《漏洞利用及渗透测试基础》实验报告

**实验名称：**

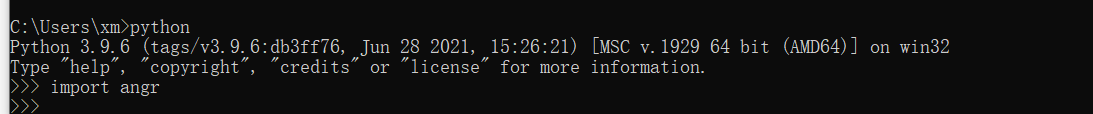
Angr应用实例

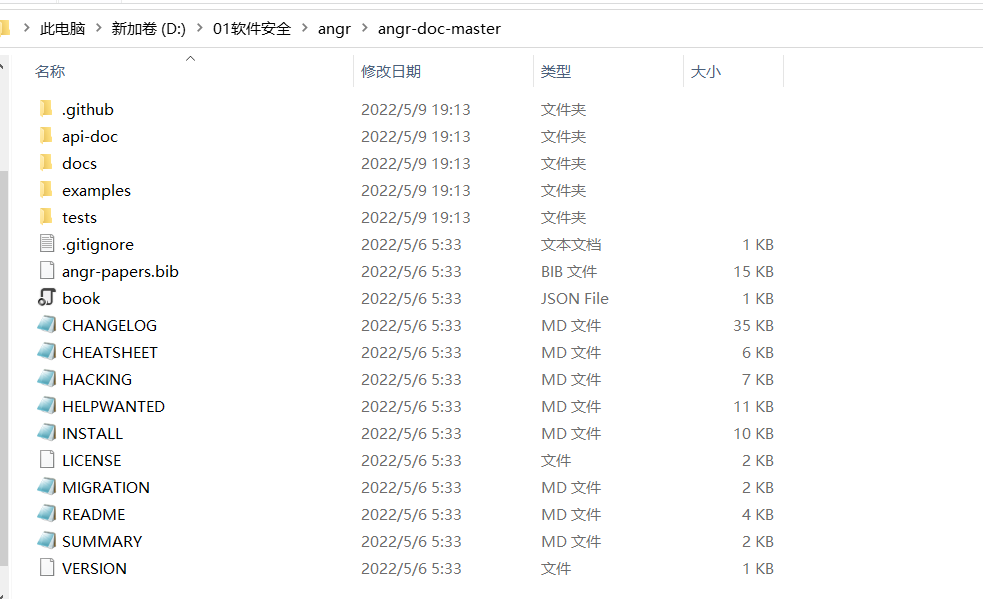
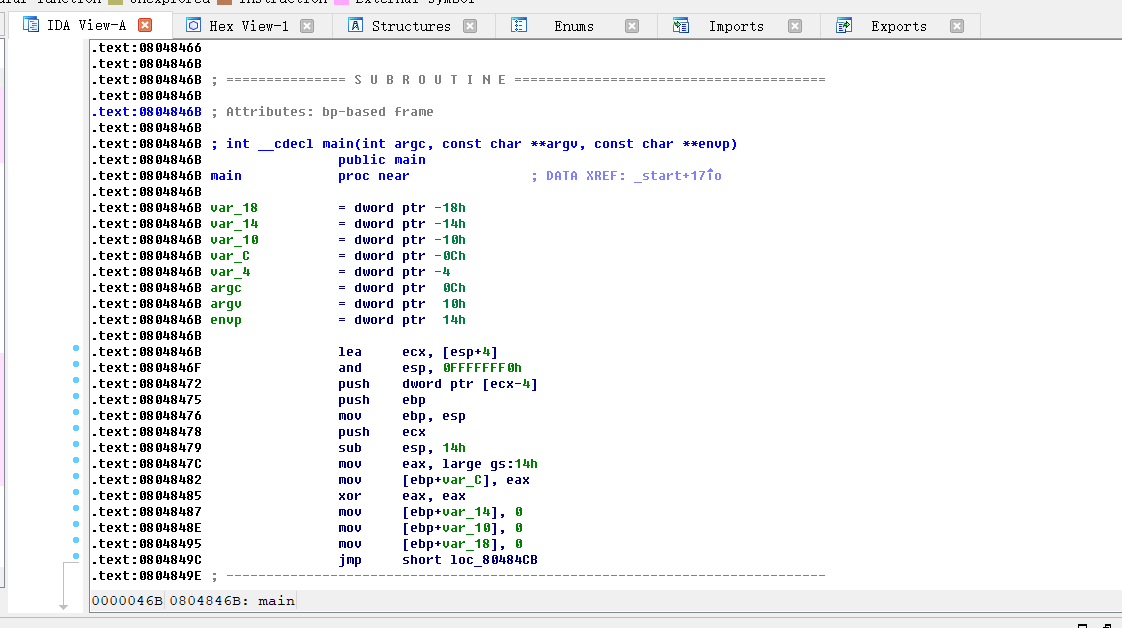
**实验要求：**

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. Angr安装



1. 下载GitHub上angr的开源项目
2. 用IDAPRO打开文件issue
3. 解法一

（1）新建一个Angr工程，并且载入二进制文件。

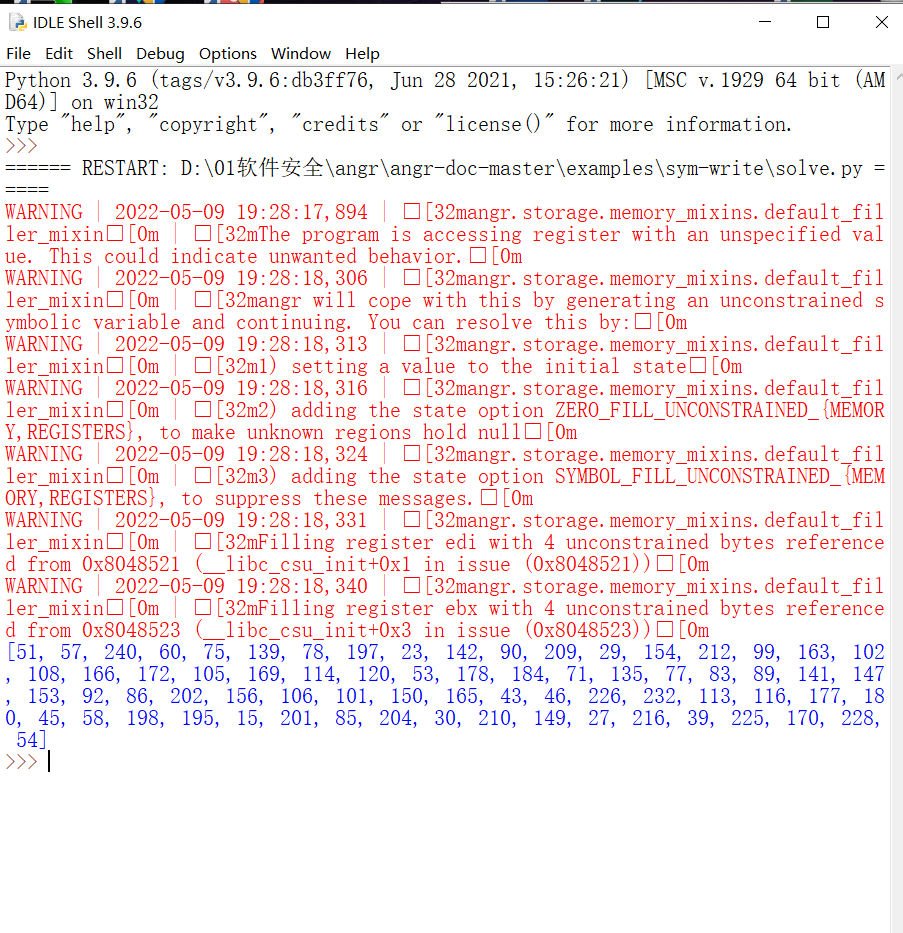
（2）初始化一个模拟程序状态的SimState对象state（使用函数entry\_state()），该对象包含了程序的内存、寄存器、文件系统数据、符号信息等等模拟运行时动态变化的数据。此外，也可以使用函数blank\_state()初始化模拟程序状态的对象state，在该函数里可通过给定参数addr的值指定程序起始运行地址。

（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。初始化的state可以经过模拟执行得到一系列的states，模拟管理器sm的作用就是对这些states进行管理。

（5）进行符号执行得到想要的状态，得到想要的状态。符号执行后，源程序里打印出的字符串里包含win字符串，而没有包含lose字符串。在这里，状态被定义为两个函数，通过符号执行得到的输出state.posix.dumps(1)中是否包含win或者lose的字符串来完成定义。

（6）获得到state之后，通过solver求解器，求解u的值。



1. 解法二

（1）采用了hook函数，将0x08048485处的长度为2的指令通过自定义的hook\_demo进行替代。

（2）进行符号执行得到想要的状态，有变化，变更为find=0x080484DB。

（3）最后，eval(u)替代了原来的eval\_upto，将打印一个结果出来。



**实验感想：**

认识到了ａｎｇｒ的妙用，学习了在python上实现二进制漏洞分析。