step1-Prepare

1. Open a terminal, go to the directory:

```
$ cd ~/Lab/BOMB
```

2. Use gdb:

```
$ gdb bomb
```

3. Have a general view of all functions: (you can find the additional phase by doing it!)

```
$ info functions
```

step2-Defuse

(i). Make sure no bomb can be exploded

```
$ break explode_bomb
```

- When you run the program and type an incorrect answer, you will see something like this:

```
Breakpoint 1, 0x08049502 in explode_bomb ()
```

- You type: `$ kill`

gdb responds: `$ Kill the program being debugged? (y or n)`

you answer should be: `$ y`

step2-Defuse

(ii). Defuse you bombs one by one (Ex. phase 1)

- Disassemble:

```
$ disas phase_1
```

- Focus on constants, such $0x80497c0
- Guess what a function does by studying its name, such as <strings_not_equal>
- Examine the data

```
$print (char *) 0x80497c0
```

- gdb responds: “Public speaking is very easy.” and that is the answer!

Further information

- Please read the the writeup carefully.

  writeup.pdf tells you everything about the lab!

  Give special focus to “Hints”
- Please read gdbnotes-x86 carefully.

  In fact, you can defuse all the bombs using no more than 5 gdb commands. Don't be anxious!
- If you don't understand the assembly language, read the text book

  Branches (if, while, switch) & Procedure (recursion)