                                            # 0x602090 <o>
                                                                                                       %rax,%rdi
0x4008c4 <generate_password>
                                                                                                       %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                                                                                            # 0x6020b8 
# 0x602098 <s>
                                                                                                        %rcx,%rsi
                                                                                                        %rax,%rdi
                                                                                                       $0x0,%eax
0x400680 <printf@plt>
$0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                            # 0x6020b0 <f>
                                                                                                     %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                      Inferior 1 [process 62608] will be killed.
 Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ 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:~ Dhrumils ssh Dpate85@23.99.192.124
Dpate85@23.99.192.124*; 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 28.806B
    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:-%pate85% ls hw1 hw2 README.md Dpate85@Dhrumil:-%dpate85% cd hw2 Dpate85@Dhrumil:-%dpate85% cd hw2 Dpate85@Dhrumil:-%dpate85% ls nuzzles
 Dpate85@Dhrumil:~/dpate85/hw25 cd puzzles
Dpate85@Dhrumil:~/dpate85/hw25 cd puzzles
Dpate85@Dhrumil:~/dpate85/hw2/puzzless ls
0 1 2 3 4 howto.txt secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzless gdb 1
GNU gdb (Ubuntu 7.7.1-eubuntu5-14.04.2) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<a href="http://www.gnu.org/software/gdb/bugs/">http://www.gnu.org/software/gdb/bugs/</a>
Find the GDB manual and other documentation resources online at:
<a href="http://www.gnu.org/software/gdb/documentation/">http://www.gnu.org/software/gdb/documentation/">http://www.gnu.org/software/gdb/documentation/</a>
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from 1...done.
  Type "apropos word" to search for community is. 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 qdb.c:17
```

# 0x602090 <o>

```
%rbp
%rsp,%rbp
$0x10,%rsp
                                                                $0x0,-0x8(%rbp)
$0x0,%edi
                                                                0x4006d0 <time@plt>
                                                                %eax.%edi
                                                                0x4006a0 srand@plt>
0x400700 <rand@plt>
                                                                %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                          # 0x6020a8 <r>
                                                               %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                          # 0x6020a0 <d>
                                                                %rdx.%rsi
                                                                %rax.%rdi
                                                                $0x0,%eax
                                                                0x4006f0 <__isoc99_scanf@plt>
                                                                -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                          # 0x602090 <o>
                                                                %rax,%rdi
0x4008c4 <generate_password>
                                                                0x201848(%rip),%rcx
                                                                                                           # 0x6020b8 
# 0x602098 <s>
                                                                0x201821(%rip),%rax
      %rcx,%rsi
                                                                %rax,%rdi
                                                                $0x0,%eax
0x400680 <printf@plt>
                                                     callq
                                                                $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                     mov
jmp
mov
                                                                                                          # 0x6020b0 <f>
                                                     mov
callq
                                                               %rax,%rdi
0x400650 <puts@plt>
                                                                $0x0,%eax
                                                     mov
leaveq
  End of assembler dump.
(gdb) ni
18 in gdb.c
  (gdb) ni
0x0000000000400811
                                       18
                                                     in gdb.c
   (gdb) ni
0x0000000000400816
                                                     in gdb.c
   (gdb) ni
0x0000000000400818
in gdb.c
  0χυυυυς
(gdb) ni
19 in gdb.c
                                                               # 0x6020a8 <r>
                                                                                                          # 0x6020a0 <d>
                                                                                                          # 0x602090 <o>
                                                                                                          # 0x6020b8 
# 0x602098 <s>
                                                                                                          # 0x6020b0 <f>
  0x00000000004008a3
End of assembler dump.
(gdb) ni
0x00000000000400822
                                                     in gdb.c
   (gdb) p $eax
$1 = 981461572
   (gdb) print $eax
$2 = 981461572
  $2 = 981461572
(gdb) ni
20 in gdb.c
  (gdb) ni
0x0000000000040082c
 20
                                                     in adb.c
                                                               issword:

%rbp

%rsp,%rbp

$0x10,%rsp

$0x0,-0x8(%rbp)

$0x0,%edi

0x4006d0 <time@plt>
                                                               0x4000d0 <time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                          # 0x6020a8 <r>
                                                               %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                          # 0x6020a0 <d>
                                                                %rdx,%rsi
%rax,%rdi
$0x0,%eax
                                                                0x4006f0 < isoc99 scanf@plt>
      0x00000000040084a <+77>:
0x00000000040084f <+82>:
0x0000000040084f <+82>:
0x0000000000040085z <+85>:
0x0000000000400855 <+88>:
0x000000000400855 <+99>:
0x0000000000400855 <+97>:
0x0000000000400865 <+100>:
0x000000000400865 <+100>:
                                                     mov
cmp
jne
mov
                                                                -0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                          # 0x602090 <o>
                                                               %rax,%rdi
0x4008c4 <generate_password>
%rax,%rdx
                                                     callq
```

```
# 0x6020b8 
# 0x602098 <s>
          0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
0x00000000000040087a <+125>:
                                                            0x201821(%rip),%rax
                                                             %rcx,%rsi
%rax,%rdi
          0x0000000000040087d <+128>:
                                                   calla
          0x00000000000400882 <+133>:
                                                            0x400680 <printf@plt>
          0x00000000000400887 <+138>:
                                                             $0x1.%eax
                                                            0x4008a2 <password+165>
0x20181b(%rip),%rax
          0x0000000000040088c <+143>:
          0x0000000000040088e <+145>:
                                                                                                 # 0x6020b0 <f>
          0x00000000000400895 <+152>:
                                                             %rax,%rdi
          0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                            0x400650 <puts@plt>
                                                   callq
                                                   mov
leaveq
                                                            $0x0.%eax
      End of assembler dump.
      (adb) ni
      0x0000000000040082f 20
                                                  in adb.c
      (gdb) ni
behold! I will only tell you the secret password if you enter the random number I just generated!
                in adb.c
(gdb) ni
0x000000000040083b
                                                  in gdb.c
      (gdb) ni
0x0000000000040083f 21
                                                  in gdb.c
                                                                                                 # 0x6020a8 <r>
                                                                                                 # 0x6020a0 <d>
                                                                            isoc99 scanf@plt>
                                                                                                 # 0x602090 <o>
                                                             %rax,%rdi
0x4008c4 <generate_password>
                                                                                                 # 0x6020b0 <f>
                                                                                                 # 0x6020a8 <r>
                                                                                                 # 0x6020a0 <d>
                                                                            _isoc99_scanf@plt>
                                                           # 0x602090 <o>
                                                                                                 # 0x6020b8 
# 0x602098 <s>
                                                                                                 # 0x6020h0 <f>
          0x000000000004008a2 <+165>:
0x0000000000004008a3 <+166>:
     End of assembler dump.
(gdb) ni
0x00000000000400845 21
     in adb.c
                                                           issword:

%rbp

%rsp,%rbp

$0x10,%rsp

$0x0,-0x8(%rbp)

$0x0,%edi

0x4006d0 <time@plt>
                                                           0x400600 <time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                 # 0x6020a8 <r>
                                                           0x2018/C(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
                                                  mov
lea
mov
mov
                                                                                                 # 0x6020a0 <d>
          0x000000000040083b <+62>:
0x0000000000040083f <+66>:
0x00000000000400842 <+69>:
                                                             %rax.%rdi
          0x00000000000400845 <+72>:
0x0000000000040084a <+77>:
                                                           0x4006f0 < isoc99 scanf@plt>
                                                   callq
```

0x201848(%rip).%rcx

0x00000000000400869 <+108>:

```
0x0000000000040084f <+82>:
                                                                -0x8(%rbp).%eax
      0x000000000400481 +82>:

0x00000000000400852 <+85>:

0x000000000000400855 <+88>:

0x000000000000400857 <+90>:

0x000000000000400856 <+97>:

0x00000000000400861 <+100>:
                                                                %eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                          # 0x602090 <o>
                                                     callo
                                                                0x4008c4 <generate_password>
      0x00000000000400866 <+105>:
                                                                0x201848(%rip).%rcx
      0x00000000000400869 <+108>:
                                                                                                           # 0x6020b8 
# 0x602098 <s>
      0x00000000000400870 <+115>:
                                                                0x201821(%rip),%rax
      0x00000000000400877 <+122>:
                                                                %rcx.%rsi
      0x0000000000040087a <+125>:
                                                                %rax.%rdi
      0x0000000000040087d <+128>:
                                                                $0x0.%eax
                                                     calla
      0x00000000000400882 <+133>:
                                                                0x400680 <printf@plt>
      0x00000000000400887 <+138>:
                                                                $0x1.%eax
                                                                0x4008a2 <password+165>
0x20181b(%rip),%rax
      0x0000000000040088c <+143>:
                                                     jmp
mov
                                                                                                          # 0x6020b0 <f>
      0x0000000000040088e <+145>:
      0x00000000000400895 <+152>:
                                                                %rax,%rdi
      0X0000000000400895 <+152>:
0X00000000000400898 <+155>:
0X000000000000400892 <+169>:
0X000000000000400833 <+166>:
                                                     calla
                                                               0x400650 <puts@plt>
                                                                $0x0.%eax
                                                     leaved
 End of assembler dump.
  (gdb) ni
  0x0000000000040084a 21
    in gdb.c
  (gdb) disas
 Dump of assembler code for function password:
                                                     push
mov
                                                                %rsp,%rbp
                                                               $0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                     sub
                                                     mov
callq
                                                               %eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                     callq
callq
                                                                %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                     mov
                                                                                                          # 0x6020a8 <r>
                                                     mov
                                                               %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                     mov
callq
                                                                                                          # 0x6020a0 <d>
                                                     mov
lea
                                                     mov
                                                                %rdx,%rsi
                                                     mov
                                                                %rax,%rdi
                                                     mov
callq
                                                                $0x0,%eax
0x4006f0 <
                                                                                  isoc99 scanf@plt>
                                                    mov
cmp
jne
                                                                -0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                          # 0x602090 <o>
                                                     mov
callq
                                                                %rax,%rdi
0x4008c4 <generate_password>
                                                                %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                     mov
mov
                                                                %rcx,%rsi
%rax,%rdi
                                                               $0x0,%eax
0x400680 <printf@plt>
$0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                     mov
callq
                                                    mov
jmp
mov
                                                                                                          # 0x6020b0 <f>
                                                               %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
# 0x6020a8 <r>
                                                                                                          # 0x6020a0 <d>
                                                                                                          # 0x602090 <0>
                                                                                                           # 0x6020b8 
# 0x602098 <s>
                                                                                                          # 0x6020h0 <f>
                                                               %rax,%rdi
0x400650 <puts@plt>
                                                    callq
      0x000000000040089d <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                     mov
leaved
                                                                $0x0.%eax
 End of assembler dump.
(gdb) ni
0x0000000000400852 22
 in adb.c
                                                               %rbp
%rsp,%rbp
%0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                               0x4006d0 <time@plt>
                                                               0x400600 <Time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                          # 0x6020a8 <r>
                                                               0X2018/C(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
      0x0000000000040082c <+47>:
0x00000000000040082f <+50>:
                                                     callo
                                                    mov
lea
mov
mov
       0×000000000000400021 <1502:
                                                                                                          # 0x6020a0 <d>
      0x00000000040083b <+62>:
0x000000000040083f <+66>:
0x000000000000400842 <+69>:
0x00000000000400845 <+72>:
                                                                %rax,%rdi
$0x0,%eax
```

```
0x0000000000040084a <+77>:
                                                   callo
                                                            0x4006f0 < isoc99 scanf@plt>
         0x00000000040084f <+82>:
0x00000000000400852 <+85>:
0x00000000000400855 <+88>:
0x00000000000400857 <+90>:
                                                             -0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                   # 0x602090 <o>
          0x0000000000040085e <+97>:
                                                   mov
callq
                                                             %14008c4 <generate_password>
          0x0000000000400861 <+100>:
          0x00000000000400866 <+105>:
                                                             0x201848(%rip).%rcx
          0x00000000000400869 <+108>:
                                                                                                   # 0x6020b8 
# 0x602098 <s>
          0x00000000000400870 <+115>:
                                                             0x201821(%rip),%rax
          0x00000000000400877 <+122>:
                                                             %rcx,%rsi
          0x0000000000040087a <+125>:
                                                             %rax.%rdi
          0x0000000000040087d <+128>:
                                                   mov
callq
                                                             $0x0.%eax
          0x00000000000400882 <+133>:
                                                             0x400680 <printf@plt>
          0x00000000000400887 <+138>:
                                                             $0x1.%eax
                                                             0x4008a2 <password+165>
0x20181b(%rip),%rax
          0x0000000000040088c <+143>:
                                                   jmp
mov
                                                                                                   # 0x6020b0 <f>
          0x0000000000040088e <+145>:
          0x00000000000400895 <+152>:
                                                             %rax,%rdi
          0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                            0x400650 <puts@plt>
                                                   callo
                                                   mov
leaveq
                                                             $0x0.%eax
End of assembler dump.
      (gdb) ni
      0x00000000000400855 22
                                                   in gdb.c
                                                                                                   # 0x6020a8 <r>
                                                                                                   # 0x6020a0 <d>
                                                                                                   # 0x602090 <o>
                                                                                                   # 0x6020b0 <f>
                                                                                                   # 0x6020a8 <r>
                                                                                                   # 0x6020a0 <d>
                                                                                                   # 0x602090 <n>
                                                                                                   # 0x6020b8 
# 0x602098 <s>
                                                                                                   # 0x6020h0 <f>
     End of assembler dump.
(gdb) ni
0x000000000040085e 23
     in adb.c
                                                            %rbp
%rsp,%rbp
%0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                            0x4006d0 <time@plt>
                                                            0x400600 <Time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                   # 0x6020a8 <r>
                                                            0X2018/C(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
          0x0000000000040082c <+47>:
0x00000000000040082f <+50>:
                                                   callo
                                                   mov
lea
mov
mov
          0×000000000000400021 <1502:
                                                                                                   # 0x6020a0 <d>
          0x00000000040083b <+62>:
0x000000000040083f <+66>:
0x000000000000400842 <+69>:
0x00000000000400845 <+72>:
```

%rax,%rdi \$0x0,%eax

```
0x0000000000040084a <+77>:
                                                     callo
                                                              0x4006f0 < isoc99 scanf@plt>
           0x000000000040084f <+82>:
0x00000000000400852 <+85>:
0x000000000000400855 <+88>:
0x000000000000400857 <+90>:
                                                               -0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                      # 0x602090 <o>
          0x0000000000040085e <+97>
                                                     mov
callq
                                                                %14008c4 <generate_password>
           0x00000000000400861 <+100>:
           0x00000000000400866 <+105>:
                                                                0x201848(%rip).%rcx
           0x00000000000400869 <+108>:
                                                                                                      # 0x6020b8 
# 0x602098 <s>
           0x00000000000400870 <+115>:
                                                                0x201821(%rip),%rax
           0x00000000000400877 <+122>:
                                                                %rcx,%rsi
           0x0000000000040087a <+125>:
                                                                %rax.%rdi
           0x0000000000040087d <+128>:
                                                     mov
callq
                                                                $0x0.%eax
           0x00000000000400882 <+133>:
                                                               0x400680 <printf@plt>
           0x00000000000400887 <+138>:
                                                                $0x1.%eax
                                                               0x4008a2 <password+165>
0x20181b(%rip),%rax
           0x0000000000040088c <+143>:
                                                     jmp
mov
                                                                                                      # 0x6020b0 <f>
           0x0000000000040088e <+145>:
           0x00000000000400895 <+152>:
                                                                %rax,%rdi
           0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                               0x400650 <puts@plt>
                                                     callo
                                                     mov
leaveq
                                                               $0x0.%eax
End of assembler dump.
       (gdb) ni
       0x00000000000400861 23
                                                                                                      # 0x6020a8 <r>
                                                                                                      # 0x6020a0 <d>
                                                                                                      # 0x602090 <o>
                                                                                                      # 0x6020b0 <f>
                                                                                                      # 0x6020a8 <r>
                                                                                                      # 0x6020a0 <d>
                                                                                                      # 0x602090 <0>
                                                                                                      # 0x6020b8 
# 0x602098 <s>
                                                                                                      # 0x6020h0 <f>
           0x000000000040089d <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                     mov
leaved
                                                               $0x0.%eax
      End of assembler dump.
(gdb) ni
0x0000000000400869 23
      in adb.c
                                                              %rbp
%rsp,%rbp
%0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                               0x4006d0 <time@plt>
                                                               0x400600 <Time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                      # 0x6020a8 <r>
                                                               0X2018/C(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
           0x0000000000040082c <+47>:
0x00000000000040082f <+50>:
                                                     callo
                                                     mov
lea
mov
mov
           0×000000000000400021 <1502:
                                                                                                      # 0x6020a0 <d>
           0x00000000040083b <+62>:
0x000000000040083f <+66>:
0x000000000000400842 <+69>:
0x00000000000400845 <+72>:
```

%rax,%rdi \$0x0,%eax

```
0x0000000000040084a <+77>:
                                                      callo
                                                                0x4006f0 < isoc99 scanf@plt>
           0x000000000040084f <+82>:
0x00000000000400852 <+85>:
0x000000000000400855 <+88>:
0x000000000000400857 <+90>:
                                                                 -0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                        # 0x602090 <o>
           0x0000000000040085e <+97>:
0x000000000000400861 <+100>:
                                                      mov
callq
                                                                 0x4008c4 <generate_password>
           0x0000000000400866 <+105>:
                                                                 0x201848(%rip).%rcx
           0x00000000000400869 <+108>:
                                                                                                        # 0x6020b8 
# 0x602098 <s>
           0x00000000000400870 <+115>:
                                                                 0x201821(%rip),%rax
           0x00000000000400877 <+122>:
                                                                 %rcx,%rsi
           0x0000000000040087a <+125>:
                                                                 %rax.%rdi
           0x0000000000040087d <+128>:
                                                      mov
callq
                                                                 $0x0.%eax
           0x00000000000400882 <+133>:
                                                                 0x400680 <printf@plt>
           0x00000000000400887 <+138>:
                                                                 $0x1.%eax
                                                                 0x4008a2 <password+165>
0x20181b(%rip),%rax
           0x0000000000040088c <+143>:
                                                      jmp
mov
                                                                                                        # 0x6020b0 <f>
           0x0000000000040088e <+145>:
           0x00000000000400895 <+152>:
                                                                 %rax,%rdi
           0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                0x400650 <puts@plt>
                                                      callo
                                                      mov
leaveq
                                                                 $0x0.%eax
End of assembler dump.
       (gdb) ni
       0x00000000000400870 23
                                                                                                        # 0x6020a8 <r>
                                                                                                        # 0x6020a0 <d>
                                                                                                        # 0x602090 <o>
                                                                                                        # 0x6020b0 <f>
                                                                                                         # 0x6020a8 <r>
                                                                                                        # 0x6020a0 <d>
                                                                                                        # 0x602090 <n>
                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                        # 0x6020h0 <f>
           0x000000000040089d <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                      mov
leaved
                                                                 $0x0.%eax
      End of assembler dump.
(gdb) ni
0x000000000040087a 23
      in adb.c
                                                               %rbp
%rsp,%rbp
%0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                                0x4006d0 <time@plt>
                                                                0x400600 <Time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                        # 0x6020a8 <r>
                                                                0X2018/C(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
           0x0000000000040082c <+47>:
0x00000000000040082f <+50>:
                                                      callo
                                                      mov
lea
mov
mov
           0×000000000000400021 <1502:
                                                                                                        # 0x6020a0 <d>
           0x00000000040083b <+62>:
0x000000000040083f <+66>:
0x000000000000400842 <+69>:
0x00000000000400845 <+72>:
                                                                 %rax,%rdi
$0x0,%eax
```

```
0x0000000000040084a <+77>:
                                                                                                                                                                                      callo
                                                                                                                                                                                                                     0x4006f0 < isoc99 scanf@plt>
                                    0x0000000000400844 <+777:
0x0000000000400854 <+85>:
0x00000000000400855 <+885:
0x000000000000400855 <+888:
0x00000000000400857 <+90>:
0x0000000000400856 <+977:
0x00000000000400851 <+100>:
                                                                                                                                                                                                                        -0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                                                                                                                                            # 0x602090 <o>
                                                                                                                                                                                      mov
callq
                                                                                                                                                                                                                          0x4008c4 <generate_password>
                                      0x00000000000400866 <+105>:
                                                                                                                                                                                                                          %rax.%rdx
                                                                                                                                                                                                                          0x201848(%rip).%rcx
                                      0x00000000000400869 <+108>:
                                                                                                                                                                                                                                                                                                                                                            # 0x6020b8 
# 0x602098 <s>
                                      0x00000000000400870 <+115>:
                                                                                                                                                                                                                          0x201821(%rip),%rax
                                       0x00000000000400877 <+122>:
                                                                                                                                                                                                                          %rcx,%rsi
                                    0x0000000000040087a <+125>:
                                                                                                                                                                                                                          %rax.%rdi
                                      0x0000000000040087d <+128>:
                                                                                                                                                                                      mov
callq
                                                                                                                                                                                                                          $0x0.%eax
                                      0x00000000000400882 <+133>:
                                                                                                                                                                                                                        0x400680 <printf@plt>
                                       0x00000000000400887 <+138>:
                                                                                                                                                                                                                          $0x1.%eax
                                                                                                                                                                                                                        0x4008a2 <password+165>
0x20181b(%rip),%rax
                                      0x0000000000040088c <+143>:
                                                                                                                                                                                      jmp
mov
                                                                                                                                                                                                                                                                                                                                                            # 0x6020b0 <f>
                                      0x0000000000040088e <+145>:
                                      0x00000000000400895 <+152>:
                                                                                                                                                                                                                       %rax,%rdi
0x400650 <puts@plt>
                                      0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                                                                                                                                      callo
                                                                                                                                                                                      mov
leaveq
                                                                                                                                                                                                                        $0x0.%eax
| The composition of the composi
                        End of assembler dump.
                        (gdb) ni
                         0x0000000000040087d 23
                                                                                                                                                                                                                                                                                                                                                            # 0x6020a8 <r>
                                                                                                                                                                                                                                                                                                                                                            # 0x6020a0 <d>
                                                                                                                                                                                                                                                                                                                                                            # 0x602090 <o>
                                                                                                                                                                                                                                                                                                                                                            # 0x6020b0 <f>
                                                                                                                                                                                                                                                                                                                                                             # 0x6020a8 <r>
                                                                                                                                                                                                                                                                                                                                                            # 0x6020a0 <d>
                                                                                                                                                                                                                                                                                                                                                            # 0x602090 <n>
                                                                                                                                                                                                                                                                                                                                                             # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                                                                                                                                                            # 0x6020h0 <f>
                                      0X00000000000400898 <+152>:
0X0000000000400898 <+155>:
0X00000000000040089d <+160>:
0X000000000004008a2 <+165>:
0X000000000004008a3 <+166>:
                                                                                                                                                                                                                        $0x0.%eax
                                                                                                                                                                                      mov
leaved
                      End of assembler dump.
                     End of assemble.
(gdb) ni
you win! the secret is:
dUJSQFAOAg==
25 in gdb.c
                     | OJSQ/HAUNG== | Code | Discovery | Code |
                                                                                                                                                                                                                     ssword:
%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                                                                                                                                     0x4006d0 <time@plt>
%eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                    0x0000000000400810 <+32>:
0x00000000000400812 <+37>:
0x000000000000400825 <+40>:
0x0000000000040082c <+47>:
0x0000000000040082f <+50>:
0x00000000000400834 <+55>:
                                                                                                                                                                                      mov
                                                                                                                                                                                                                                                                                                                                                            # 0x6020a8 <r>
                                                                                                                                                                                                                     0x2018/c(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
                                                                                                                                                                                      callo
                                                                                                                                                                                                                                                                                                                                                            # 0x6020a0 <d>
                                                                                                                                                                                      mov
lea
                                      0x0000000000040083b <+62>:
0x0000000000040083f <+66>:
```

```
0x00000000000400842 <+69>:
                                                                                                                                  %rax.%rdi
                        0x00000000000400845 <+72>:
0x00000000000040084a <+77>:
0x00000000000040084f <+82>:
                                                                                                                                   $0x0.%eax
                                                                                                                                  0x4006f0 <
                                                                                                              callo
                                                                                                                                                                  isoc99 scanf@plt>
                                                                                                                                   -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                        0x0000000000400852 <+85>
                        0x00000000000400855 <+88>:
                                                                                                                                   0x40088e <password+145>
0x201832(%rip),%rax
                        0x00000000000400857 <+90>:
                                                                                                                                                                                                                # 0x602090 <o>
                        0x000000000040085e <+97>:
0x00000000000400861 <+100>:
                                                                                                              mov
callq
                                                                                                                                   0x4008c4 <generate_password>
                        0x0000000000400866 <+105>:
0x00000000000400869 <+108>:
                                                                                                                                   %rax.%rdx
                                                                                                                                   0x201848(%rip).%rcx
                                                                                                                                                                                                                # 0x6020b8 
# 0x602098 <s>
                        0x00000000000400870 <+115>:
                                                                                                                                   0x201821(%rip),%rax
                        0x00000000000400877 <+122>:
                                                                                                                                   %rcx.%rsi
                        0x0000000000040087a <+125>:
                                                                                                                                   %rax.%rdi
                        0x0000000000040087d <+128>:
                                                                                                                                   $0x0.%eax
                        0x00000000000400882 <+133>:
                                                                                                              callo
                                                                                                                                  0x400680 <printf@plt>
                       0x00000000000400887 <+138>:
                                                                                                                                   $0x1.%eax
                      0x000000000400887 <+1385:
0x0000000000400882 <+1435:
0x00000000000400882 <+1455:
0x0000000000400883 <+1555:
0x0000000000400839 <+1565:
0x000000000400839 <+1655:
0x000000000400833 <+1665:
0x0000000000400833 <+1665:
                                                                                                                                  0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                              j mp
mov
                                                                                                                                                                                                                # 0x6020b0 <f>
                                                                                                                                 %rax,%rdi
0x400650 <puts@plt>
                                                                                                              callq
                                                                                                              mov
leaveq
                                                                                                                                  $0x0,%eax
| Care | Color | Color
               End of assembler dump.
               (qdb) ni
                0x0000000000040088c 25
                                                                                                                                                                                                                # 0x6020a8 <r>
                                                                                                                                                                                                                # 0x6020a0 <d>
                                                                                                                                                                                                                # 0x602090 <o>
                                                                                                                                                                                                                # 0x6020b0 <f>
                                                                                                             # 0x6020a8 <r>
                                                                                                                                                                                                                # 0x6020a0 <d>
                                                                                                                                                                                                               # 0x602090 <n>
                                                                                                                                                                                                                # 0x6020b8 
# 0x602098 <s>
                                                                                                                                  # 0x6020b0 <f>
                         0x00000000000400895 <+152>:
                                                                                                                                 %rax,%rdi
0x400650 <puts@plt>
                      0x000000000400898 <+155>:
0x0000000000040089d <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                                                              calla
                                                                                                              mov
leaveq
                                                                                                                                  $0x0.%eax
               End of assembler dump.
                (adb) ni
                (gdb) ni
0x000000000004008a3 29
              in adb.c
                                                                                                                               issword:

%rbp

%rsp,%rbp

$0x10,%rsp

$0x0,-0x8(%rbp)

$0x0,%edi

0x4006d0 <time@plt>
                                                                                                                                 %eax,%edi
0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                                                 %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                        0x0000000000400822 <+37>:
0x00000000000400825 <+40>:
                                                                                                              mov
                                                                                                                                                                                                                # 0x6020a8 <r>
                                                                                                                                0x2018/c(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
                        0x000000000040082c <+40>:
0x0000000000040082c <+47>:
0x0000000000040082f <+50>:
0x00000000000400834 <+55>:
                                                                                                              callo
                                                                                                                                                                                                                # 0x6020a0 <d>
                                                                                                              mov
lea
                        0x0000000000040083b <+62>:
0x0000000000040083f <+66>:
```

```
        0x000000000400842
        <-605.</td>

        0x000000000400842
        <-725.</td>

        0x00000000000400844
        <-775.</td>

        0x000000000400854
        <-855.</td>

        0x000000000400855
        <-895.</td>

        0x0000000000400855
        <-895.</td>

        0x0000000000400855
        <-975.</td>

        0x0000000000400855
        <-975.</td>

        0x000000000400856
        <-105.</td>

        0x000000000400865
        <-105.</td>

        0x000000000400867
        <-1165.</td>

        0x0000000000400873
        <-1155.</td>

        0x0000000000400877
        <-1275.</td>

        0x0000000000400877
        <-1275.</td>

                                                                                                                                                                                  $0x0.%eax
                                                                                                                                                                                0x4006f0 <
                                                                                                                                                   callo
                                                                                                                                                                                                                                  isoc99 scanf@plt>
                                                                                                                                                                                   -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                                                                                                                                  0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                                                                                       # 0x602090 <o>
                                                                                                                                                                                   %rax,%rdi
                                                                                                                                                   calla
                                                                                                                                                                                  0x4008c4 <generate_password>
                                                                                                                                                                                   %rax.%rdx
                                                                                                                                                                                  0x201848(%rip).%rcx
                                                                                                                                                                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                   0x201821(%rip),%rax
               %rcx.%rsi
                                                                                                                                                                                   %rax.%rdi
                                                                                                                                                                                   $0x0.%eax
                                                                                                                                                   callo
                                                                                                                                                                                0x400680 <printf@plt>
                                                                                                                                                                                  $0x1.%eax
                                                                                                                                                                                0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                   j mp
mov
                                                                                                                                                                                                                                                                                                       # 0x6020b0 <f>
                                                                                                                                                                              %rax,%rdi
0x400650 <puts@plt>
                                                                                                                                                  callq
                                                                                                                                                  mov
leaveq
                                                                                                                                                                                $0x0,%eax
     End of assembler dump.
      (qdb) ni
       0x000000000004008b2 in main () at qdb.c:33
       33 in gdb.c
(gdb) disas
  | Company | Comp
                                                                                                                                                                                %rbp
%rsp,%rbp
                                                                                                                                                   mov $0x0,%eax
callq 0x4007fd <password>
                                                                                                                                                                                  %al,%al
0x4008bd <main+25>
                                                                                                                                                                                  $0x0,%eax
0x4008c2 <main+30>
                                                                                                                                                                                  $0x1,%eax
                                                                                                                                                                                  %rbp
     End of assembler dump.
(gdb) ni
0x000000000004008b4 33
in qdb.c
   Inferior 1 [process 63153] will be killed.
   Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cat secrets.txt
0. dETRIENAw==
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
  benoid: I will only tell you the secret password if you enter the random numbe 981461572
you lose:(
Dayte85@bhrumil:~/dpate85/hw2/puzzles$ gdb 1
GNU gdb (Ubuntu 7.7.1-eubuntu5-14.04.2) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPL93+: GNU GPL version 3 or later <a href="http://gnu.org/licenses/gpl.html">http://gnu.org/licenses/gpl.html</a>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying" and "show warranty" for details.
This GOB was configured as "x88.6 64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<a href="http://www.gnu.org/software/gdb/bug/>->"hind the GOB manual and other documentation resources online at:
<a href="http://www.gnu.org/software/gdb/documentation/>->">-</a>
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) b 1
Breakpoint 1 at 0x400805: file gdb.c, line 1.
       (adb) disas
     No frame selected.
      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
  (gdb) disas
Dump of assembler code for function password:
0x000000000004007fd <+0>: push %rbp
0x0000000000040007fc <+1>: mov %rsp,%r
0x00000000000400001 <+4>: su 50x10,%
0x000000000004000055 <+8>: movl 50x0,-0
0x000000000004000055 <+15>: mov 50x0, 40x0,-0
0x0000000000004000051 <+20>: callq 0x40060
                                                                                                                                              tion password:

push %rbp

mov %rsp,%rbp

sub $0x10,%rsp

movl $0x0,-0x8(%rbp)

mov $0x0,%edi

callq 0x4006d0 <time@plt>
```

0x00000000000400842 <+69>:

%rax.%rdi

```
0x00000000000400816 <+25>:
                                                                                                                                    %eax.%edi
               0x0000000000400816 <+25>:
0x0000000000400818 <+27>:
0x00000000000040081d <+32>:
0x000000000000400822 <+37>:
0x00000000000400825 <+40>:
0x00000000000400825 <+50>:
0x00000000000400827 <+50>:
                                                                                                              calla
                                                                                                                                   0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                              callo
                                                                                                                                    %eax.-0x4(%rbp)
                                                                                                                                    0x20187c(%rip),%rax
                                                                                                                                                                                                                         # 0x6020a8 <r>
                                                                                                                                    %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                              calla
                                                                                                             mov
lea
mov
mov
                0x00000000000400834 <+55>
                                                                                                                                                                                                                         # 0x6020a0 <d>
                0x000000000040083b <+62>:
0x0000000000040083f <+66>:
0x000000000000400842 <+69>:
0x000000000000400845 <+72>:
                                                                                                                                    %rdx.%rsi
                                                                                                                                    %rax.%rdi
              0x0000000000400845 <-77>:
0x000000000040084a <-77>:
0x0000000000040084a <-77>:
0x00000000000400852 <-885>:
0x000000000000400857 <-882-:
0x000000000000400857 <-995>:
0x000000000000400856 <-997>:
0x000000000000400856 <-195>:
0x00000000000400856 <-1105>:
0x00000000000400856 <-1105>:
0x00000000000400873 <-125>:
0x0000000000000400877 <-1225>:
0x0000000000000400877 <-125>:
                                                                                                              mov
callq
                                                                                                                                    $0x0.%eax
                                                                                                                                    0x4006f0 <
                                                                                                                                                                      isoc99 scanf@plt>
                                                                                                                                    0X4000T0 <___1S0C99_SCAN1
-0X8(%rbp),%eax
%eax,-0X4(%rbp)
0X40088e <password+145>
0X201832(%rip),%rax
                                                                                                              cmp
jne
                                                                                                                                                                                                                         # 0x602090 <o>
                                                                                                                                    %rax.%rdi
                                                                                                                                    0x4008c4 <generate password>
                                                                                                              callo
                                                                                                              mov
                                                                                                                                    %rax.%rdx
                                                                                                                                    0x201848(%rip),%rcx
                                                                                                              mov
                                                                                                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                                                    0x201821(%rip),%rax
                                                                                                                                    %rcx,%rsi
%rax,%rdi
                0x000000000040087a <+125>:
0x0000000000040087d <+128>:
                                                                                                              mov
                                                                                                                                    $0x0,%eax
                0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                              callq
                                                                                                                                    0x400680 <printf@plt>
                                                                                                                                    $0x1,%eax
                                                                                                                                    0x4008a2 <password+165>
0x20181b(%rip),%rax
                 0x000000000040088c <+143>:
                                                                                                              jmp
mov
                0x0000000000040088C <+1.43>:
0x000000000400886 <+1.52>:
0x00000000000400898 <+1.55>:
0x000000000000400894 <+1.65>:
0x000000000000400894 <+1.65>:
0x000000000000400832 <+1.65>:
0x000000000000400833 <+1.66>:
                                                                                                                                                                                                                         # 0x6020b0 <f>
                                                                                                                                    %rax,%rdi
0x400650 <puts@plt>
                                                                                                              callq
                                                                                                              mov
leaveq
                                                                                                                                    $0x0,%eax
        End of assembler dump.
        (gdb) ni
18 i
                                in qdb.c
       (gdb) ni
0x00000000000400811
                                                                                  18
                                                                                                            in qdb.c
        (gdb) ni
0x0000000000400816
                                                                                 18
                                                                                                            in qdb.c
        (gdb) ni
0x0000000000400818
   | Section | Sec
                                                                                                            in qdb.c
       0χυυυυς
(gdb) ni
10 in gdb.c
                                                                                                                                # 0x6020a8 <r>
                                                                                                                                                                                                                         # 0x6020a0 <d>
                                                                                                                                                                                                                         # 0x602090 <o>
                                                                                                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                         # 0x6020b0 <f>
# 0x6020a8 <r>
              # 0x6020a0 <d>
                                                                                                                                                                      isoc99 scanf@plt>
                                                                                                                                    0x4000T0 <___1soc99_scant
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                              mov
cmp
jne
mov
mov
                                                                                                                                                                                                                         # 0x602090 <o>
                                                                                                                                    %rax,%rdi
0x4008c4 <generate_password>
                                                                                                              callq
                                                                                                             mov
mov
mov
mov
mov
                                                                                                                                    %rax.%rdx
                                                                                                                                    %rax,%rux
0x201848(%rip).%rcx
                                                                                                                                                                                                                          # 0x6020b8 
# 0x602098 <s>
                0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                                                                    0x201821(%rip),%rax
                                                                                                                                    %rcx,%rsi
%rax,%rdi
                0x00000000040087a <+125>:
0x00000000000040087d <+128>:
0x00000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                                                    $0x0,%eax
0x400680 <printf@plt>
                                                                                                              calla
                                                                                                              mov
jmp
mov
                                                                                                                                    $0x1.%eax
                                                                                                                                    $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                0x0000000000440887 <+1382.
0x0000000000044088c <+143>:
0x0000000000044088e <+145>:
0x00000000000440895 <+152>:
                                                                                                                                                                                                                         # 0x6020b0 <f>
                                                                                                                                   %rax,%rdi
0x400650 <puts@plt>
                0x0000000000400898 <+155>:
0x0000000000040089d <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                                                              callo
                                                                                                                                    $0x0.%eax
                                                                                                              leaven
      End of assembler dump.
       (gdb) p $eax
$1 = 1111437705
```

```
in gdb.c
       (qdb) disas
     ssword:
%rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
                                                                                                                                            0x4006d0 <time@plt>
             0x00000000000400816 <+25>
                                                                                                                                             %eax.%edi
                                                                                                                                           %eax,%ed1
0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                                     calla
                                                                                                                     callo
                                                                                                                     mov
                                                                                                                                             %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                     mov
                                                                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                                            %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                     calla
                                                                                                                                                                                                                                       # 0x6020a0 <d>
                                                                                                                     mov
lea
                                                                                                                     mov
                                                                                                                                             %rdx.%rsi
                                                                                                                     mov
                                                                                                                                             %rax,%rdi
                                                                                                                                             $0x0,%eax
                                                                                                                     callq
                                                                                                                                            0x4006f0 <__isoc99_scanf@plt>
                                                                                                                     mov
                                                                                                                                             -0x8(%rbp),%eax
%eax,-0x4(%rbp)
               cmp
jne
                                                                                                                                             0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                       # 0x602090 <o>
                                                                                                                                              %rax,%rdi
                                                                                                                                             0x4008c4 <qenerate password>
                                                                                                                     callq
                                                                                                                     mov
                                                                                                                                             %rax,%rdx
                                                                                                                                             0x201848(%rip),%rcx
                                                                                                                     mov
                                                                                                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                                                                                                                                             0x201821(%rip),%rax
                                                                                                                     mov
                                                                                                                                             %rcx,%rsi
%rax,%rdi
                                                                                                                     mov
                                                                                                                                            $0x0,%eax
0x400680 <printf@plt>
                                                                                                                     callq
                                                                                                                                            $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                     mov
                                                                                                                     jmp
mov
                                                                                                                                                                                                                                       # 0x6020b0 <f>
                                                                                                                     mov
callq
                                                                                                                                           %rax,%rdi
0x400650 <puts@plt>
                                                                                                                     mov
leaveq
                                                                                                                                            $0x0,%eax
End of assembler dump.
(gdb) ni
0x0000000000040082c
                                                                                                                     in gdb.c
                                                                                                                                        assword:
%rbp
%rsp,%rbp
%rsp,%rbp
$8x10,%rsp
$8x10,%rsp
$8x10,-0x8(%rbp)
$8x0,-0x8(%rbp)
$8x0,-0x8(%rbp)
$8x0,%edi
0x400660 <ird>crandeplt>
0x400700 <randeplt>
0x400700 <randeplt>
%eax,-0x4(%rbp)
0x20187C(%rip),%rax # 0
%rax,%rdi
0x201855(%rip),%rax # 0
%rax,%rdi
$8x0,%eax
0x400676 <_irdo,%rax # 0
%rax,%rdi
$8x0,%eax
0x400676 <_irdo,%rax # 0
%rax,%rdi
0x400838 </rdo,%rax # 0
%rax,%rdi
0x400838 </rd>
%rax,%rdi
0x400810 <_irdo,%rax # 0
%rax,%rdi
0x201832(%rip),%rax # 0
%rax,%rdi
0x201832(%rip),%rax # 0
%rax,%rdi
0x201831(%rip),%rcx # 0
%rax,%rdi
                                                                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                                                                                                                                        # 0x6020a0 <d>
                                                                                                                                                                                                                                       # 0x602090 <o>
                                                                                                                                                                                                                                      # 0x6020b8 
                                                                                                                                          0x201821(%rip),%rdx%rcx,%rsi
%rcx,%rdi
%rax,%rdi
$0x0,%eax
0x4006600 <printf@plt>
50x1,%eax
0x400862 <password+165>
0x20181b(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
50x0,%eax
                                                                                                                                                                                                                                       # 0x6020h0 <f>
     | Ggdb | n1 | gdb c | c | gdb | | c | 
                                                                                                                                         ssword:
%rbp
%rsp,%rbp
$0x10,%rsp
$0x10,%rsp
$0x00,%edi
0x400600 <time@plt>
%eax,%edi
0x400600 <cramd@plt>
%eax,%edi
0x400700 <cramd@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax # 0
%rax,%rdi
0x40050 <puts@plt>
0x20187c(%rip),%rax # 0
%rax,%rdi
0x20185(%rip),%rax # 0
%rax,%rdi
0x201865(%rip),%rax # 0
%rax,%rdi
0x201865(%rip),%rax # 0
%rdx,%rsi
%rax,%rdi
$0x0,%eax
0x400670 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
                                                                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                    callq
mov
lea
mov
mov
mov
callq
                                                                                                                                                                                                                                       # 0x6020a0 <d>
               mov
cmp
jne
mov
mov
                                                                                                                                             -0x8(%rbp),%eax
%eax,-0x4(%rbp)
                                                                                                                                             0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                       # 0x602090 <o>
                 0x000000000040085; <+97>:
0x00000000000400861 <+100>:
0x00000000000400866 <+105>:
0x00000000000400869 <+108>:
                                                                                                                                             %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                     callo
                                                                                                                     mov
mov
mov
mov
mov
                                                                                                                                             %rax,%rdx
0x201848(%rip),%rcx
                                                                                                                                                                                                                                        # 0x6020b8 
# 0x602098 <s>
                  0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                                                                             0x201821(%rip).%rax
                                                                                                                                             %rcx,%rsi
%rax,%rdi
                 0x00000000040087a <+125>:
0x00000000000040087d <+128>:
0x00000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                                                             $0x0.%eax
                                                                                                                     calla
                                                                                                                                            0x400680 <printf@plt>
                                                                                                                    mov
jmp
mov
mov
                                                                                                                                             $0x1.%eax
                                                                                                                                             $0x1,%eax
0x4008a2 <password+165>
                  0x0000000000040088c <+143>:
                                                                                                                                                                                                                                       # 0x6020h0 <f>
                  0x0000000000040088e <+145>:
                                                                                                                                             0x20181b(%rip),%rax
                  0×00000000000400895 <+152>:
                                                                                                                                           %rax,%rdi
0x400650 <puts@plt>
                  0×00000000000400898 <+155>:
                                                                                                                     callo
                 0x00000000004400896 <+155>:
0x00000000000440089d <+160>:
0x0000000000044008a2 <+165>:
0x0000000000044008a3 <+166>:
                                                                                                                                            $0x0.%eax
                                                                                                                     leaved
```

End of assembler dump.

(gdb) ni

```
(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
                 | In the content of t
                             of assembler code for function password:
                                                                                                                                                                           %rbp
%rsp,%rbp
                                                                                                                                               sub
                                                                                                                                                                            $0x10.%rst
                                                                                                                                                                            $0x0.-0x8(%rbp)
                                                                                                                                                                            $0x0,%edi
                                                                                                                                               callq
                                                                                                                                                                           0x4006d0 <time@plt>
                                                                                                                                                                            %eax.%edi
                                                                                                                                               calla
                                                                                                                                                                           0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                                                               callo
                                                                                                                                               mov
                                                                                                                                                                            %eax.-0x4(%rbp)
                                                                                                                                                                            0x20187c(%rip),%rax
                                                                                                                                               mov
                                                                                                                                                                                                                                                                                         # 0x6020a8 <r>
                                                                                                                                                                          %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                               calla
                                                                                                                                                                                                                                                                                         # 0x6020a0 <d>
                                                                                                                                               mov
lea
                                                                                                                                               mov
                                                                                                                                                                            %rdx,%rsi
                                                                                                                                               mov
                                                                                                                                                                            %rax,%rdi
                                                                                                                                               mov
callq
                                                                                                                                                                            $0x0,%eax
                                                                                                                                                                           0x4006f0 <__isoc99_scanf@plt>
                    0x000000000400841 <-822:
0x000000000400852 <-865:
0x000000000400855 <-888:
0x0000000000400855 <-977:
0x00000000000400856 <-997:
0x00000000000400856 <-1055:
0x00000000000400856 <-1055:
0x000000000004008576 <-11055:
0x00000000000400877 <-1125:
0x00000000000400877 <-1125:
                                                                                                                                               mov
                                                                                                                                                                            -0x8(%rbp),%eax
                                                                                                                                               cmp
jne
                                                                                                                                                                            %eax,-0x4(%rbp)
                                                                                                                                                                           0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                                                                        # 0x602090 <o>
                                                                                                                                                                           %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                               callq
                                                                                                                                               mov
mov
                                                                                                                                                                            %rax,%rdx
                                                                                                                                                                            0x201848(%rip),%rcx
                                                                                                                                                                                                                                                                                          # 0x6020b8 
# 0x602098 <s>
                                                                                                                                               mov
                                                                                                                                                                            0x201821(%rip),%rax
                     mov
                                                                                                                                                                            %rcx,%rsi
                                                                                                                                               mov
                                                                                                                                                                            %rax,%rdi
                                                                                                                                                                            $0x0,%eax
0x400680 <printf@plt>
                                                                                                                                               callq
                                                                                                                                               mov
jmp
mov
                                                                                                                                                                           $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                                                                                                                                         # 0x6020b0 <f>
                                                                                                                                               mov
callq
                                                                                                                                                                          %rax,%rdi
0x400650 <puts@plt>
                                                                                                                                                                           $0x0,%eax
                                                                                                                                               mov
leaveq
         End of assembler dump.
(gdb) ni
0x000000000040083b 21
in gdb.c
                                                                                                                                                                      3ssword:
%rbp
%rsp,%rbp
$ssvord:
%rbp
%rsp,%rbp
$80x10,%rsp
$80x10,%rsp
$80x10,%rsp
$80x10,%rsp
$80x0,-0x8(%rbp)
$80x0,wedi
0x4006600 <ri>6xeax,%edi
0x4006600 <radeplt>
0x400760 <radeplt>
0x20187C(%rip),%rax # 0
%rax,%rdi
0x201855(%rip),%rax # 0
%rax,%rdi
9x201865(%rip),%rax # 0
%rax,%rdi
$80x0,%eax
0x400676 <_isoc99_scanf@plt>
-0x8(%rbp),%eax
%rax,%rdi
$80x0,%eax
0x400676 <_isoc99_scanf@plt>
-0x8(%rbp),%eax
%rax,%rdi
$80x0,%eax
0x201848(%rip),%rax # 0
%rax,%rdi
%rax,%rdi
$8x0,%eax
0x201848(%rip),%rax # 0
%x018121(%rip),%rax # 0
%x018121(%rip),%rax # 0
%x0201821(%rip),%rax # 0
%x0201848(%rip),%rax # 0
%x0201810(%rip),%rax # 0
%x0201810(%r
                                                                                                                                                                                                                                                                                         # 0x6020a8 <r>
                                                                                                                                                                                                                                                                                         # 0x6020a0 <d>
                                                                                                                                                                                                                                                                                        # 0x602090 <o>
                                                                                                                                                                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                                                                                         # 0x6020h0 <f>
 assword:
%rbp
%rsp,%rbp
$0x0,%rsp
$0x0,%rsp
$0x0,%edi
$0x4006d0 etime@plt>
%eax,%edi
$0x4006d0 erand@plt>
%eax,%edi
$0x4006d0 erand@plt>
%eax,%edi
$0x4006d0 erand@plt>
%eax,%edi
$0x40050 erand@plt>
%eax,%edi
$0x20187c(%rip),%rax
%rax,%rdi
$0x201855(%rip),%rax
%rdi
$0x0,%rsi
%rax,%rdi
$0x0,%eax
                                                                                                                                                                                                                                                                                         # 0x6020a8 <r>
                 # 0x6020a0 <d>
                                                                                                                                                                          $000,%eax
0x4006f0 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax # #
                                                                                                                                               callq
                                                                                                                                              mov
cmp
jne
mov
mov
                                                                                                                                                                                                                                                                                         # 0x602090 <o>
                                                                                                                                                                           %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                               calla
                                                                                                                                               mov
mov
mov
mov
mov
                                                                                                                                                                            %rax.%rdx
                                                                                                                                                                            0x201848(%rip).%rcx
                                                                                                                                                                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                       0x0000000000400870 <+115>:
0x00000000000400877 <+122>:
                                                                                                                                                                            0x201821(%rip),%rax
                                                                                                                                                                            %rcx,%rsi
%rax,%rdi
                       0x0000000000040087a <+125>:
                       0x0000000000040087d <+128>:
                                                                                                                                                                            $0x0.%eax
                       0x0000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                                                               calla
                                                                                                                                                                           0x400680 <printf@plt>
                                                                                                                                               mov
                                                                                                                                                                            $0x1.%eax
                                                                                                                                                                           0x4008a2 <password+165>
0x20181b(%rip),%rax
                       0x0000000000040088c <+143>:
0x0000000000040088e <+145>:
                                                                                                                                               j mp
mov
                                                                                                                                                                                                                                                                                         # 0x6020h0 <f>
                      0x00000000004400886 <+145>:
0x0000000000004400895 <+152>:
0x0000000000004400898 <+155>:
0x00000000000440089d <+160>:
                                                                                                                                                                          %rax,%rdi
0x400650 <puts@plt>
                                                                                                                                               callo
                                                                                                                                                                           $0x0.%eax
                      0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                                                                                               leaveg
```

```
(adb) ni
   0x00000000000400842
                                                           21
                                                                                         in adb.c
   (adb) ni
   (gdb) ni
0x00000000000400845 21
                                                                                         in adb.c
   (adb) ni
   (gdb) ni
0x0000000000040084a 21
                                                                                          in adb.c
  (gdb) disas
Dump of assembler code for function password:
         push
mov
                                                                                                             %rsp.%rbp
                                                                                           sub
                                                                                                              $0x10.%rsc
                                                                                            movl
                                                                                                               $0x0.-0x8(%rbp)
                                                                                                             $0x0,%edi
0x4006d0 <time@plt>
                                                                                           calla
         %eax.%edi
                                                                                           mov
callq
                                                                                                              0x4006a0 srand@plt>
0x400700 <rand@plt>
                                                                                           callo
                                                                                           mov
                                                                                                               %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                           mov
                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                             %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                           callq
                                                                                           mov
lea
                                                                                                                                                                                       # 0x6020a0 <d>
                                                                                           mov
                                                                                                               %rdx,%rsi
           0x00000000000400842 <+69>:
0x00000000000400845 <+72>:
                                                                                           mov
                                                                                                               %rax,%rdi
       $0x0,%eax
                                                                                                             0x4006f0 <_isoc99_scanf@plt>

-0x8(%rbp),%eax

%eax,-0x4(%rbp)

0x40088e <password+145>

0x201832(%rip),%rax
                                                                                           callq
                                                                                          mov
cmp
jne
mov
                                                                                                                                                                                       # 0x602090 <o>
                                                                                           mov
callq
                                                                                                               %rax,%rdi
0x4008c4 <generate_password>
                                                                                           mov
mov
                                                                                                               %rax,%rdx
                                                                                                              %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                                                                                                        # 0x6020b8 
# 0x602098 <s>
                                                                                           mov
                                                                                           mov
                                                                                                               %rcx,%rsi
                                                                                           mov
                                                                                                               %rax,%rdi
                                                                                           mov
callq
                                                                                                               $0x0,%eax
0x400680 <printf@plt>
                                                                                          mov
jmp
mov
                                                                                                              $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                                       # 0x6020b0 <f>
                                                                                                            %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                                                           mov
callq
                                                                                           mov
leaveq
End of assembler dump.
(gdb) ni
1111437705
                                                                                                           assword:
    %rbp, %rbp
    %rsp, %rbp
    $80.10, %rsp
    $80.10, %rsp

                                                                                                                                                                                       # 0x6020a8 <r>
                                                                                                                                                                                       # 0x6020a0 <d>
                                                                                                                                                                                       # 0x602090 <o>
                                                                                                                                                                                       # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                       # 0x6020b0 <f>
                                                                                                             %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
   0x000000000004008a3 <+ioc
End of assembler dump.
(gdb) ni
0x00000000000400852 22
                                                                                          in gdb.c
 0x0000000000400801 <+4>:
0x00000000000400805 <+8>:
0x000000000000400805 <+15>:
0x0000000000000400811 <+20>:
0x000000000000400816 <+25>:
0x000000000000400818 <+27>:
                                                                                                           0x400600 ctime@plt>
%eax,%edi
0x4006a0 crand@plt>
0x400700 crand@plt>
%eax,-0x4(%rbp)
0x20187c(%rip),%rax
%rax,%rdi
0x400650 <puts@plt>
0x201805(%rip),%rax
-0x8(%rbp),%rdx
%rdx,%rsi
%rdx,%rsi
                                                                                          callq
mov
callq
callq
mov
mov
callq
       # 0x6020a8 <r>
                                                                                          mov
lea
mov
mov
mov
callq
                                                                                                                                                                                       # 0x6020a0 <d>
                                                                                                               %rax,%rdi
                                                                                                              $0x0,%eax
0x4006f0 <__isoc99_scanf@plt>
                                                                                           mov
cmp
jne
mov
mov
                                                                                                               -0x8(%rbp).%eax
                                                                                                               %eax.-0x4(%rbp)
                                                                                                              0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                       # 0x602090 <o>
           %rax,%rdi
0x4008c4 <generate_password>
                                                                                           calla
                                                                                          mov
mov
mov
                                                                                                               %rax,%rdx
0x201848(%rip),%rcx
                                                                                                                                                                                        # 0x6020b8 
# 0x602098 <s>
                                                                                                               0x201821(%rip).%rax
           0×000000000000400877 <+122>:
                                                                                                               %rcx,%rsi
%rax,%rdi
           0×0000000000040087a <+125>:
           0×00000000000040087d <+128>:
                                                                                                              $0x0,%eax
0x400680 <printf@plt>
           0x00000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                           callo
                                                                                                               $0x1.%eax
                                                                                                             0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                           jmp
mov
           0x0000000000040088c <+143>:
0x0000000000040088e <+145>:
```

# 0x6020b0 <f>

End of assembler dump.

```
mov %rax,%rdi
callq 0x400650 <puts@plt>
                   0x00000000000400895 <+152>:
                   0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                                                                                                             mov
leaveq
                                                                                                                                                                          $0x0.%eax
     End of assembler dump.
        (adb) ni
        0x00000000000400855 22
                                                                                                                                             in adb.c
        (adb) disas
     Dump of assembler code for function password:
                push
mov
                                                                                                                                                                          %rbp
                                                                                                                                                                       %rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                                                                                                             sub
                                                                                                                                             movl
   ### STATES | STATES |
### ST
                                                                                                                                             calla
                                                                                                                                                                           %eax,%edi
                                                                                                                                             calla
                                                                                                                                                                          0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                                                                                                             callo
                                                                                                                                             mov
                                                                                                                                                                          %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                                                                                                                                                                                         # 0x6020a8 <r>
                                                                                                                                             mov
                                                                                                                                                                         %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                                                                                                             callq
                                                                                                                                             mov
lea
                                                                                                                                                                                                                                                                                         # 0x6020a0 <d>
                                                                                                                                             mov
                                                                                                                                                                           %rdx,%rsi
                                                                                                                                             mov
                                                                                                                                                                           %rax,%rdi
                                                                                                                                                                           $0x0,%eax
                                                                                                                                                                         50%0,%eax
0x4006f0 <_isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax # (
                                                                                                                                             callq
                                                                                                                                            mov
cmp
jne
                                                                                                                                                                                                                                                                                         # 0x602090 <o>
                                                                                                                                             mov
callq
                                                                                                                                                                           %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                                                          %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                                                                                                             mov
                                                                                                                                             mov
                                                                                                                                                                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                                                             mov
                                                                                                                                             mov
                                                                                                                                                                           %rcx,%rsi
%rax,%rdi
                                                                                                                                             mov
                                                                                                                                             mov
callq
                                                                                                                                                                          $0x0,%eax
0x400680 <printf@plt>
                                                                                                                                            mov
jmp
mov
                                                                                                                                                                          $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                                                                                                                                                                         # 0x6020b0 <f>
                                                                                                                                                                         %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                                                                                                             mov
callq
                                                                                                                                             mov
leaveq
   ### Recommended Re
                                                                                                                                                                      # 0x6020a8 <r>
                                                                                                                                                                                                                                                                                         # 0x6020a0 <d>
                                                                                                                                                                                                                                                                                         # 0x602090 <o>
                                                                                                                                                                                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                                                                                                                                         # 0x6020b0 <f>
                                                                                                                                                                         %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
        0x000000000004008a3 <+ioc
End of assembler dump.
(gdb) ni
0x0000000000040085e 23
in gdb.c
              # 0x6020a8 <r>
                                                                                                                                            mov
lea
mov
mov
mov
callq
                                                                                                                                                                                                                                                                                         # 0x6020a0 <d>
                                                                                                                                                                         %0x0,%eax
0x4006f0 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
                                                                                                                                            mov
cmp
jne
mov
mov
                                                                                                                                                                           %eax.-0x4(%rbp)
                                                                                                                                                                          0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                                                                                                                                                                                         # 0x602090 <o>
                                                                                                                                                                           %rax,%rdi
0x4008c4 <generate_password>
                                                                                                                                             calla
                                                                                                                                            mov
mov
mov
                                                                                                                                                                           %rax,%rdx
0x201848(%rip),%rcx
                                                                                                                                                                                                                                                                                           # 0x6020b8 
# 0x602098 <s>
                                                                                                                                                                           0x201821(%rip).%rax
                   0x00000000000400877 <+122>:
                                                                                                                                                                           %rcx,%rsi
%rax,%rdi
                    0×0000000000040087a <+125>:
                    0×00000000000040087d <+128>:
                                                                                                                                                                          $0x0,%eax
0x400680 <printf@plt>
                    0x00000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                                                                                                             callo
                                                                                                                                                                           $0x1.%eax
                                                                                                                                                                         0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                                             jmp
mov
                   0x0000000000040088c <+143>:
0x0000000000040088e <+145>:
                                                                                                                                                                                                                                                                                         # 0x6020b0 <f>
```

```
mov %rax,%rdi
callq 0x400650 <puts@plt>
        0x00000000000400895 <+152>:
        0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                            mov
leaveq
                                                                         $0x0.%eax
  End of assembler dump.
   (adb) ni
   0x00000000000400861 23
                                                            in adb.c
   (adb) disas
  Dump of assembler code for function password:
       push
mov
                                                                         %rbp
                                                                        %rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                            sub
                                                            movl
      calla
                                                                         %eax,%edi
                                                            calla
                                                                         0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                            callo
                                                            mov
                                                                         %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                         # 0x6020a8 <r>
                                                            mov
                                                                        %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                            callq
                                                            mov
lea
                                                                                                                         # 0x6020a0 <d>
                                                            mov
                                                                         %rdx,%rsi
                                                            mov
                                                                         %rax,%rdi
                                                                         $0x0,%eax
                                                                        50%0,%eax
0x4006f0 <_isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax # (
                                                            callq
                                                            mov
cmp
jne
                                                                                                                         # 0x602090 <o>
                                                            mov
callq
                                                                         %rax,%rdi
0x4008c4 <generate_password>
                                                                         %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                            mov
                                                            mov
                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                            mov
                                                            mov
                                                                         %rcx,%rsi
%rax,%rdi
                                                            mov
                                                            mov
callq
                                                                         $0x0,%eax
0x400680 <printf@plt>
                                                            mov
jmp
mov
                                                                         $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                         # 0x6020b0 <f>
                                                                        %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                            mov
callq
                                                            mov
leaveq
retq
   End of assembler dump.
(gdb) ni
0x00000000000400866 23
 in gdb.c
                                                                       # 0x6020a8 <r>
                                                                                                                         # 0x6020a0 <d>
                                                                                                                         # 0x602090 <o>
                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                                                                         # 0x6020b0 <f>
                                                                        %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
   0x000000000004008a3 <+ioc
End of assembler dump.
(gdb) ni
0x00000000000400869 23
in gdb.c
      0x000000000400822 <+13/5:
0x000000000400822 <+140:
0x000000000400822 <+40:
0x000000000400822 <+475:
0x000000000400823 <+50:
0x000000000400823 <+50:
0x000000000400823 <+50:
0x000000000400823 <+50:
0x000000000400824 <+50:
0x000000000400847 <+60:
0x0000000000400847 <+70:
0x0000000000400847 <+775:
0x0000000000400847 <+775:
0x0000000000400847 <+70:
0x0000000000400857 <+85:
0x0000000000400857 <+975:
0x0000000000400856 <+105:
0x0000000000400856 <+105:
0x0000000000400866 <+105:
0x0000000000400866 <+108:
0x00000000000400867 <+1185:
0x000000000000400887 <+1152:
                                                                                                                         # 0x6020a8 <r>
                                                            mov
lea
mov
mov
mov
callq
                                                                                                                         # 0x6020a0 <d>
                                                                        %0x0,%eax
0x4006f0 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
                                                            mov
cmp
jne
mov
mov
                                                                         %eax.-0x4(%rbp)
                                                                         0x40088e <password+145>
0x201832(%rip),%rax
                                                                                                                         # 0x602090 <o>
                                                                         %rax,%rdi
0x4008c4 <generate_password>
                                                            calla
                                                            mov
mov
mov
                                                                         %rax,%rdx
0x201848(%rip),%rcx
                                                                                                                         # 0x6020b8 
# 0x602098 <s>
                                                                         0x201821(%rip).%rax
        0×000000000000400877 <+122>:
                                                            mov
                                                                         %rcx,%rsi
%rax,%rdi
        0×0000000000040087a <+125>:
        0×00000000000040087d <+128>:
                                                                         $0x0,%eax
0x400680 <printf@plt>
        0x00000000000400882 <+133>:
0x00000000000400887 <+138>:
                                                            callo
                                                                         $0x1.%eax
                                                                        0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                            jmp
mov
        0x0000000000040088c <+143>:
0x0000000000040088e <+145>:
```

# 0x6020b0 <f>

```
mov %rax,%rdi
callq 0x400650 <puts@plt>
      0x00000000000400895 <+152>:
      0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                mov
leaveq
                                                         $0x0.%eax
  End of assembler dump.
  (adb) ni
  0x00000000000400870 23
                                                in adb.c
  (adb) disas
  Dump of assembler code for function password:
     push
mov
                                                         %rbp
                                                         %rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                sub
                                                movl
     calla
                                                          %eax,%edi
                                                calla
                                                         0x4006a0 <srand@plt>
0x400700 <rand@plt>
                                                callo
                                                mov
                                                         %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                               # 0x6020a8 <r>
                                                mov
                                                         %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                callq
                                                mov
lea
                                                                                               # 0x6020a0 <d>
                                                mov
                                                          %rdx,%rsi
                                                mov
                                                          %rax,%rdi
                                                          $0x0,%eax
                                                         50%0,%eax
0x4006f0 <_isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax # (
                                                callq
                                               mov
cmp
jne
                                                                                               # 0x602090 <o>
                                                mov
callq
                                                          %rax,%rdi
0x4008c4 <generate_password>
                                                         %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                mov
                                                mov
                                                                                               # 0x6020b8 
# 0x602098 <s>
                                                mov
                                                mov
                                                          %rcx,%rsi
%rax,%rdi
                                                mov
                                                mov
callq
                                                         $0x0,%eax
0x400680 <printf@plt>
                                               mov
jmp
mov
                                                         $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                               # 0x6020b0 <f>
                                                         %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
                                                mov
callq
                                                mov
leaveq
retq
  End of assembler dump.
(gdb) ni
0x00000000000400877 23
 in gdb.c
                                                        # 0x6020a8 <r>
                                                                                               # 0x6020a0 <d>
                                                                                               # 0x602090 <o>
                                                                                               # 0x6020b8 
# 0x602098 <s>
                                                                                               # 0x6020b0 <f>
                                                         %rax,%rdi
0x400650 <puts@plt>
$0x0,%eax
  0x0000000000004008a3 <+100
End of assembler dump.
(gdb) ni
0x00000000000040087a 23
in gdb.c
     # 0x6020a8 <r>
                                               mov
lea
mov
mov
mov
callq
                                                                                               # 0x6020a0 <d>
                                                         %0x0,%eax
0x4006f0 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
                                               mov
cmp
jne
mov
mov
                                                          %eax.-0x4(%rbp)
                                                         0x40088e <password+145>
0x201832(%rip),%rax
                                                                                               # 0x602090 <o>
                                                          %rax,%rdi
0x4008c4 <generate_password>
                                                calla
                                               mov
mov
mov
                                                          %rax,%rdx
0x201848(%rip),%rcx
                                                                                                # 0x6020b8 
# 0x602098 <s>
                                                          0x201821(%rip).%rax
      0×00000000000400877 <+122>:
                                                mov
                                                          %rcx,%rsi
%rax,%rdi
      0x00000000000040087a <+125>:
      0×00000000000040087d <+128>:
                                                         $0x0,%eax
0x400680 <printf@plt>
      0x00000000000400872 <+133>:
0x000000000000400887 <+138>:
                                                callo
                                                          $0x1.%eax
                                                         0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                jmp
mov
      0x0000000000040088c <+143>:
0x0000000000040088e <+145>:
                                                                                               # 0x6020b0 <f>
```

```
mov %rax,%rdi
callq 0x400650 <puts@plt>
       0x0000000000400895 <+152>:
       0x0000000000400898 <+155>:
0x000000000000400894 <+160>:
0x000000000004008a2 <+165>:
0x000000000004008a3 <+166>:
                                                             mov
leaveq
                                                                          $0x0.%eax
  End of assembler dump.
   (adb) ni
   0x0000000000040087d 23
                                                            in adb.c
      (adb) disas
  Dump of assembler code for function password:
                                                            push
mov
                                                                          %rbp
                                                                        %rbp
%rsp,%rbp
$0x10,%rsp
$0x0,-0x8(%rbp)
$0x0,%edi
0x4006d0 <time@plt>
                                                             sub
                                                             movl
                                                             calla
                                                                          %eax.%edi
                                                            calla
                                                                         0x4006a0 srand@plt>
0x400700 <rand@plt>
                                                             callo
                                                             mov
                                                                          %eax,-0x4(%rbp)
0x20187c(%rip),%rax
                                                                                                                          # 0x6020a8 <r>
                                                             mov
                                                                         %rax,%rdi
0x400650 <puts@plt>
0x201865(%rip),%rax
-0x8(%rbp),%rdx
                                                             callq
                                                             mov
lea
                                                                                                                          # 0x6020a0 <d>
                                                             mov
                                                                          %rdx,%rsi
                                                             mov
                                                                          %rax,%rdi
                                                                          $0x0,%eax
                                                                        $0x0,%eax
0x4006f0 <__isoc99_scanf@plt>
-0x8(%rbp),%eax
%eax,-0x4(%rbp)
0x40088e <password+145>
0x201832(%rip),%rax # (
                                                             callq
                                                             mov
                                                             cmp
jne
                                                                                                                          # 0x602090 <o>
                                                                          %rax,%rdi
0x4008c4 <generate_password>
                                                             callq
                                                                          %rax,%rdx
0x201848(%rip),%rcx
0x201821(%rip),%rax
                                                             mov
                                                             mov
                                                                                                                          # 0x6020b8 
# 0x602098 <s>
                                                             mov
                                                             mov
                                                                          %rcx,%rsi
%rax,%rdi
                                                             mov
                                                             mov
callq
                                                                         $0x0,%eax
0x400680 <printf@plt>
                                                            mov
jmp
mov
                                                                         $0x1,%eax
0x4008a2 <password+165>
0x20181b(%rip),%rax
                                                                                                                          # 0x6020b0 <f>
                                                            mov %rax,%rdi
callq 0x400650 <puts@plt>
mov $0x0,%eax
                                                            mov
leaveq
retq
  End of assembler dump.
(gdb) ni
0x000000000000400882 23
in gdb.c
                                                                       # 0x6020a8 <r>
                                                                                                                          # 0x6020a0 <d>
                                                                                                                          # 0x602090 <o>
                                                                                                                          # 0x6020b8 
# 0x602098 <s>
                                                                                                                          # 0x6020b0 <f>
               Inferior 1 [process 63200] will be killed.
 Quit anyway? (y or n) y
Dpate85@Dhrumil:-/dpate85/hw2/puzzles$ 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
  The 0 executable gave the answer right away. I just had to run the executable and it gave the secret right away!
  For this one. I had to:
  ror 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 Seax" 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\$