Debugging with GDB (GNU Debugger)

C Program (With Logical Error)

Problem Description

The program is intended to **calculate the sum of numbers from 0 to N**, but it contains an **incorrect loop condition**, resulting in a wrong output.

// sum_bug.c

```
#include<stdio.h>

int main()
{
int n=5,sum=0;
for(int i=0;i<=n;i++)  //logical error
{
sum+=i;
}
printf("\nSum = %d\n",sum);
return 0;
}
```

Expected Output

Sum = 15

Actual Output

Sum = 0

2.Compiling the Program with Debug Symbols

To enable debugging, compile the program using the -g option:

gcc -g sum_bug.c -o sum_bug

3.Starting GDB

Launch GDB with the compiled program:

gdb ./sum_bug

```
student@student-virtual-machine:~/programs$ gdb ./sum_bug
GNU gdb (Ubuntu 12.1-0ubuntu1~22.04.2) 12.1
Copyright (C) 2022 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:
<https://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 ./sum_bug...
(gdb)
```

4.Setting Breakpoints

Set a breakpoint at the beginning of the main() function:

break main
run

```
(gdb) break main
Breakpoint 1 at 0x1155: file sum_bug.c, line 7.
(gdb) start
Temporary breakpoint 2 at 0x1155: file sum_bug.c, line 7.
Starting program: /home/student/programs/sum_bug
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main () at sum_bug.c:7
7           int n=5,sum=0;
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/student/programs/sum_bug
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main () at sum_bug.c:7
7           int n=5,sum=0;
(gdb)
```

5.Inspecting Variable Values

Check the values of variables before the loop executes:

print n
print sum
print i

observing values:

- n = 5
- sum = 0
- i is uninitialized before loop execution

```
(gdb) print n
$1 = 0
(gdb) print sum
$2 = 0
(gdb) print i
No symbol "i" in current context.
```

6. Stepping Through the Program

Step line-by-line to observe program execution:

next
next

At the loop condition:

for (i = 0; i >= n; i++)

here we can see:

- 0 >= 5 is **false**
- The loop body is never executed

```
(gdb) next
8           for(int i=0;i>=n;i++) // logical error
(gdb) next
12          printf("%d",sum);
(gdb) next
13          return 0;
```

7.Identifying the Logical Error

Error Identified

The loop condition is incorrect.

```
i >= n   // incorrect
```

Correct Condition

```
i <= n
```

8.Corrected Program

// sum_fixed.c

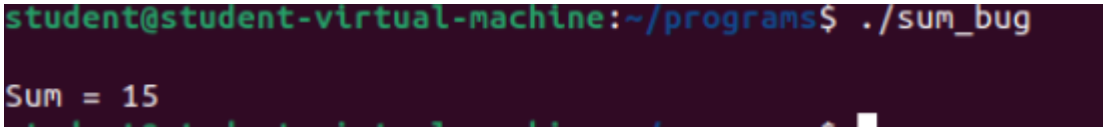
```
#include<stdio.h>

int main()
{
int n=5,sum=0;
for(int i=0;i<=n;i++)  //fixed
{
sum+=i;
}
printf("\nSum = %d\n",sum);
return 0;
}
```

9.Recompile and Verify

```
gcc -g sum_bug.c -o sum_bug
./sum_bug
```

Output

Sum = 15



Important GDB Commands Used

Command	Purpose
break main	Set breakpoint
run/start	Start program
next	Execute next line
print variable	Inspect variable

Command	Purpose
list	View source code
quit	Exit GDB