**栈溢出检测**

1.1 SARD-testsuite-6/testcaseid=1544

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

正常情况下程序会读取上一栈帧的内容（函数参数），难以区分

1. 改进

难以改进

1.2 SARD-testsuite-6/testcaseid=1545

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

正常

1. 原因分析：

无

1. 改进

无

1.3 SARD-testsuite-6/testcaseid=1546

1)CWE编号

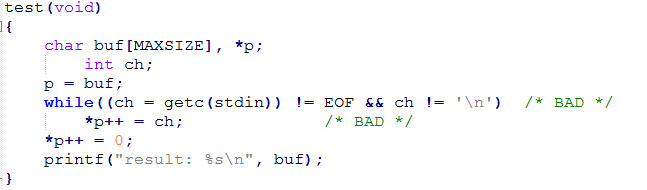
CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

1. 原因分析：

angr对getc没有进行建模。



1. 改进

等待angr官方改进或自己增加对getc函数建模

1.4 SARD-testsuite-6/testcaseid=1547

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

正常

3)原因分析：

无

4)改进

无

1.5 SARD-testsuite-6/testcaseid=1548

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

正常

3)原因分析：

无

4)改进

无

5)注：

虽然能测出，但存在循环嵌套，16G仍然偏小，速度较慢，存在卡顿

1.6 SARD-testsuite-6/testcaseid=1549

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

正常

3)原因分析：

无

4)改进

无

1.7 SARD-testsuite-6/testcaseid=1563

1)CWE编号

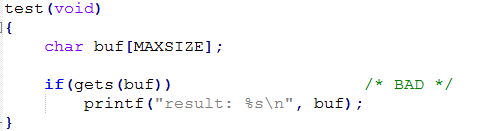
CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

angr对gets没有进行建模。



4)改进

等待angr官方改进或自己增加对gets函数建模

1.8 SARD-testsuite-6/testcaseid=1564

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

angr符号值转具体存在bug

4)改进

待angr开发者修复

1.9 SARD-testsuite-6/testcaseid=1565

1)CWE编号

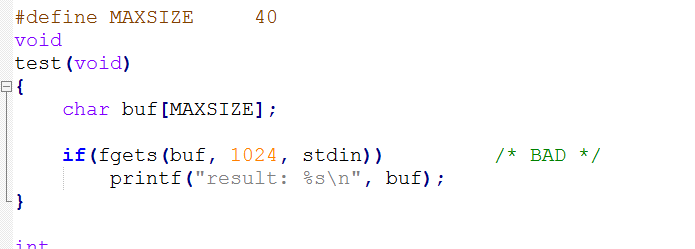
CWE-121: Stack-based Buffer Overflow

2)检测结果:

正常失败

3)原因分析：

angr使用fgets读入数据时，会打开一个文件（包括标准输入输出，网络操作），如果没有则创建一个新文件，fgets读的过程中会寻找’\n’，找不到的话，相当于读入数据为空，结果并不会造成溢出。



**4)改进**

可做：制作检测补丁：自动创建一些待操作文件，构造一些输入。

1.10 SARD-testsuite-6/testcaseid=1616

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

angr缺少对snprintf的建模

4)改进

等待官方完善

1.11 SARD-testsuite-6/testcaseid=1620

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

angr缺少对snprintf的建模

4)改进

无

1.12 SARD-testsuite-6/testcaseid=1620

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

angr缺少对snprintf的建模

4)改进

等待官方完善

1.13 SARD-testsuite-6/testcaseid=1622

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

缺少对snprintf的建模

4)改进

等待官方完善

1.14 SARD-testsuite-6/testcaseid=1624

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

缺少对snprintf的建模

4)改进

等待官方完善

1.15 SARD-testsuite-6/testcaseid=1626

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

缺少对snprintf的建模

4)改进

等待官方完善

1.16 SARD-testsuite-6/testcaseid=1636

1)CWE编号

CWE-121: Stack-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

缺少对sprintf的建模获取数据太短，无法导致溢出

4)改进

等待官方完善