Module.2

Use Case 2: Debugging Null Pointer Dereference with Reverse Debugging

Overview

A null pointer dereference occurs when a program tries to access memory using a null pointer, causing a segmentation fault. Reverse debugging helps identify where the pointer was assigned a null value.

To find null pointer dereference which causing segmentation fault.

segmentation_fault_rd.c

```
#include <stdio.h>
#include <stdlib.h>

int main() {
   int *array = NULL;
   int n = 5;


   // Logical error: Conditional  that skips memory allocation
   if(n < 0){
      array = malloc(n * sizeof(int));
   }

   // Attempting to dereference a NULL pointer
   array[0] = 10; // Causes segmentation fault
   printf("Value at index 0: %d\n", array[0]);

   free(array); //Free allocated memory
   return 0;

}
```

Steps to debug with gdb to find segmentation fault:-

gcc -g -o segmentation_fault_rd segmentation_fault_rd.c

gdb ./ segmentation_fault_rd

break main

target record-full

run

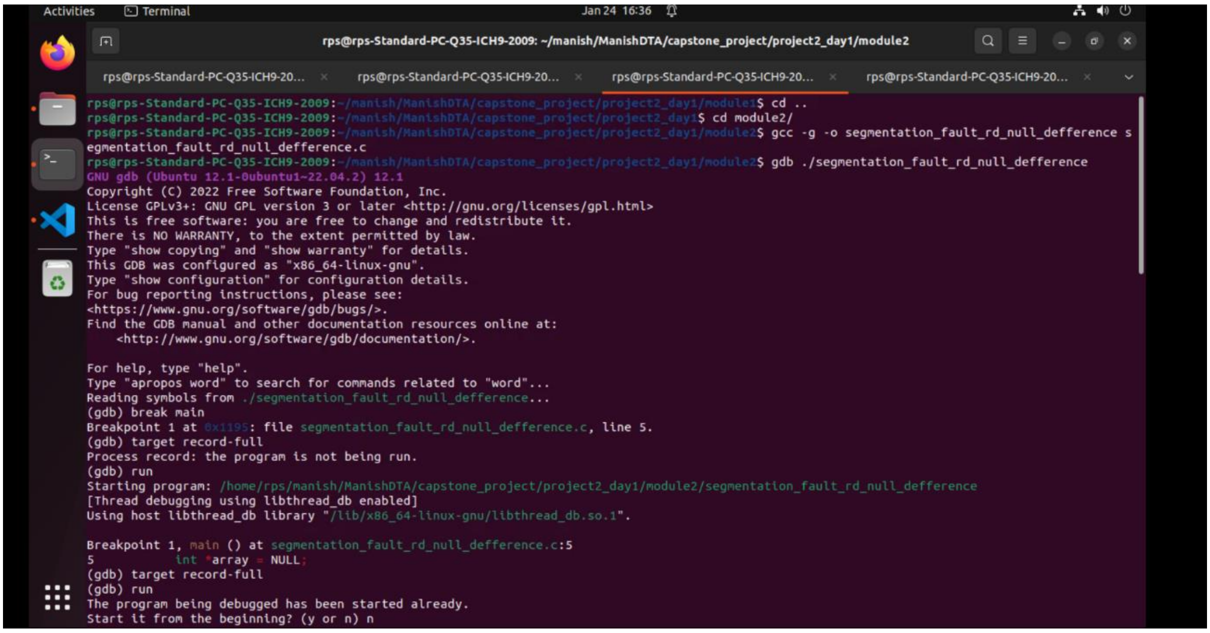
next

print array

print n

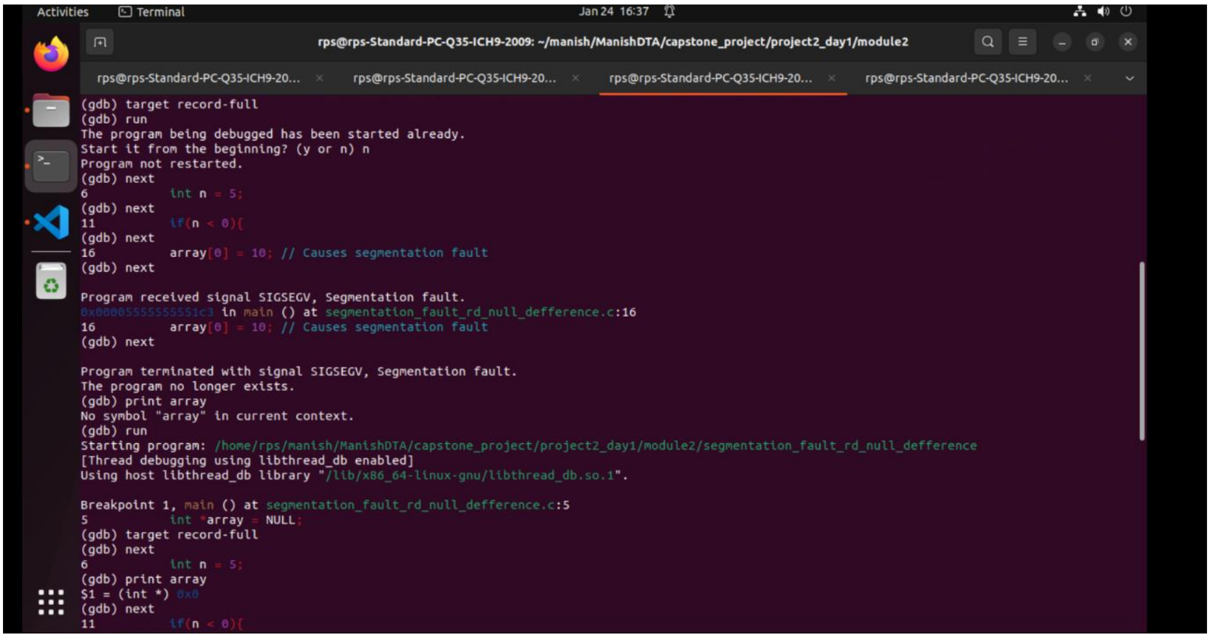
reverse-next

print array



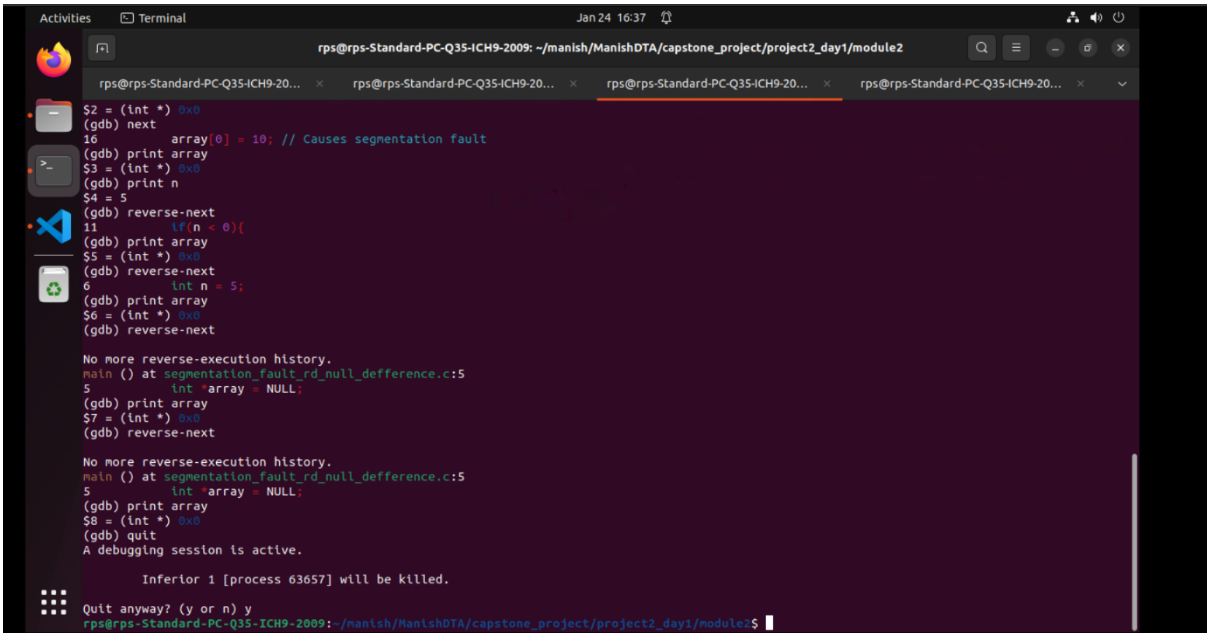
Activities
Terminal
Jan 24 16:36
rps@rps-Standard-PC-Q35-ICH9-2009: ~/manish/ManishDTA/capstone_project/project2_day1/module2
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...

```
rps@rps-Standard-PC-Q35-ICH9-2009:~/manish/ManishDTA/capstone_project/project2_day1/module1$ cd ..
rps@rps-Standard-PC-Q35-ICH9-2009:~/manish/ManishDTA/capstone_project/project2_day1$ cd module2/
rps@rps-Standard-PC-Q35-ICH9-2009:~/manish/ManishDTA/capstone_project/project2_day1/module2$ gcc -g -o segmentation_fault_rd_null_defference s
egmentation_fault_rd_null_defference.c
rps@rps-Standard-PC-Q35-ICH9-2009:~/manish/ManishDTA/capstone_project/project2_day1/module2$ gdb ./segmentation_fault_rd_null_defference
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 ./segmentation_fault_rd_null_defference...
(gdb) break main
Breakpoint 1 at 0x1195: file segmentation_fault_rd_null_defference.c, line 5.
(gdb) target record-full
Process record: the program is not being run.
(gdb) run
Starting program: /home/rps/manish/ManishDTA/capstone_project/project2_day1/module2/segmentation_fault_rd_null_defference
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main () at segmentation_fault_rd_null_defference.c:5
5           int *array = NULL;
(gdb) target record-full
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) n
```



Activities
Terminal
Jan 24 16:37
rps@rps-Standard-PC-Q35-ICH9-2009: ~/manish/ManishDTA/capstone_project/project2_day1/module2
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...

```
(gdb) target record-full
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) n
Program not restarted.
(gdb) next
6           int n = 5;
(gdb) next
11          if(n < 0){
(gdb) next
16          array[0] = 10; // Causes segmentation fault
(gdb) next

Program received signal SIGSEGV, Segmentation fault.
0x00005555555551c3 in main () at segmentation_fault_rd_null_defference.c:16
16          array[0] = 10; // Causes segmentation fault
(gdb) next

Program terminated with signal SIGSEGV, Segmentation fault.
The program no longer exists.
(gdb) print array
No symbol "array" in current context.
(gdb) run
Starting program: /home/rps/manish/ManishDTA/capstone_project/project2_day1/module2/segmentation_fault_rd_null_defference
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main () at segmentation_fault_rd_null_defference.c:5
5           int *array = NULL;
(gdb) target record-full
(gdb) next
6           int n = 5;
(gdb) print array
$1 = (int *) 0x0
(gdb) next
11          if(n < 0){
```



Activities
Terminal
Jan 24 16:37
rps@rps-Standard-PC-Q35-ICH9-2009: ~/manish/ManishDTA/capstone_project/project2_day1/module2
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...

```
$2 = (int *) 0x0
(gdb) next
16          array[0] = 10; // Causes segmentation fault
(gdb) print array
$3 = (int *) 0x0
(gdb) print n
$4 = 5
(gdb) reverse-next
11          if(n < 0){
(gdb) print array
$5 = (int *) 0x0
(gdb) reverse-next
6           int n = 5;
(gdb) print array
$6 = (int *) 0x0
(gdb) reverse-next

No more reverse-execution history.
main () at segmentation_fault_rd_null_defference.c:5
5           int *array = NULL;
(gdb) print array
$7 = (int *) 0x0
(gdb) reverse-next

No more reverse-execution history.
main () at segmentation_fault_rd_null_defference.c:5
5           int *array = NULL;
(gdb) print array
$8 = (int *) 0x0
(gdb) quit
A debugging session is active.

        Inferior 1 [process 63657] will be killed.

Quit anyway? (y or n) y
rps@rps-Standard-PC-Q35-ICH9-2009:~/manish/ManishDTA/capstone_project/project2_day1/module2$
```

Fixed segmentation fault which causing segmentation fault.

fixed_segmentation_fault_rd.c

```
#include <stdio.h>

#include <stdlib.h>
```

```
int main() {
   int *array = NULL;
   int n = 5;

   // Fixed Conditional to ensure proper memory allocation
   if(n > 0){
      array = malloc(n * sizeof(int));
   }
   else{
      printf("Invalid size.\n");
      return -1;
   }

   // Now safe to dereference the pointer
   array[0] = 10; // Causes segmentation fault
   printf("Value at index 0: %d\n", array[0]);

   free(array); //Free allocated memory
   return 0;

}
```

Steps to debug with gdb to find segmentation fault fixed or not:-

```
gcc -g -o fixed_segmentation_fault_rd fixed_segmentation_fault_rd.c
gdb ./ fixed_segmentation_fault_rd.c
break main
target record-full
run
next
print array
```

print n

next

print array[0]

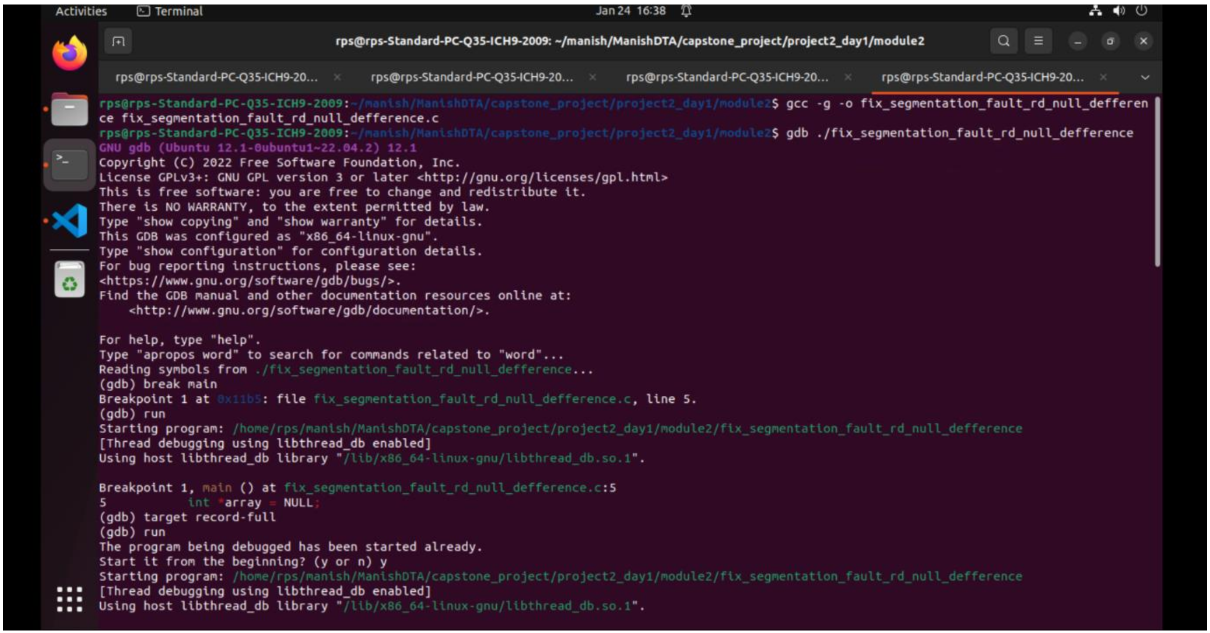
reverse-next

print array

continue

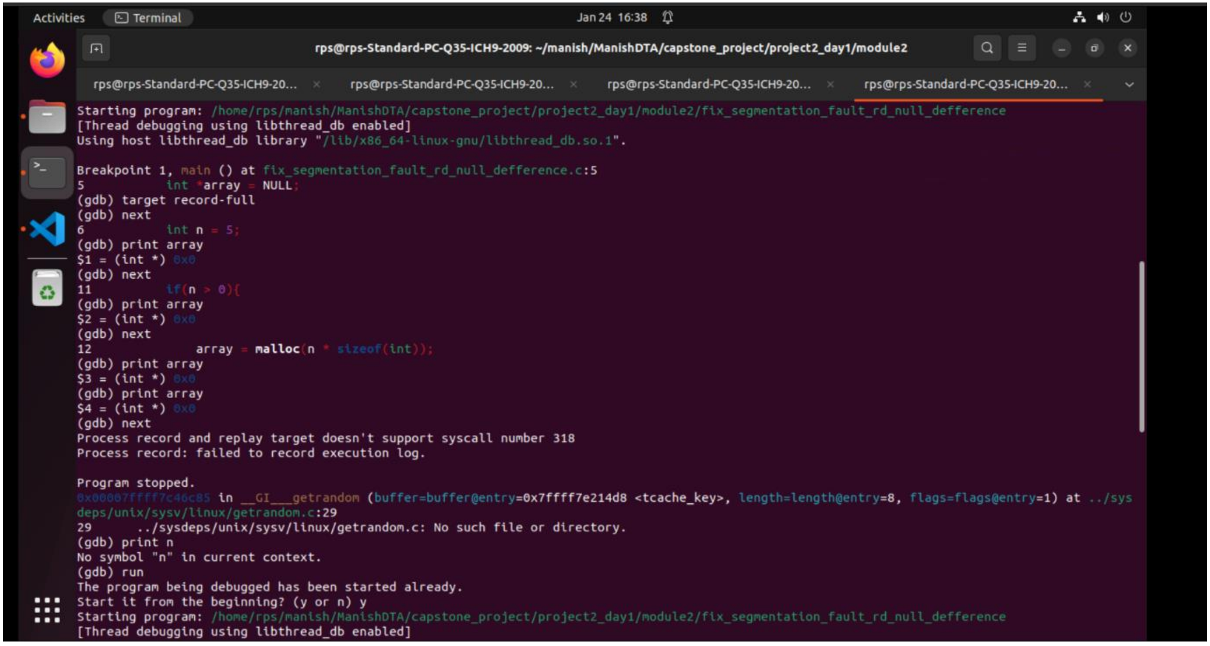
gcc -g -o fixed_segmentation_fault_rd.c

./ fixed_segmentation_fault_rd



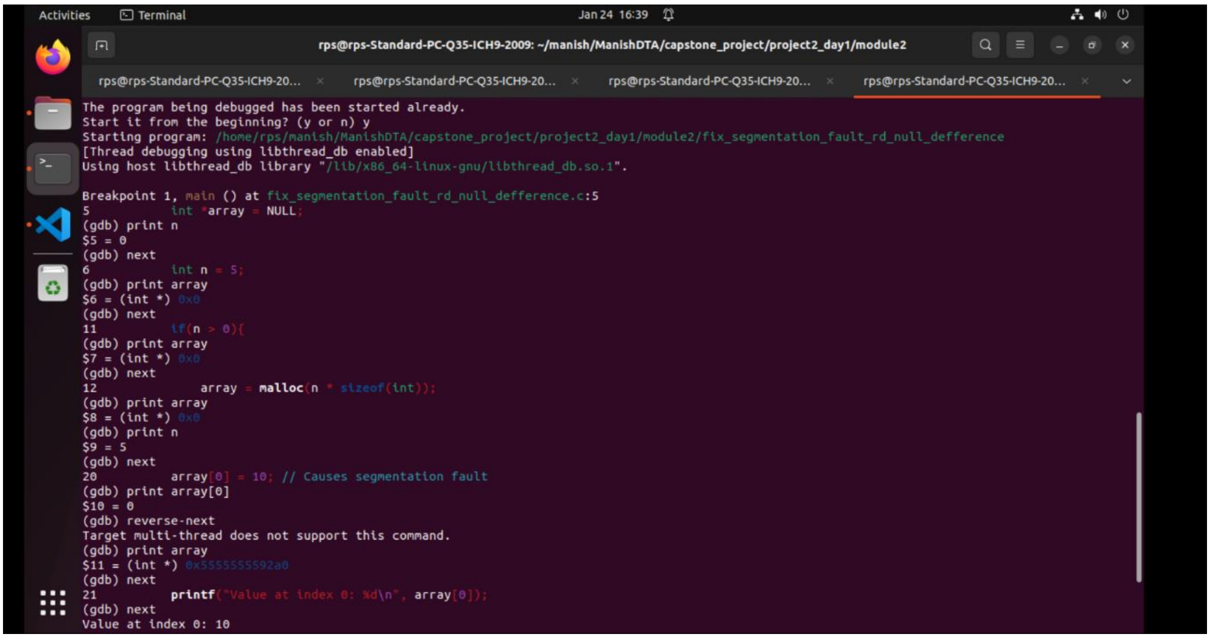
Activities
Terminal
Jan 24 16:38
rps@rps-Standard-PC-Q35-ICH9-2009: ~/manish/ManishDTA/capstone_project/project2_day1/module2
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...

```
rps@rps-Standard-PC-Q35-ICH9-2009:~/manish/ManishDTA/capstone_project/project2_day1/module2$ gcc -g -o fix_segmentation_fault_rd_null_defferen
ce fix_segmentation_fault_rd_null_defference.c
rps@rps-Standard-PC-Q35-ICH9-2009:~/manish/ManishDTA/capstone_project/project2_day1/module2$ gdb ./fix_segmentation_fault_rd_null_defference
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 ./fix_segmentation_fault_rd_null_defference...
(gdb) break main
Breakpoint 1 at 0x11b5: file fix_segmentation_fault_rd_null_defference.c, line 5.
(gdb) run
Starting program: /home/rps/manish/ManishDTA/capstone_project/project2_day1/module2/fix_segmentation_fault_rd_null_defference
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main () at fix_segmentation_fault_rd_null_defference.c:5
5           int *array = NULL;
(gdb) target record-full
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/rps/manish/ManishDTA/capstone_project/project2_day1/module2/fix_segmentation_fault_rd_null_defference
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
```

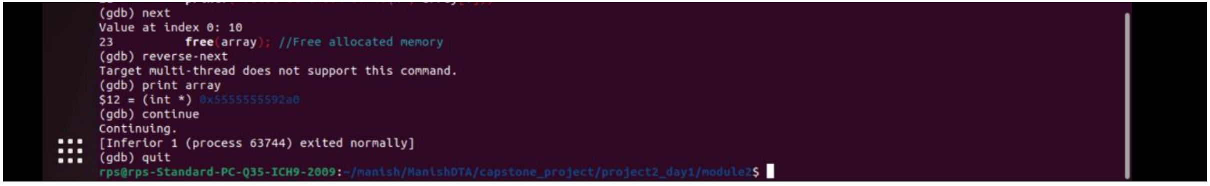


Activities
Terminal
Jan 24 16:38
rps@rps-Standard-PC-Q35-ICH9-2009: ~/manish/ManishDTA/capstone_project/project2_day1/module2
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...

```
Starting program: /home/rps/manish/ManishDTA/capstone_project/project2_day1/module2/fix_segmentation_fault_rd_null_defference
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main () at fix_segmentation_fault_rd_null_defference.c:5
5           int *array = NULL;
(gdb) target record-full
(gdb) next
6           int n = 5;
(gdb) print array
$1 = (int *) 0x0
(gdb) next
11          if(n > 0){
(gdb) print array
$2 = (int *) 0x0
(gdb) next
12              array = malloc(n * sizeof(int));
(gdb) print array
$3 = (int *) 0x0
(gdb) print array
$4 = (int *) 0x0
(gdb) next
Process record and replay target doesn't support syscall number 318
Process record: failed to record execution log.

Program stopped.
0x00007ffff7c46c85 in __GI___getrandom (buffer=buffer@entry=0x7ffff7e214d8 <tcache_key>, length=length@entry=8, flags=flags@entry=1) at ../sys
deps/unix/sysv/linux/getrandom.c:29
29      ../sysdeps/unix/sysv/linux/getrandom.c: No such file or directory.
(gdb) print n
No symbol "n" in current context.
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/rps/manish/ManishDTA/capstone_project/project2_day1/module2/fix_segmentation_fault_rd_null_defference
[Thread debugging using libthread_db enabled]
```


Activities
Terminal
Jan 24 16:39
rps@rps-Standard-PC-Q35-ICH9-2009: ~/manish/ManishDTA/capstone_project/project2_day1/module2
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...
rps@rps-Standard-PC-Q35-ICH9-20...

```
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/rps/manish/ManishDTA/capstone_project/project2_day1/module2/fix_segmentation_fault_rd_null_defference
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main () at fix_segmentation_fault_rd_null_defference.c:5
5           int *array = NULL;
(gdb) print n
$5 = 0
(gdb) next
6           int n = 5;
(gdb) print array
$6 = (int *) 0x0
(gdb) next
11          if(n > 0){
(gdb) print array
$7 = (int *) 0x0
(gdb) next
12              array = malloc(n * sizeof(int));
(gdb) print array
$8 = (int *) 0x0
(gdb) print n
$9 = 5
(gdb) next
20          array[0] = 10; // Causes segmentation fault
(gdb) print array[0]
$10 = 0
(gdb) reverse-next
Target multi-thread does not support this command.
(gdb) print array
$11 = (int *) 0x5555555592a0
(gdb) next
21          printf("Value at index 0: %d\n", array[0]);
(gdb) next
Value at index 0: 10
```



```
(gdb) next
Value at index 0: 10
23          free(array); //Free allocated memory
(gdb) reverse-next
Target multi-thread does not support this command.
(gdb) print array
$12 = (int *) 0x5555555592a0
(gdb) continue
Continuing.
[Inferior 1 (process 63744) exited normally]
(gdb) quit
rps@rps-Standard-PC-Q35-ICH9-2009:~/manish/ManishDTA/capstone_project/project2_day1/module2$ 
```