《漏洞利用及渗透测试基础》实验报告

姓名： 许健 学号：2013018 班级：信安班

**实验名称：**

Angr应用

**实验要求：**

根据课本8.4.3章节，复现sym-write示例的两种angr求解方法，并就如何使用angr以及怎么解决一些实际问题做一些探讨。

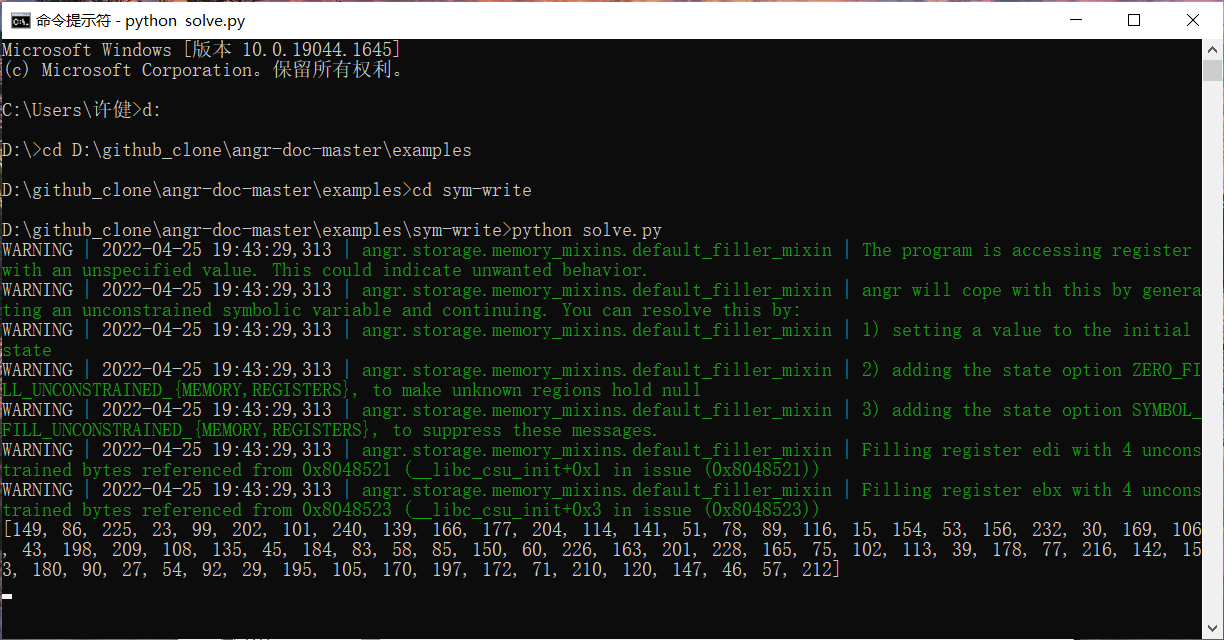
**实验过程：**

1. **复现sym-write示例的两种angr求解方法**

主要步骤：

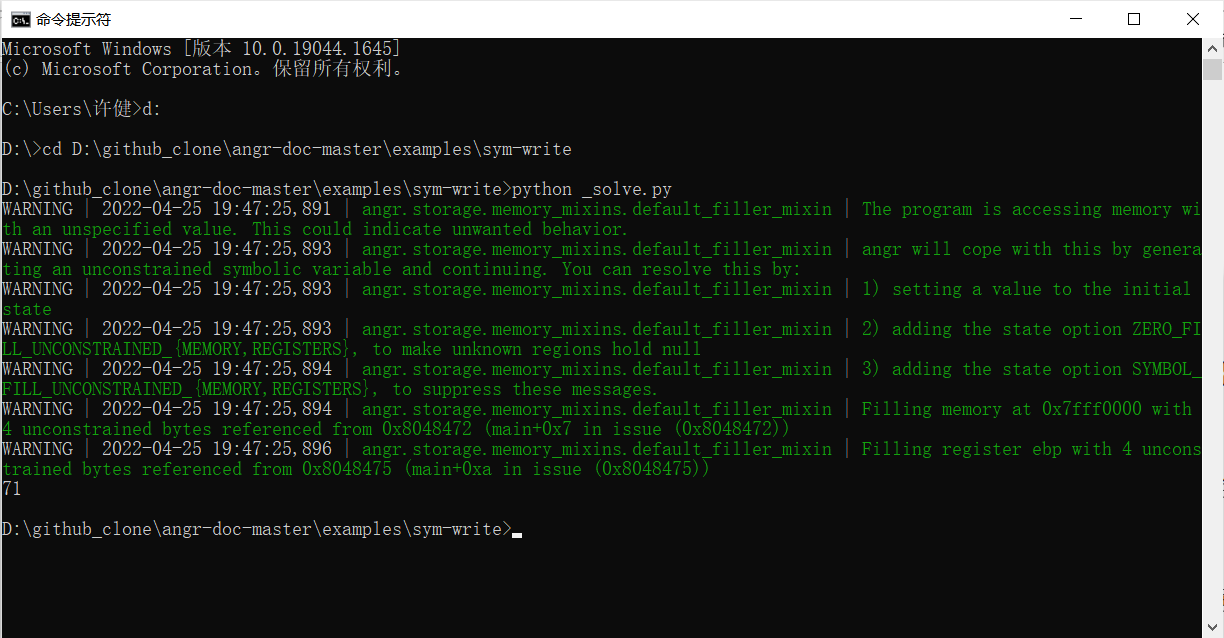
1. 新建一个Angr工程，并且载入二进制文件
2. 初始化一个模拟程序状态的SimState对象state
3. 将要求解的变量符号化
4. 创建模拟管理器（Simulation Managers）进行程序执行管理
5. 进行符号执行得到想要的状态
6. 获得到state之后，通过solver求解器，求解u的值。

采用eval\_upto(e, n, cast\_to=None, \*\*kwargs) 求解一个表达式多个可能的求解方案。运行如下：



其他解法：

1. 采用了hook函数
2. 进行符号执行得到想要的状态，只需要给定一个find条件
3. eval(u)替代了原来的eval\_upto，将打印一个结果，如图中的71



1. **使用angr解决实际问题**

Angr是一个基于python的二进制漏洞分析框架，能够进行动态的符号执行分析，也能够进行多种静态分析。可以用来进行漏洞挖掘、软件分析，比如：二进制爆破、堆溢出等等。

使用Angr的主要步骤包括：

1. 变量符号化
2. 动态符号执行
3. 获取路径约束条件
4. 约束求解

使用Angr可以管理状态对象以及打印标准输出等，得到程序运行路径的输入。

还可以采用其他方式，比如Hook。Angr还可以进行CTF逆向分析。

使用Angr约束求解要防止路径爆炸问题