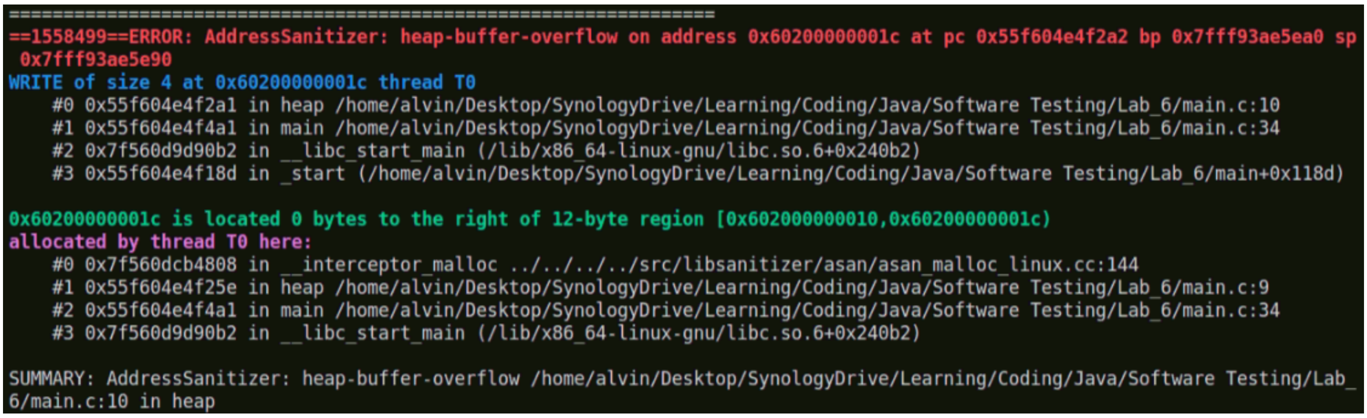
Heap out-of-bounds read/write

Code

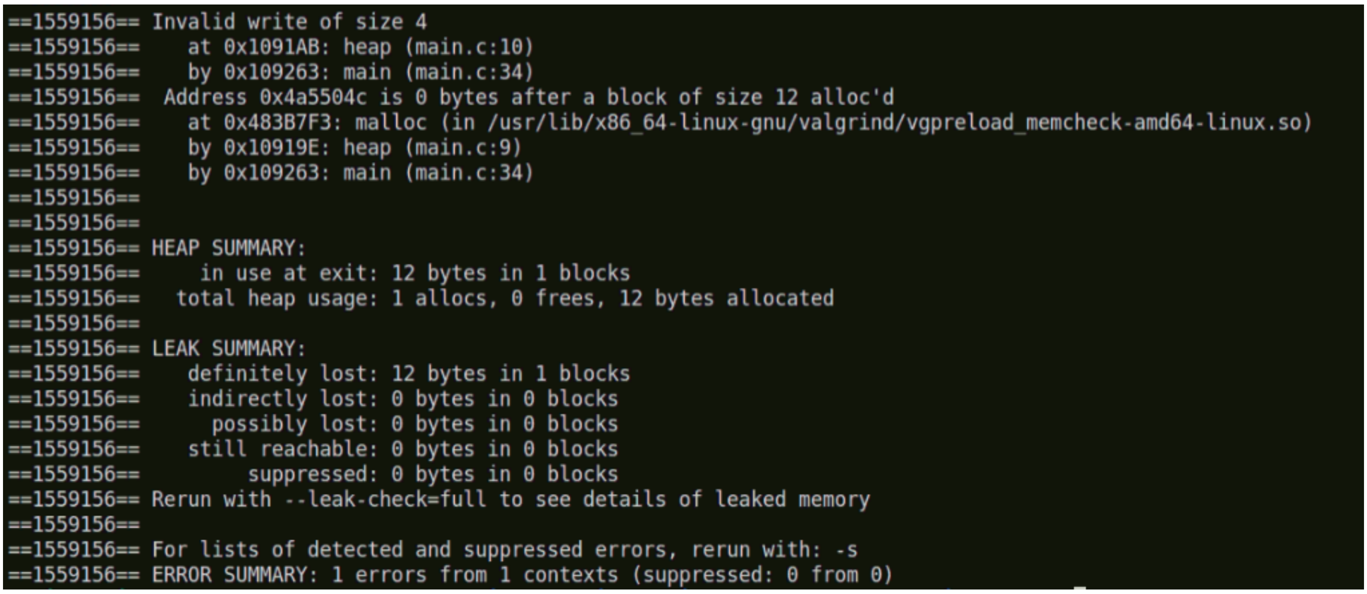
```
void heap(){
    int* a = malloc(sizeof(int)*3);
    a[3] = 0;
}
```

AScan Report



```
=================================================================
==1558499==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000001c at pc 0x55f604e4f2a2 bp 0x7fff93ae5ea0 sp
 0x7fff93ae5e90
WRITE of size 4 at 0x60200000001c thread T0
    #0 0x55f604e4f2a1 in heap /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:10
    #1 0x55f604e4f4a1 in main /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:34
    #2 0x7f560d9d90b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
    #3 0x55f604e4f18d in _start (/home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main+0x118d)

0x60200000001c is located 0 bytes to the right of 12-byte region [0x602000000010,0x60200000001c)
allocated by thread T0 here:
    #0 0x7f560dcb4808 in __interceptor_malloc ../../../../src/libsanitizer/asan/asan_malloc_linux.cc:144
    #1 0x55f604e4f25e in heap /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:9
    #2 0x55f604e4f4a1 in main /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:34
    #3 0x7f560d9d90b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_
6/main.c:10 in heap
```

Valgrind Report



```
==1559156== Invalid write of size 4
==1559156==    at 0x1091AB: heap (main.c:10)
==1559156==    by 0x109263: main (main.c:34)
==1559156==  Address 0x4a5504c is 0 bytes after a block of size 12 alloc'd
==1559156==    at 0x483B7F3: malloc (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==1559156==    by 0x10919E: heap (main.c:9)
==1559156==    by 0x109263: main (main.c:34)
==1559156==
==1559156==
==1559156== HEAP SUMMARY:
==1559156==     in use at exit: 12 bytes in 1 blocks
==1559156==   total heap usage: 1 allocs, 0 frees, 12 bytes allocated
==1559156==
==1559156== LEAK SUMMARY:
==1559156==    definitely lost: 12 bytes in 1 blocks
==1559156==    indirectly lost: 0 bytes in 0 blocks
==1559156==      possibly lost: 0 bytes in 0 blocks
==1559156==    still reachable: 0 bytes in 0 blocks
==1559156==         suppressed: 0 bytes in 0 blocks
==1559156== Rerun with --leak-check=full to see details of leaked memory
==1559156==
==1559156== For lists of detected and suppressed errors, rerun with: -s
==1559156== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

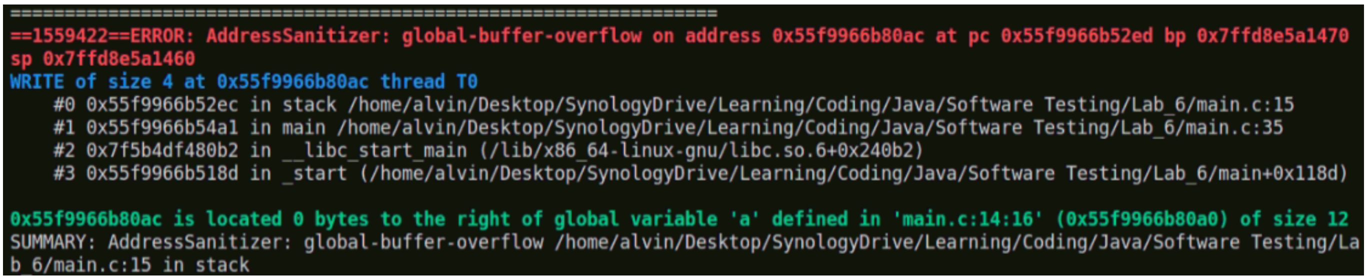
ASan✅ Valgrind✅

Stack out-of-bounds read/write

Code

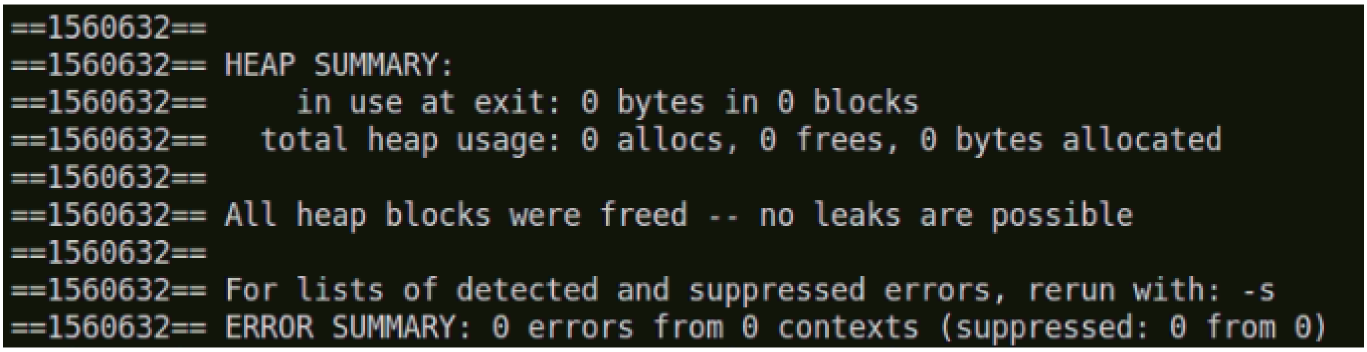
```
void stack() {
    static int a[3]={0};
    a[3] = 0;
}
```

AScan Report



```
==================================================================
==1559422==ERROR: AddressSanitizer: global-buffer-overflow on address 0x55f9966b80ac at pc 0x55f9966b52ed bp 0x7ffd8e5a1470
sp 0x7ffd8e5a1460
WRITE of size 4 at 0x55f9966b80ac thread T0
    #0 0x55f9966b52ec in stack /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:15
    #1 0x55f9966b54a1 in main /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:35
    #2 0x7f5b4df480b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
    #3 0x55f9966b518d in _start (/home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main+0x118d)

0x55f9966b80ac is located 0 bytes to the right of global variable 'a' defined in 'main.c:14:16' (0x55f9966b80a0) of size 12
SUMMARY: AddressSanitizer: global-buffer-overflow /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/La
b_6/main.c:15 in stack
```

Valgrind Report



```
==1560632==
==1560632== HEAP SUMMARY:
==1560632==     in use at exit: 0 bytes in 0 blocks
==1560632==   total heap usage: 0 allocs, 0 frees, 0 bytes allocated
==1560632==
==1560632== All heap blocks were freed -- no leaks are possible
==1560632==
==1560632== For lists of detected and suppressed errors, rerun with: -s
==1560632== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

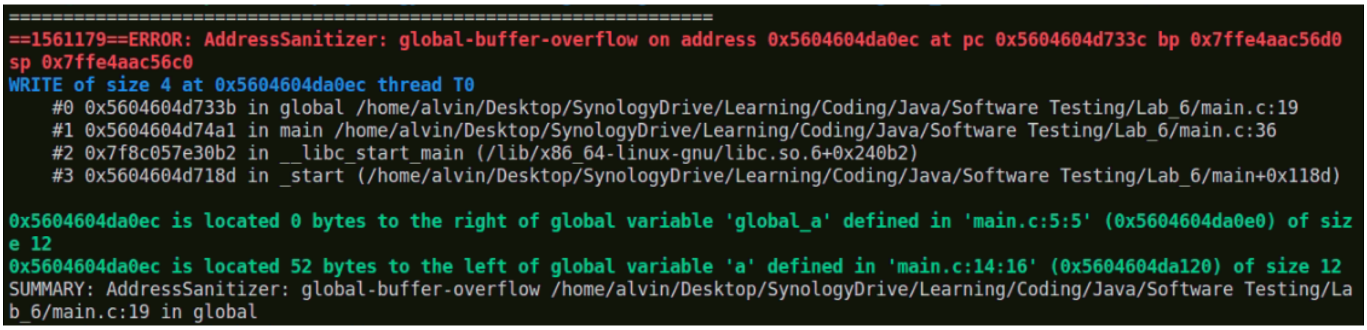
ASan✅ Valgrind❌

Global out-of-bounds read/write

Code

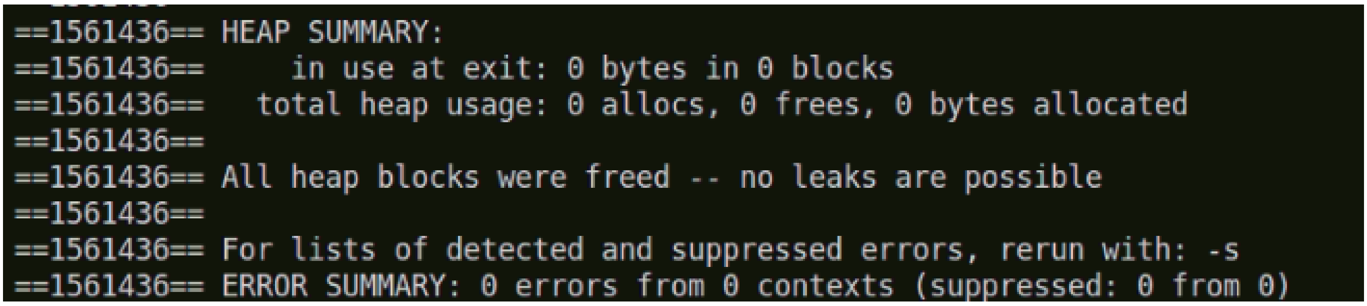
```
int global_a[3]={0};

void global(){
    global_a[3] = 0;
}
```

AScan Report



```
==================================================================
==1561179==ERROR: AddressSanitizer: global-buffer-overflow on address 0x5604604da0ec at pc 0x5604604d733c bp 0x7ffe4aac56d0
sp 0x7ffe4aac56c0
WRITE of size 4 at 0x5604604da0ec thread T0
    #0 0x5604604d733b in global /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:19
    #1 0x5604604d74a1 in main /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:36
    #2 0x7f8c057e30b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
    #3 0x5604604d718d in _start (/home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main+0x118d)

0x5604604da0ec is located 0 bytes to the right of global variable 'global_a' defined in 'main.c:5:5' (0x5604604da0e0) of siz
e 12
0x5604604da0ec is located 52 bytes to the left of global variable 'a' defined in 'main.c:14:16' (0x5604604da120) of size 12
SUMMARY: AddressSanitizer: global-buffer-overflow /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/La
b_6/main.c:19 in global
```

Valgrind Report



```
==1561436== HEAP SUMMARY:
==1561436==     in use at exit: 0 bytes in 0 blocks
==1561436==   total heap usage: 0 allocs, 0 frees, 0 bytes allocated
==1561436==
==1561436== All heap blocks were freed -- no leaks are possible
==1561436==
==1561436== For lists of detected and suppressed errors, rerun with: -s
==1561436== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

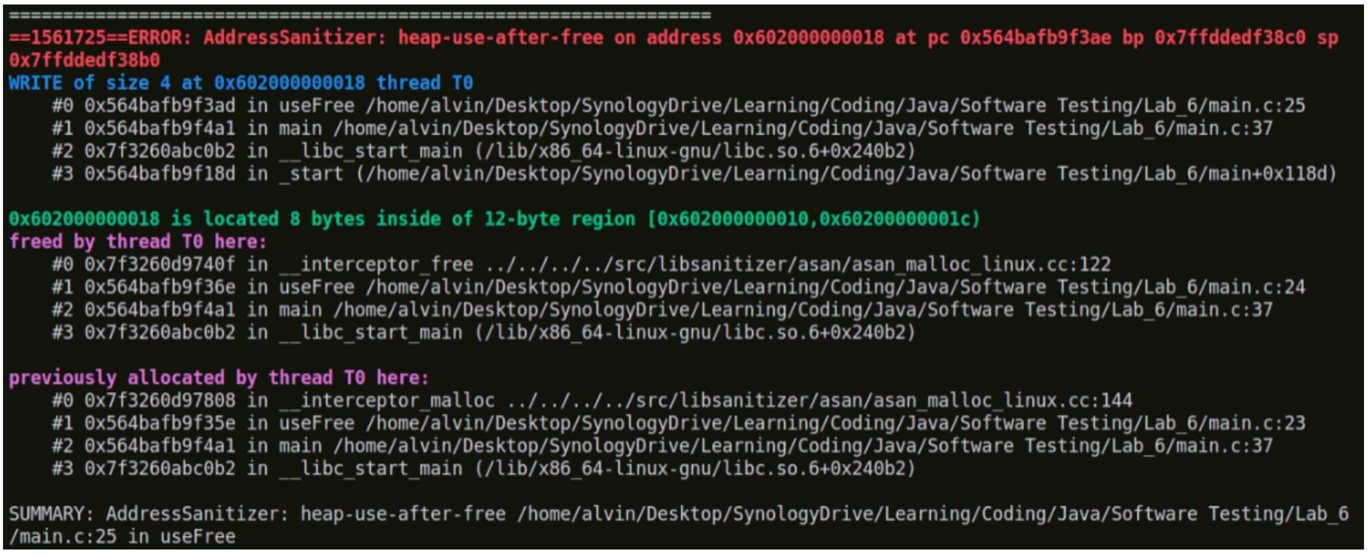
ASan✅ Valgrind❌

Use-after-free

Code

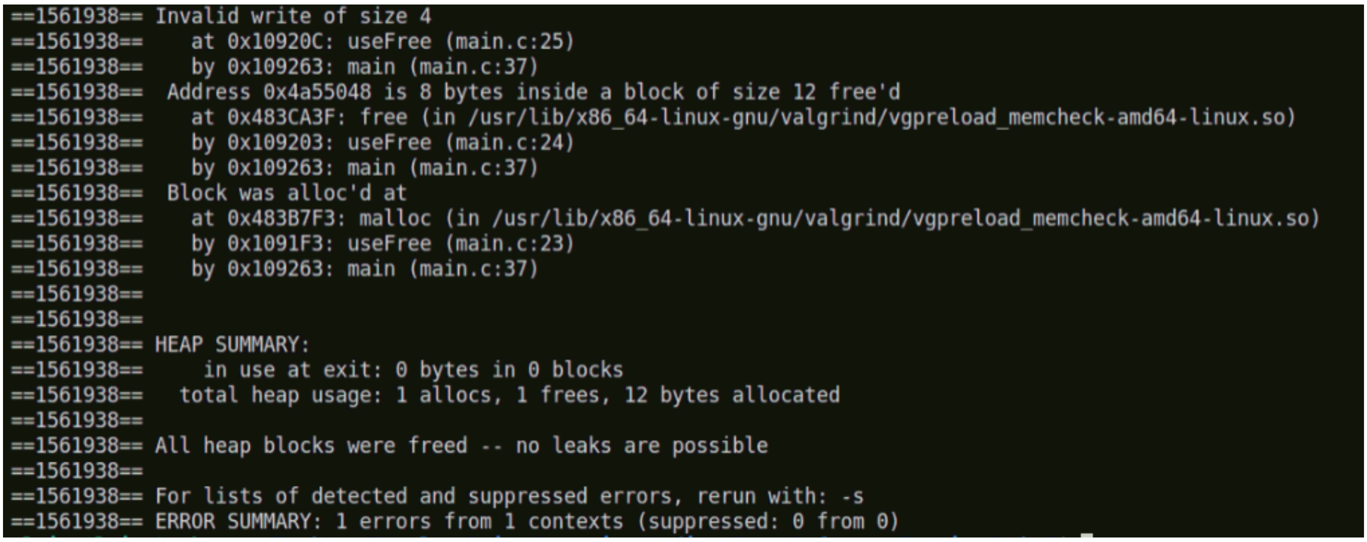
```
void useFree(){
    int* a = malloc(sizeof(int)*3);
    free(a);
    a[2] = 1;
}
```

AScan Report



```
=================================================================
==1561725==ERROR: AddressSanitizer: heap-use-after-free on address 0x602000000018 at pc 0x564bafb9f3ae bp 0x7ffddedf38c0 sp
0x7ffddedf38b0
WRITE of size 4 at 0x602000000018 thread T0
    #0 0x564bafb9f3ad in useFree /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:25
    #1 0x564bafb9f4a1 in main /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:37
    #2 0x7f3260abc0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
    #3 0x564bafb9f18d in _start (/home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main+0x118d)

0x602000000018 is located 8 bytes inside of 12-byte region [0x602000000010,0x60200000001c)
freed by thread T0 here:
    #0 0x7f3260d9740f in __interceptor_free ../../../../src/libsanitizer/asan/asan_malloc_linux.cc:122
    #1 0x564bafb9f36e in useFree /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:24
    #2 0x564bafb9f4a1 in main /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:37
    #3 0x7f3260abc0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)

previously allocated by thread T0 here:
    #0 0x7f3260d97808 in __interceptor_malloc ../../../../src/libsanitizer/asan/asan_malloc_linux.cc:144
    #1 0x564bafb9f35e in useFree /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:23
    #2 0x564bafb9f4a1 in main /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6/main.c:37
    #3 0x7f3260abc0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)

SUMMARY: AddressSanitizer: heap-use-after-free /home/alvin/Desktop/SynologyDrive/Learning/Coding/Java/Software Testing/Lab_6
/main.c:25 in useFree
```

Valgrind Report



```
==1561938== Invalid write of size 4
==1561938==    at 0x10920C: useFree (main.c:25)
==1561938==    by 0x109263: main (main.c:37)
==1561938==  Address 0x4a55048 is 8 bytes inside a block of size 12 free'd
==1561938==    at 0x483CA3F: free (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==1561938==    by 0x109203: useFree (main.c:24)
==1561938==    by 0x109263: main (main.c:37)
==1561938==  Block was alloc'd at
==1561938==    at 0x483B7F3: malloc (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==1561938==    by 0x1091F3: useFree (main.c:23)
==1561938==    by 0x109263: main (main.c:37)
==1561938==
==1561938==
==1561938== HEAP SUMMARY:
==1561938==     in use at exit: 0 bytes in 0 blocks
==1561938==   total heap usage: 1 allocs, 1 frees, 12 bytes allocated
==1561938==
==1561938== All heap blocks were freed -- no leaks are possible
==1561938==
==1561938== For lists of detected and suppressed errors, rerun with: -s
==1561938== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

ASan✅ Valgrind✅

Use-after-return

Code

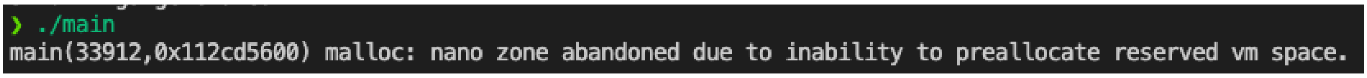
```
//if Asan want to detect error need to use
//fsanitize-address-use-after-return
char* x;

void useReturn() {
    char stack_buffer[42];
    x = &stack_buffer[13];
}

int main(){
    useReturn();
    *x = 42;
}
```

ASan❌ Valgrind❌

redzone

```
void redzone(){
    int a[8] = {0};
    int b[8] = {0};
    a[16] = 0;
}
```

ASan不會找到錯誤，但會有提示。



```
❯ ./main
main(33912,0x112cd5600) malloc: nano zone abandoned due to inability to preallocate reserved vm space.
```