

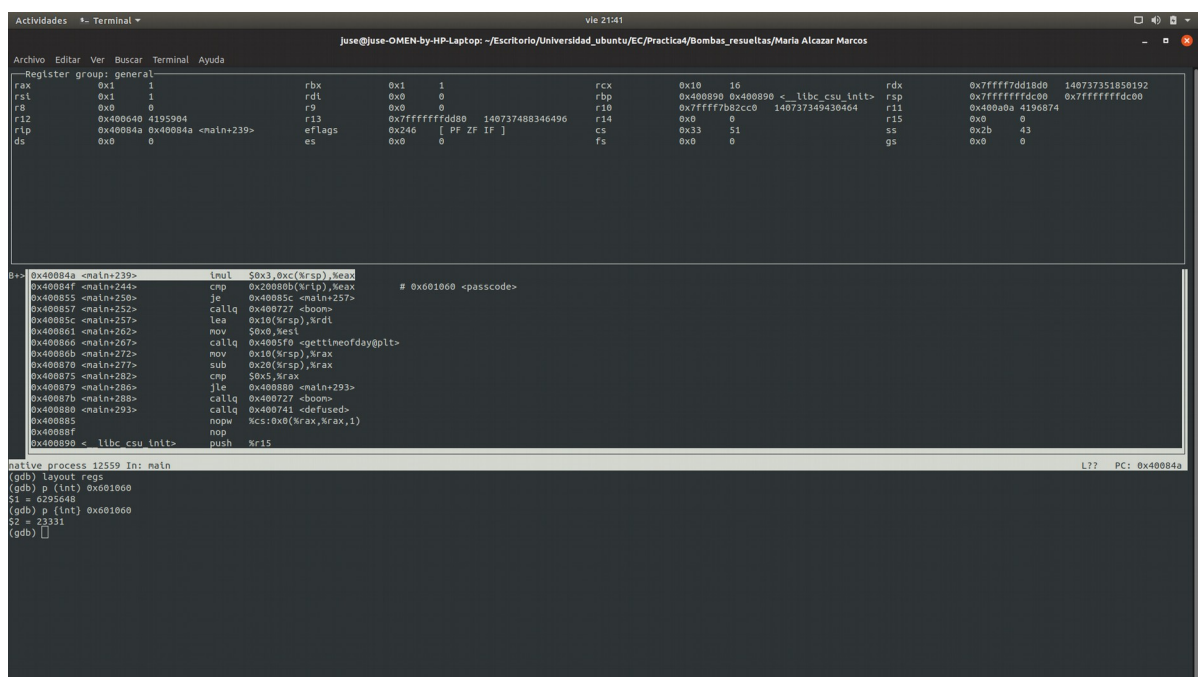
Practica 4: Bombas resueltas

- Bomba Alberto Villanueva Copado**

Contraseña:contrasenia Pincod:1221

Seguimos el mismo procedimiento de la anterior bomba, ponemos un `br *main` y `run`. Con `ni` llegamos hasta la dirección `0x400962` y observamos que el valor del registro `%rsi` es `contrasenia`.

Tras obtener la contraseña seguimos hasta la dirección `0x400a5e` y ahí se compara el pin, hacemos `p (int) $eax` y obtenemos `1221` que es el pincod



```
Actividades - Terminal - vie 21:41
juse@juse-OMEN-by-HP-Laptop: ~/Escritorio/Universidad_ubuntu/EC/Practica4/Bombas_resueltas/Maria Alcazar Marcos

--Register group: general--
rax      0x1      1      rbx      0x1      1      rcx      0x10     16      rdx      0x7ffffdd18d0  140737351850192
rsi      0x1      1      rdi      0x0      0      rbp      0x400890  0x400890 < libc_csu_init>  0x7ffffdfdc00
r8       0x0      0      r9       0x0      0      r10      0x7ffff7b2cc0  140737349430464
r12      0x400640  4195904  r13      0x7fffffd00  140737488346496
rip      0x40084a  0x40084a <main+239>  eflags   0x246     [ PF ZF IF ]
ds       0x0      0      fs       0x0      0      gs       0x0      0

0x40084a <main+239>    inul    $0x3,0xc(rsp),%eax
0x40084f <main+244>    cmp     0x200800(%rip),%eax
0x400855 <main+250>    je      0x40085c <main+257> # 0x01060 <passcode>
0x400857 <main+252>    callq  0x400727 <boom>
0x40085c <main+257>    lea     0x10(%rsp),%rdi
0x400861 <main+265>    mov     $0x0,%esi
0x400866 <main+267>    callq  0x4005f0 <gettimeofday@plt>
0x40086b <main+272>    mov     0x10(%rsp),%rax
0x400870 <main+277>    sub     0x20(%rsp),%rax
0x400875 <main+282>    cmp     $0x5,%rax
0x400879 <main+286>    jle     0x400880 <main+293>
0x40087b <main+288>    callq  0x400727 <boom>
0x400880 <main+293>    callq  0x400741 <defused>
0x400885    nopw    %cs:0x0(%rax,%rax,1)
0x40088f    nop
0x400890 < libc_csu_init> push    %r15

Native process 12559 in: main
(gdb) layout reg
(gdb) p (int) 0x01060
$1 = 6295648
(gdb) p (int) 0x01060
$2 = 23331
(gdb)
```