Lesson 13

Christian Schwarz, Jakob Krebs

03.02.2020

Contents

Valgrind

Motivation

We want to find memory related bugs, like

- uninitialized values
- double free
- invalid reads

usage

```
1 valgrind name_of_binary
```

You want to build the binary with `-g`, to have line numbers in the valgrind output

uninitialized values

code:

```
1 int a;
2
3 if (a == 23) bla();
```

valgrind output:

```
1 Conditional jump or move depends on uninitialised value(s)
2    at 0x48D955D: _itoa_word (in /usr/lib/libc-2.30.so)
3    by 0x48F313B: __vfprintf_internal (in /usr/lib/libc-2.30.so)
4    by 0x48DF26E: printf (in /usr/lib/libc-2.30.so)
5    by 0x1091E7: main (in /pathToCode/a.out)
6  Uninitialised value was created by a stack allocation
7    at 0x109169: main (in /pathToCode/a.out)
```

double free

code:

```
1 free(a);
2 free(a);
```

valgrind output:

```
1 Invalid free() / delete / delete[] / realloc()
2    at 0x48399AB: free (vg_replace_malloc.c:540)
3    by 0x10922F: main (in /pathToCode/a.out)
4  Address 0x1fff000980 is on thread 1's stack
5  in frame #1, created by main (???:)
```

invalid reads

code:

```
1 free(a);
2 bla = a->myptr;
```

valgrind output:

```
1 Invalid read of size 8
2    at 0x109234: main (in /pathToCode/a.out)
3  Address 0x4a52048 is 8 bytes inside a block of size 16 free'd
4    at 0x48399AB: free (vg_replace_malloc.c:540)
5    by 0x10922F: main (in /pathToCode/a.out)
6  Block was alloc'd at
7    at 0x483877F: malloc (vg_replace_malloc.c:309)
8    by 0x10919A: main (in /pathToCode/a.out)
```

Tetris

What's missing?

- farben
- scoring
- game over

Questions