root@kali:~/Desktop/luckyguess# gdb LuckyGuess

```
root@kali:~/Desktop/luckyguess# gdb LuckyGuess
GNU gdb (Debian 8.2.1-2) 8.2.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from LuckyGuess...(no debugging symbols found)...done.
gdb-peda$
```

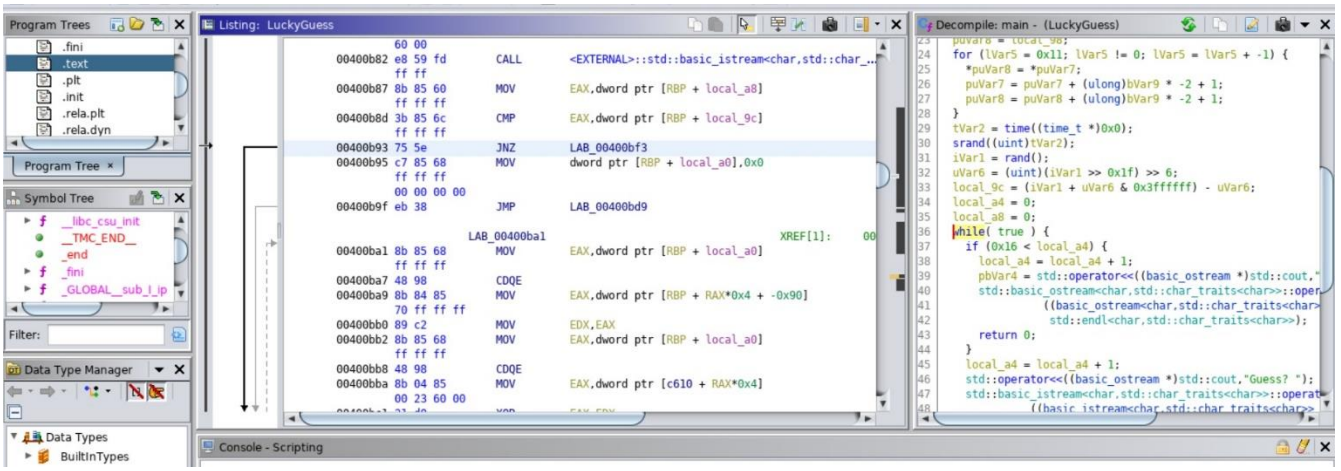
gdb-peda$ info files

```
gdb-peda$ info files
Symbols from "/root/Desktop/luckyguess/LuckyGuess".
Local exec file:
    `/root/Desktop/luckyguess/LuckyGuess', file type elf64-x86-64.
    Entry point: 0x400940
    0x0000000000400238 - 0x0000000000400254 is .interp
    0x0000000000400254 - 0x0000000000400274 is .note.ABI-tag
    0x0000000000400274 - 0x0000000000400298 is .note.gnu.build-id
    0x0000000000400298 - 0x00000000004002cc is .gnu.hash
    0x00000000004002d0 - 0x0000000000400498 is .dynsym
    0x0000000000400498 - 0x0000000000400655 is .dynstr
    0x0000000000400656 - 0x000000000040067c is .gnu.version
    0x0000000000400680 - 0x00000000004006c0 is .gnu.version_r
    0x00000000004006c0 - 0x0000000000400708 is .rela.dyn
    0x0000000000400708 - 0x0000000000400840 is .rela.plt
    0x0000000000400840 - 0x000000000040085a is .init
    0x0000000000400860 - 0x0000000000400940 is .plt
    0x0000000000400940 - 0x0000000000400d32 is .text
    0x0000000000400d34 - 0x0000000000400d3d is .fini
    0x0000000000400d40 - 0x0000000000400e08 is .rodata
    0x0000000000400e08 - 0x0000000000400e5c is .eh_frame_hdr
    0x0000000000400e60 - 0x0000000000400fd4 is .eh_frame
    0x0000000000601df8 - 0x0000000000601e08 is .init_array
    0x0000000000601e08 - 0x0000000000601e10 is .fini_array
    0x0000000000601e10 - 0x0000000000601e18 is .jcr
    0x0000000000601e18 - 0x0000000000601ff8 is .dynamic
    0x0000000000601ff8 - 0x0000000000602000 is .got
    0x0000000000602000 - 0x0000000000602080 is .got.plt
    0x0000000000602080 - 0x0000000000602090 is .data
    0x00000000006020a0 - 0x00000000006023e8 is .bss
gdb-peda$
```

gdb-peda$ b *0x0000000000400940

```
gdb-peda$ b *0x0000000000400940
Breakpoint 1 at 0x400940
gdb-peda$
```

gdb-peda$ r



讓 if (local_a8 == local_9c) break;執行成功跳出 while 迴圈，進入 for 迴圈得到 flag，修改 jnz 指令為 nop 指令。

gdb-peda$ set {char}0x0000000000400B93=0x74

gdb-peda$ c