

Maze Game Analysis

Team 6

Jon Beason, Ben McAnulty, Tabitha Pflieger, Bryce Schaefer

Demo Time :)

Compilation: `gcc -g -Wall -Wpendantic -ansi -Wcoverage main.c -o main -l ncurses`
Execution: `./main maze#.txt`

Memory Management Analysis

valgrind --leak-check=full ./main maze#.txt

Successful by removing ncurses specific variable placements

```
-bash-4.2$ valgrind --leak-check=full ./main maze1.txt
==41120== Memcheck, a memory error detector
==41120== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==41120== Using Valgrind-3.15.0 and LibVEX; rerun with -h for copyright info
==41120== Command: ./main maze1.txt
==41120==
Score: 0
==41120==
==41120== HEAP SUMMARY:
==41120==    in use at exit: 189,581 bytes in 458 blocks
==41120==   total heap usage: 480 allocs, 22 frees, 199,399 bytes allocated
==41120==
==41120== LEAK SUMMARY:
==41120==    definitely lost: 0 bytes in 0 blocks
==41120==    indirectly lost: 0 bytes in 0 blocks
==41120==    possibly lost: 0 bytes in 0 blocks
==41120==    still reachable: 189,581 bytes in 458 blocks
==41120==    suppressed: 0 bytes in 0 blocks
==41120== Reachable blocks (those to which a pointer was found) are not shown.
==41120== To see them, rerun with: --leak-check=full --show-leak-kinds=all
==41120==
==41120== For lists of detected and suppressed errors, rerun with: -s
==41120== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```





```
-bash-4.2$ gcc -g -Wall --pedantic -ansi --coverage main.c -o main -l ncurses
main.c: In function 'main':
main.c:162:5: warning: pointer targets in passing argument 1 of 'strncpy' differ in signedness [-Wpointer-sign]
      strncpy(gameMaze[row], line, (int)width); /*warning during compile excluded from consideration -
      ^
In file included from main.c:4:0:
/usr/include/string.h:128:14: note: expected 'char * __restrict__' but argument is of type 'unsigned char *'
extern char *strncpy (char * __restrict __dest,
                    ^
-bash-4.2$
```

Static Analysis

CERT-C 2016 Mandatory
Violation Scrub

Overall Result: CONDITIONAL PASS

Code Review Report

	Quality Result	Uniq Violations		No in Function	Breakdown of Violations
		% in Function			
main	Conditional Pass	61		Unique violations - 14	14-O
isTreasure	Conditional Pass	9		Unique violations - 2	2-O
isZombie	Conditional Pass	13		Unique violations - 3	3-O
willCollide	Conditional Pass	17		Unique violations - 4	4-O
					(23 out of 295 checked)

Test Coverage Analysis

Forceful 100% Test Coverage

Without need of gdb, full test coverage was successfully reached.

```
-bash-4.2$ gcov main.c  
File 'main.c'  
Lines executed:100.00% of 165  
Creating 'main.c.gcov'
```

Testing:

maze8.txt - empty file

maze9.txt - nonexistent file

maze10.txt - file in incorrect format

Execution without file argument

Directing player into zombie from each direction

Using specifically maze7.txt to score

Removing one unused function

Fuzz Testing

AFL Fuzz Tool

`afl-fuzz -m 1000 -t 2000 -i inputfiles -o outputResults ./main @@`

american fuzzy lop 2.52b (main)

process timing run time : 0 days, 1 hrs, 2 min, 28 sec last new path : 0 days, 0 hrs, 3 min, 1 sec last uniq crash : 0 days, 0 hrs, 2 min, 58 sec last uniq hang : 0 days, 0 hrs, 44 min, 20 sec	overall results cycles done : 0 total paths : 73 uniq crashes : 18 uniq hangs : 1
cycle progress now processing : 5 (6.85%) paths timed out : 0 (0.00%)	map coverage map density : 0.13% / 0.18% count coverage : 2.72 bits/tuple
stage progress now trying : interest 32/8 stage execs : 114/18.8k (0.61%) total execs : 95.0k exec speed : 0.81/sec (zzzz...)	findings in depth favored paths : 13 (17.81%) new edges on : 16 (21.92%) total crashes : 7959 (18 unique) total tmouts : 1 (1 unique)
fuzzing strategy yields bit flips : 17/6880, 8/6877, 2/6871 byte flips : 0/860, 1/347, 0/393 arithmetics : 10/17.9k, 0/2694, 0/0 known ints : 0/1219, 0/9380, 0/7480 dictionary : 0/0, 0/0, 0/0 havoc : 45/33.0k, 0/0 trim : 2.60%/400, 62.04%	path geometry levels : 2 pending : 71 pend fav : 12 own finds : 65 imported : n/a stability : 100.00%

[cpu000: 29%]

- Changed to while(false) and compiled with afl-gcc
- Sample ncurses demo inputs
- File with weird characters
- File that starts in correct format and rest has gibberish

american fuzzy lop 2.52b (main)

process timing run time : 0 days, 11 hrs, 40 min, 48 sec last new path : 0 days, 3 hrs, 35 min, 46 sec last uniq crash : 0 days, 2 hrs, 43 min, 32 sec last uniq hang : 0 days, 1 hrs, 42 min, 34 sec	overall results cycles done : 2 total paths : 112 uniq crashes : 25 uniq hangs : 7
cycle progress now processing : 109 (97.32%) paths timed out : 0 (0.00%)	map coverage map density : 0.13% / 0.22% count coverage : 2.75 bits/tuple
stage progress now trying : interest 32/8 stage execs : 86/684 (12.57%) total execs : 568k exec speed : 0.81/sec (zzzz...)	findings in depth favored paths : 19 (16.96%) new edges on : 23 (20.54%) total crashes : 47.9k (25 unique) total tmouts : 1126 (7 unique)
fuzzing strategy yields bit flips : 22/33.0k, 10/32.9k, 3/32.9k byte flips : 0/4119, 1/2101, 0/2209 arithmetics : 15/113k, 0/23.5k, 0/345 known ints : 0/8094, 0/56.8k, 0/96.5k dictionary : 0/0, 0/0, 0/0 havoc : 78/159k, 0/0 trim : 31.34%/2086, 49.81%	path geometry levels : 4 pending : 88 pend fav : 3 own finds : 104 imported : n/a stability : 100.00%

[cpu000: 25%]

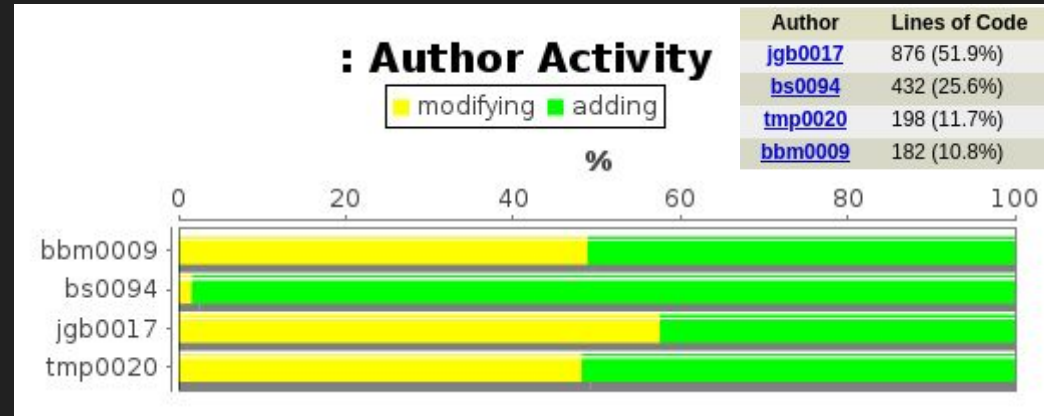
american fuzzy lop 2.52b (main)

process timing run time : 0 days, 18 hrs, 27 min, 16 sec last new path : 0 days, 0 hrs, 51 min, 23 sec last uniq crash : 0 days, 9 hrs, 30 min, 0 sec last uniq hang : 0 days, 1 hrs, 34 min, 50 sec	overall results cycles done : 2 total paths : 120 uniq crashes : 25 uniq hangs : 11
cycle progress now processing : 112* (93.33%) paths timed out : 0 (0.00%)	map coverage map density : 0.09% / 0.22% count coverage : 2.92 bits/tuple
stage progress now trying : havoc stage execs : 21.4k/26.2k (81.69%) total execs : 680k exec speed : 2.32/sec (zzzz...)	findings in depth favored paths : 19 (15.83%) new edges on : 23 (19.17%) total crashes : 56.8k (25 unique) total tmouts : 3034 (11 unique)
fuzzing strategy yields bit flips : 22/33.4k, 10/33.4k, 3/33.3k byte flips : 0/4175, 1/2154, 0/2256 arithmetics : 15/116k, 0/24.6k, 0/345 known ints : 0/8346, 0/58.1k, 0/99.1k dictionary : 0/0, 0/0, 0/0 havoc : 79/160k, 0/0 trim : 31.09%/2099, 49.15%	path geometry levels : 5 pending : 93 pend fav : 0 own finds : 112 imported : n/a stability : 100.00%

[cpu000: 27%]

- Commenting for the LDRA process skewed the results a bit but we all cosign that we did equal work

Generated:
2022-04-27 18:14
Head revision:
23
Report Period:
2022-04-07 to 2022-04-26
Total Files:
18
Total Lines of Code:
964
Developers:
4



SVN Stats