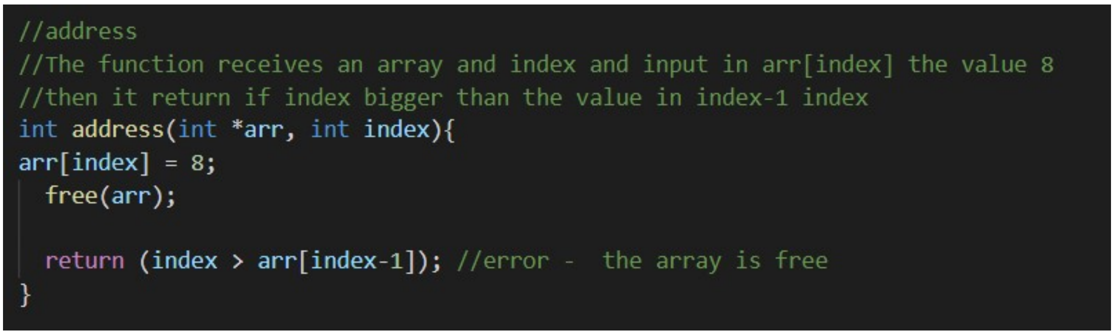
README for C part

gcc version 7.4.0

In this part I wrote a c-program including 4 functions each demonstrating a different issue of flagged by GCC-sanitizer.

This tool helps us to detect errors on run-time.

First function: address

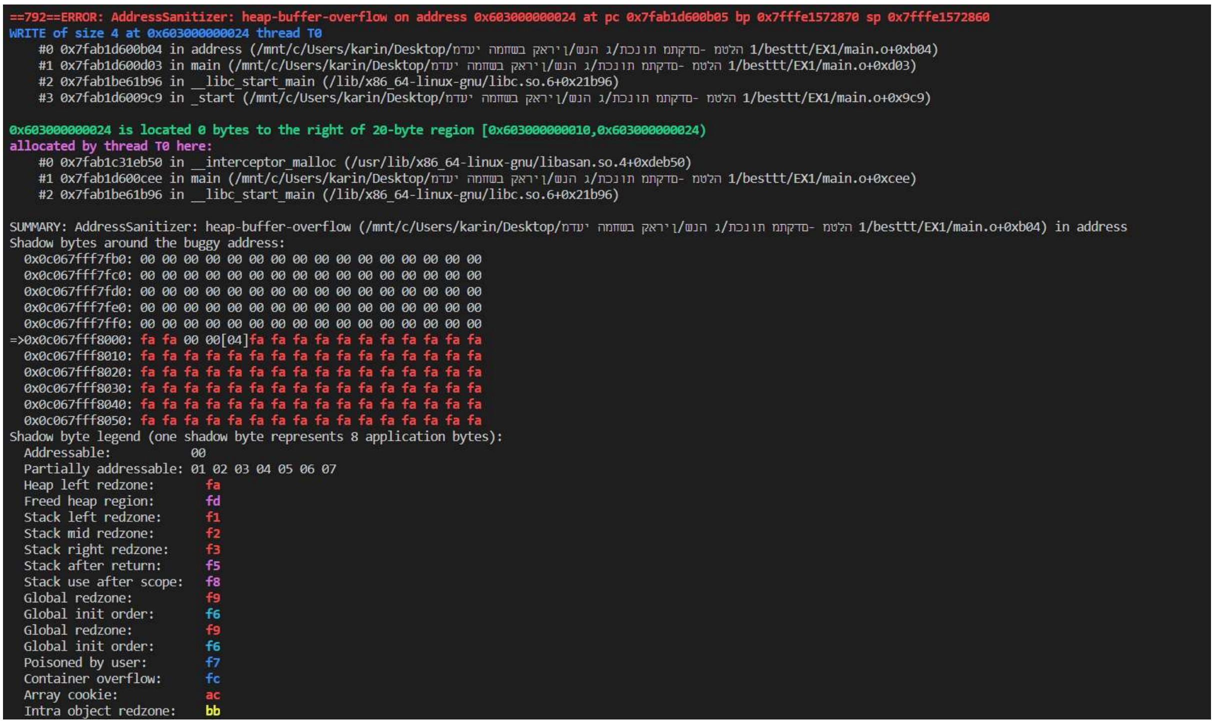


```
//address
//The function receives an array and index and input in arr[index] the value 8
//then it return if index bigger than the value in index-1 index
int address(int *arr, int index){
arr[index] = 8;
  free(arr);

  return (index > arr[index-1]); //error -  the array is free
}
```

In this function you can see that I tried to access a place in the array after I released it.

When I compile the file (gcc -fsanitize=address main.c -o main.o) and run it , I got this massage which means that I tried to access a place that doesn't exist.

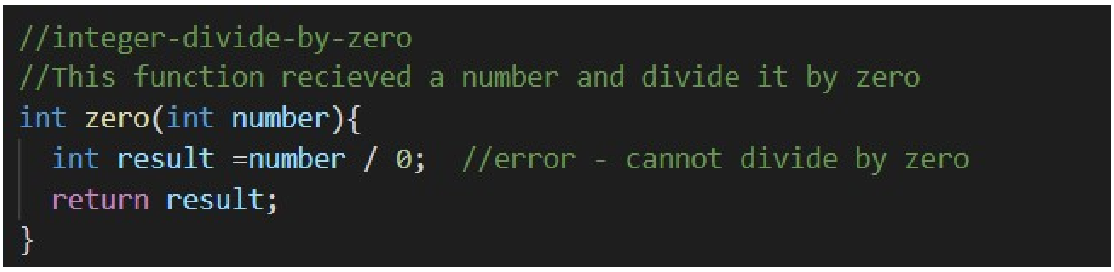


```
==792==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000024 at pc 0x7fab1d600b05 bp 0x7fffe1572870 sp 0x7fffe1572860
WRITE of size 4 at 0x603000000024 thread T0
    #0 0x7fab1d600b04 in address (/mnt/c/Users/karin/Desktop/יעדמ המחשב ןיראק/הנש ג/תוכנת מתקדם- הלטמ 1/besttt/EX1/main.o+0xb04)
    #1 0x7fab1d600d03 in main (/mnt/c/Users/karin/Desktop/יעדמ המחשב ןיראק/הנש ג/תוכנת מתקדם- הלטמ 1/besttt/EX1/main.o+0xd03)
    #2 0x7fab1be61b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #3 0x7fab1d6009c9 in _start (/mnt/c/Users/karin/Desktop/יעדמ המחשב ןיראק/הנש ג/תוכנת מתקדם- הלטמ 1/besttt/EX1/main.o+0x9c9)

0x603000000024 is located 0 bytes to the right of 20-byte region [0x603000000010,0x603000000024)
allocated by thread T0 here:
    #0 0x7fab1c31eb50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
    #1 0x7fab1d600cee in main (/mnt/c/Users/karin/Desktop/יעדמ המחשב ןיראק/הנש ג/תוכנת מתקדם- הלטמ 1/besttt/EX1/main.o+0xcee)
    #2 0x7fab1be61b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/mnt/c/Users/karin/Desktop/יעדמ המחשב ןיראק/הנש ג/תוכנת מתקדם- הלטמ 1/besttt/EX1/main.o+0xb04) in address
Shadow bytes around the buggy address:
  0x0c067fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c067fff8000: fa fa 00 00[04]fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
```

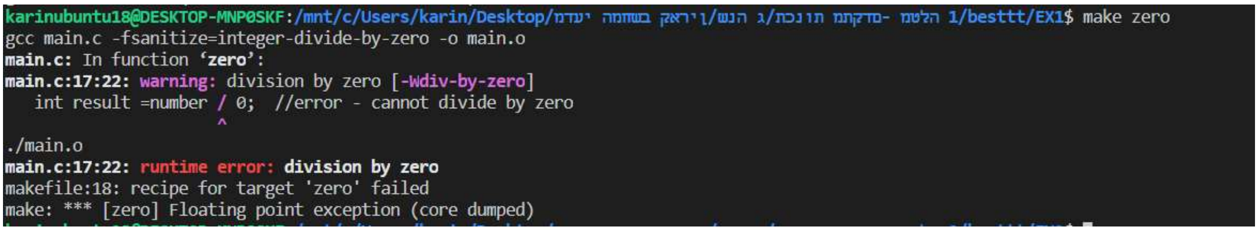
second function: integer-divide-by-zero



```
//integer-divide-by-zero
//This function recieved a number and divide it by zero
int zero(int number){
  int result =number / 0;  //error - cannot divide by zero
  return result;
}
```

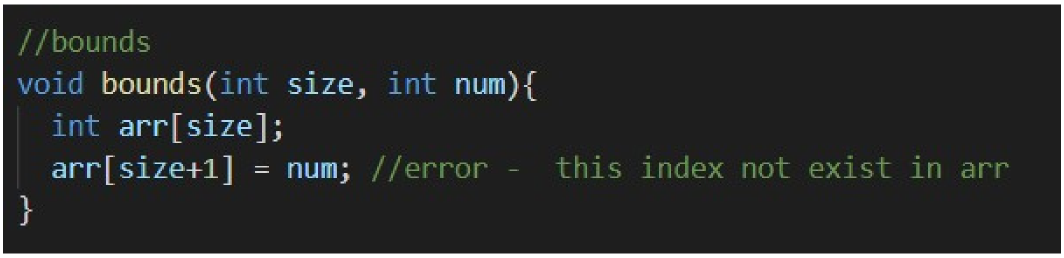
In this function I tried to divide a number by zero.

When I compile the file (gcc -fsanitize= integer-divide-by-zero main.c -o main.o) and run it I got this massage which means that I can't divide any number by zero.



```
karinubuntu18@DESKTOP-MNP0SKF:/mnt/c/Users/karin/Desktop/מדעי המחשב קארין/שנה ג/תוכנות מתקדם- מטלה 1/besttt/EX1$ make zero
gcc main.c -fsanitize=integer-divide-by-zero -o main.o
main.c: In function ‘zero’:
main.c:17:22: warning: division by zero [-Wdiv-by-zero]
   int result =number / 0;  //error - cannot divide by zero
                      ^
./main.o
main.c:17:22: runtime error: division by zero
makefile:18: recipe for target 'zero' failed
make: *** [zero] Floating point exception (core dumped)
```

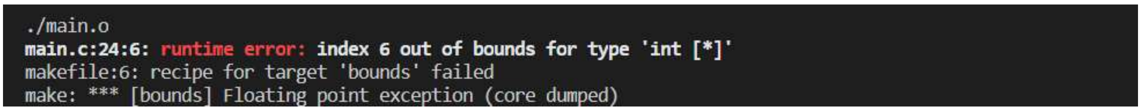
third function: bounds



```
//bounds
void bounds(int size, int num){
  int arr[size];
  arr[size+1] = num; //error -  this index not exist in arr
}
```

In this function I tried to access a place in an array that doesn’t exist, a position outside the array boundary.

When I compile the file (gcc -fsanitize= bounds main.c -o main.o) and run it I got this massage which means that I tried to access a position outside the array boundary.

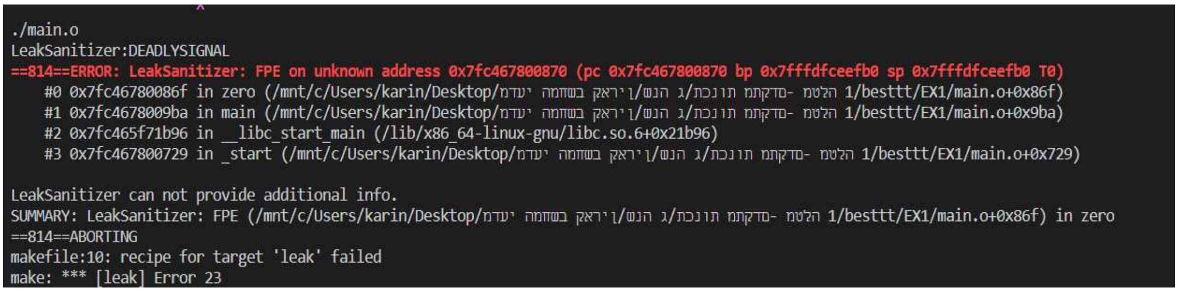


```
./main.o
main.c:24:6: runtime error: index 6 out of bounds for type 'int [*]'
makefile:6: recipe for target 'bounds' failed
make: *** [bounds] Floating point exception (core dumped)
```

fourth function: leak

In this function I assigned arrays, but I didn't release them all when I finished.

When I compile the file (gcc -fsanitize= leak main.c -o main.o) and run it I got this massage which means that there is a memory leak.



```
./main.o
LeakSanitizer:DEADLYSIGNAL
==814==ERROR: LeakSanitizer: FPE on unknown address 0x7fc467800870 (pc 0x7fc467800870 bp 0x7fffdfceefb0 sp 0x7fffdfceefb0 T0)
    #0 0x7fc46780086f in zero (/mnt/c/Users/karin/Desktop/מדעי המחשב בקראין/שנה ג/תכנות מתקדם- מטלה 1/besttt/EX1/main.o+0x86f)
    #1 0x7fc4678009ba in main (/mnt/c/Users/karin/Desktop/מדעי המחשב בקראין/שנה ג/תכנות מתקדם- מטלה 1/besttt/EX1/main.o+0x9ba)
    #2 0x7fc465f71b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #3 0x7fc467800729 in _start (/mnt/c/Users/karin/Desktop/מדעי המחשב בקראין/שנה ג/תכנות מתקדם- מטלה 1/besttt/EX1/main.o+0x729)

LeakSanitizer can not provide additional info.
SUMMARY: LeakSanitizer: FPE (/mnt/c/Users/karin/Desktop/מדעי המחשב בקראין/שנה ג/תכנות מתקדם- מטלה 1/besttt/EX1/main.o+0x86f) in zero
==814==ABORTING
makefile:10: recipe for target 'leak' failed
make: *** [leak] Error 23
```