实验报告

课程名称：软件测试

实验名称：KLEE实验课

专业班级：软件工程 16级四班

学 号：1611736

姓 名：钟腾

2018年 12月 11日

实验一

|  |  |  |  |
| --- | --- | --- | --- |
| 实验名称 | KLEE实验课 | | |
| 实验地点 | 泰达5区105 | 实验时间 | 2018/12/11 |
| 实验目的和要求 | | | |
| 1）熟悉 Linux 系统使用方式；  2）了解 LLVM 的架构和使用方式；  3）了解 Docker 使用  4）了解Github 使用方式  5) 了解并掌握基于约束的自动化测试工具的基本原理和使用。 | | | |
| 实验环境 | | | |
| Docker 2.0.0.0  Mac os 10.13.5 | | | |
| 实验过程 | | | |

|  |
| --- |
| 1、一开始在mac os中使用sudo apt-get安装KLEE失败，后来发现mac os没有apt-get功能，于是采用docker安装KLEE镜像。  2、完成tutorial 1和tutorial 2 ：      3、用c语言编写缺陷代码如下：  #include<stdio.h>  #include<stdlib.h>  void kleeTest(int a){      int sz[10];      int d[10];      for (int i = 0; i < 10; i++){ //赋初始值          sz[i] = i;      }      if (a < -50){ //求余分母为0          for (int i = 0; i < 10; i++){              int num = i;              d[i] = sz[i] % num;          }      }      else if(a < -25){ //除法分母为0          for (int i = 0; i <= 10; i++){              int num = i ;              d[i] = sz[i] / num;          }      }      else if (a < 0){ //数组越界          for(int i = 0; i<= 11; i++){              sz[i] = i;          }      }      else if (a < 25){ //空指针          int \*a = NULL;          int b = \*a + 1;      }      else if(a < 50){ //内存泄漏          free(sz);      }  }  int main(){      int n;      klee\_make\_symbolic(&n, sizeof(n), "n");      kleeTest(n);      return 0;  }  生成文件截图：  ../../../Library/Containers/com.tencent.qq/Data/Library/Application%20Support/QQ/Users/754159742/QQ/Temp.db/44E9A0BC-E6FC-40FF-B8A9-05DC9E4A7323.png  错误文件内容：  1、分母为0    2、空指针    3、分母为0    4、内存泄漏    5、数组越界 |

|  |
| --- |
| 心得体会 |
| 本次实验学会了使用docker和klee工具，并学会了如何编写带有软件缺陷的程序，对于掌握软件测试的各种方法具有很大帮助。鉴于国内外对于klee工具使用的说明介绍较少，因为将本次作业作为了技术帖发布在了csdn等网站。对于掌握新知识，我感到很兴奋。 |