

网络攻防技术基础课程实验报告

|  |  |
| --- | --- |
| 实验名称： | 实验六  模糊测试 |
| 实验日期： | 2024-05-21 |
| 实验地点： | 西部片区4号楼301 |
|  | |
| 学号： | 33920212204567 |
| 姓名： | 任宇 |
| 专业年级： | 软工2021级 |
| 学年学期： | 2023-2024学年第二学期 |

1. **实验目的**

* 学习模糊测试(Fuzz)。

1. **实验用到的软件或工具**

虚拟机软件：VMware Workstation Pro 17

虚拟机环境 xpsp3\_xmu\_lesson2

EasyFuzzer2.0

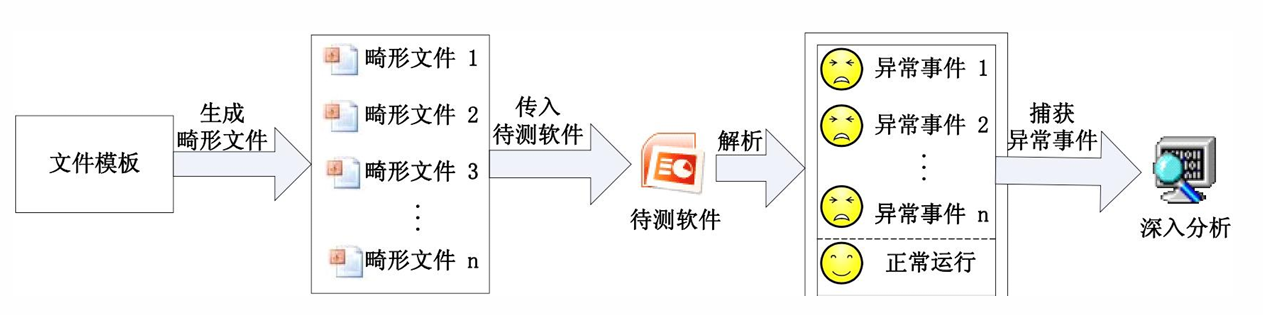
FTPFUZZ

OllyICE

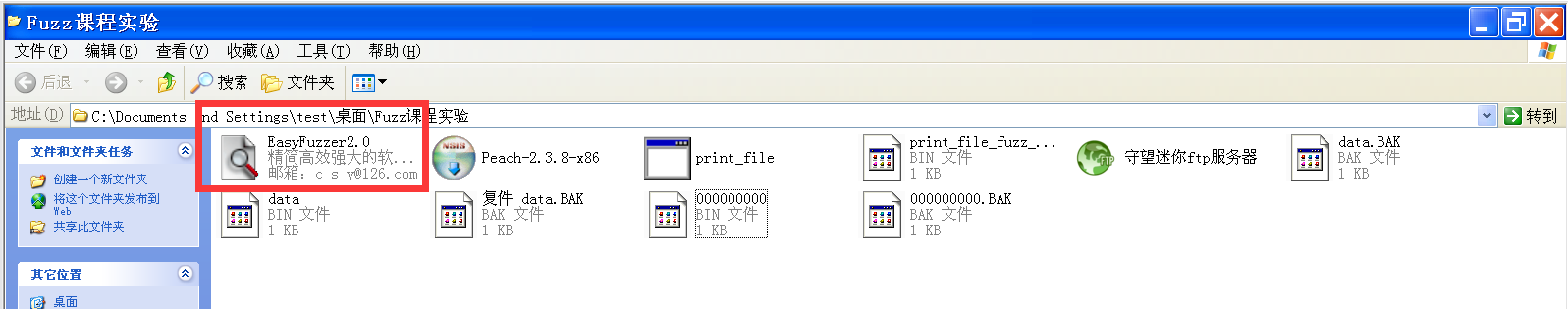
守望迷你ftp服务器

1. **实验过程**

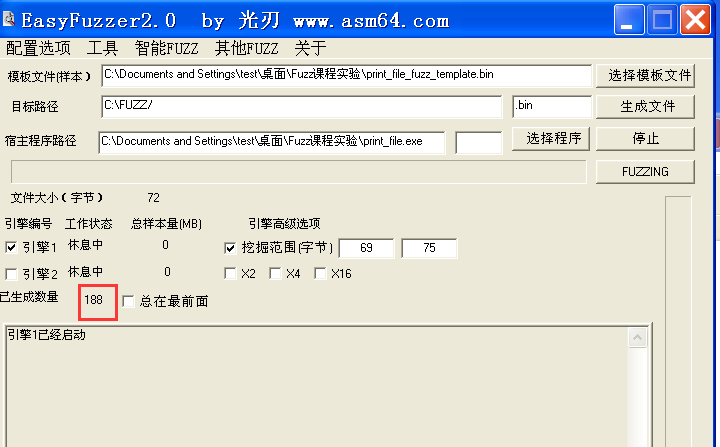
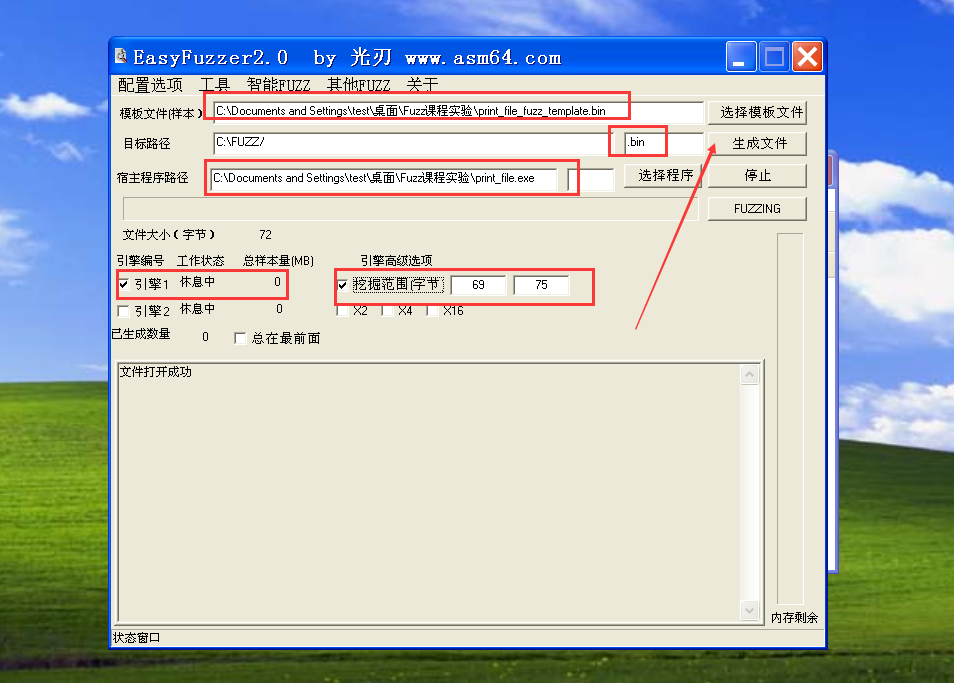
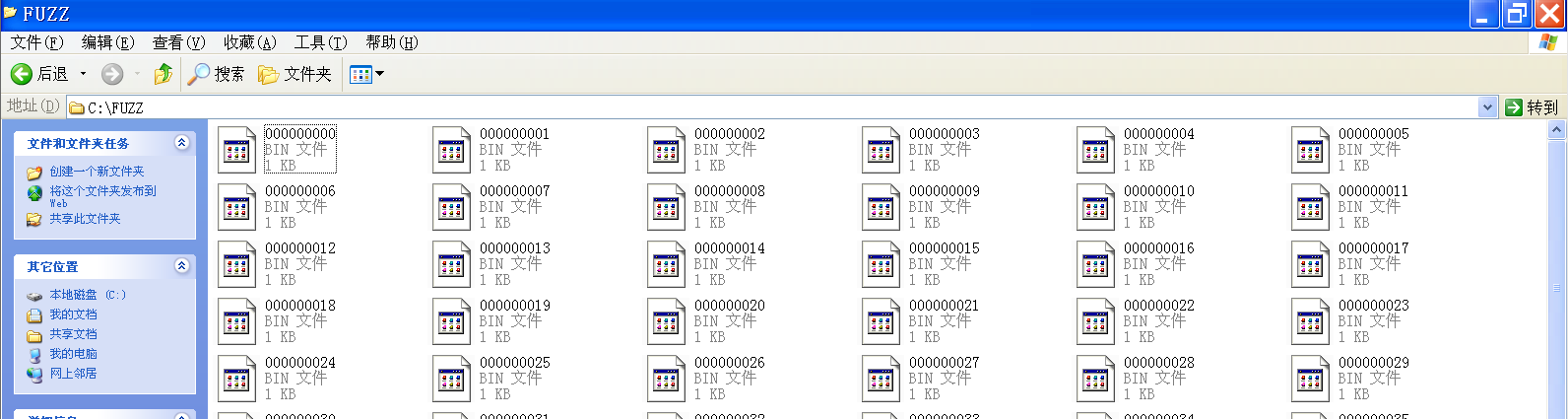
模糊测试是基于黑盒（或灰盒）的测试技术，其通过向目标系统提供非预期的输入并监视异常结果来发现软件漏洞。本次实验为对print\_file进行文件Fuzz，流程如下图所示：



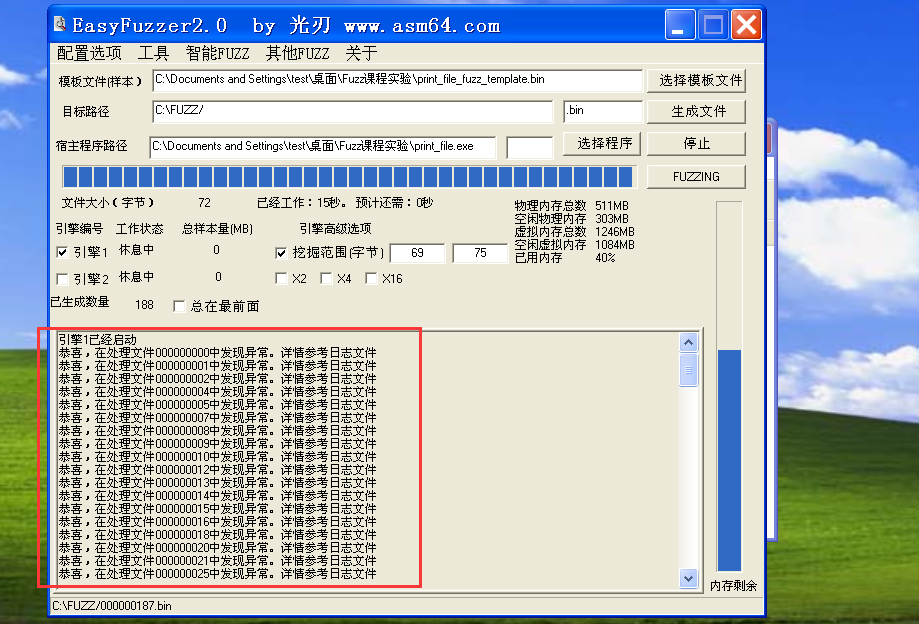
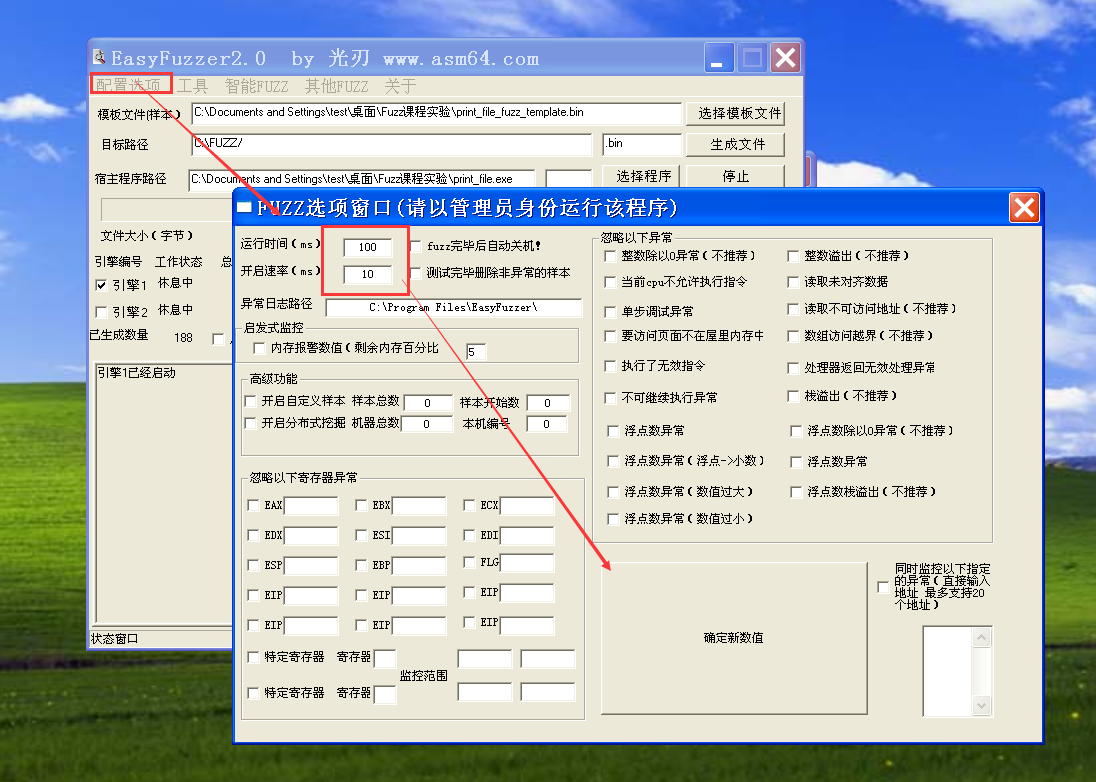
1. **打开EasyFuzzer2.0模糊测试软件并导入模板文件print\_file\_fuzz\_template.bin：**



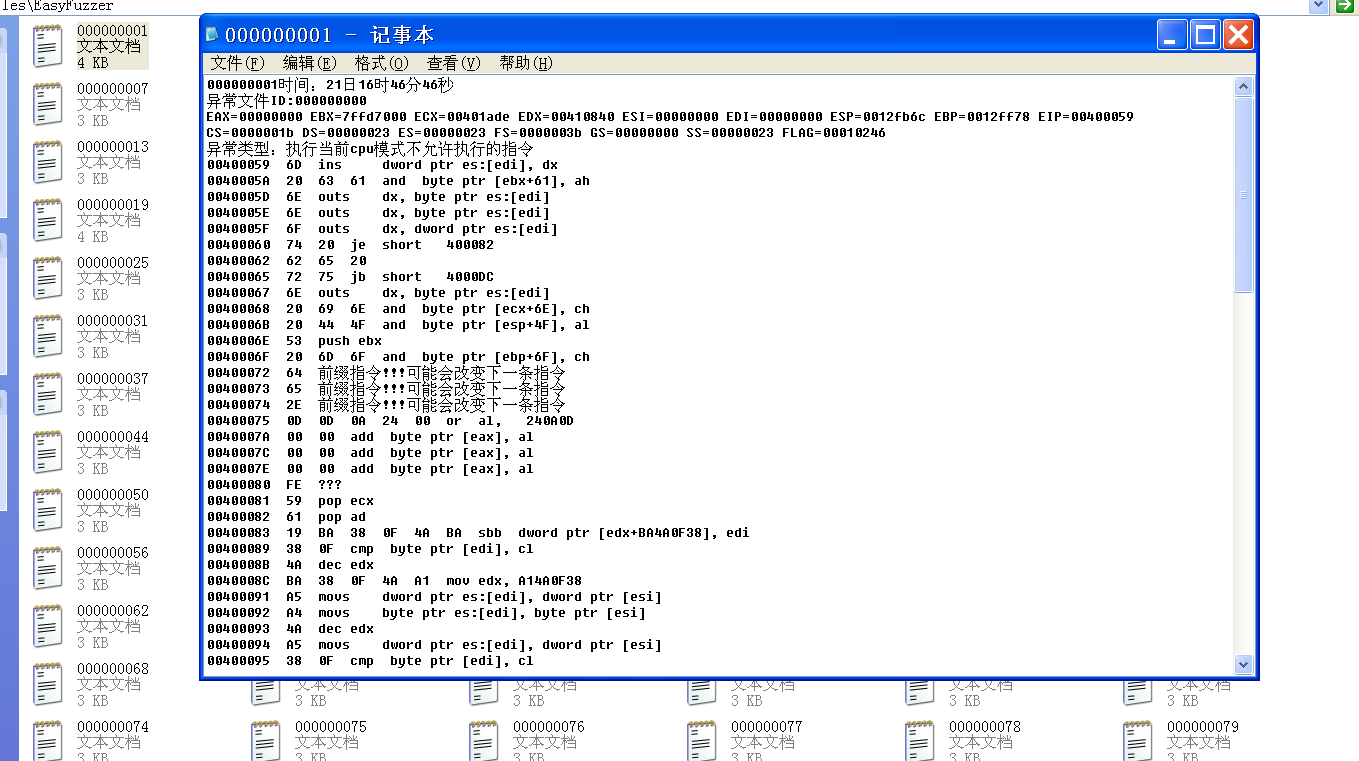
1. **选取合适的引擎，批量生成一些畸形文件，目标路径C:\FUZZ/：**

****

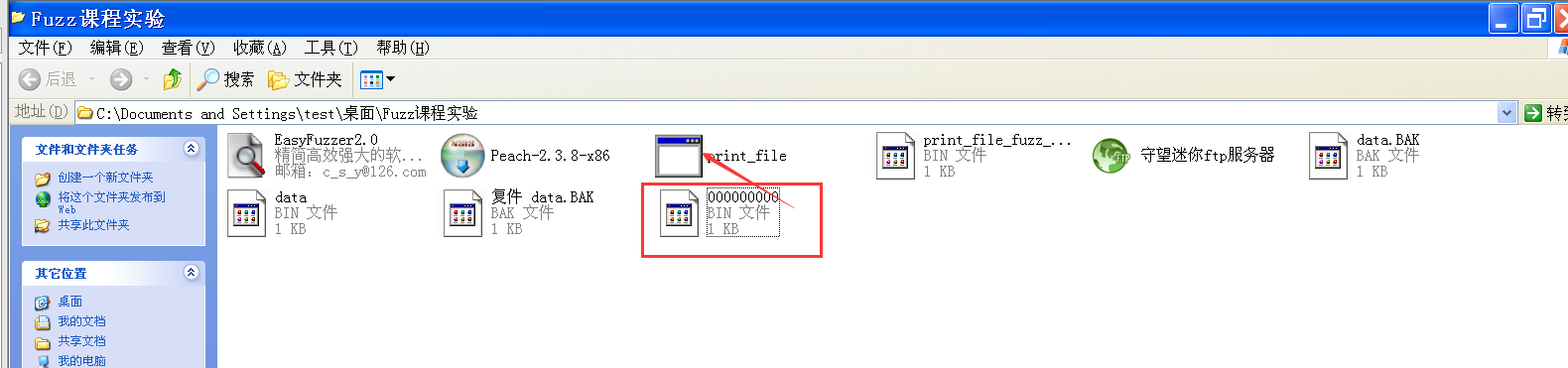
1. **点击fuzzing进行批量模糊测试：**



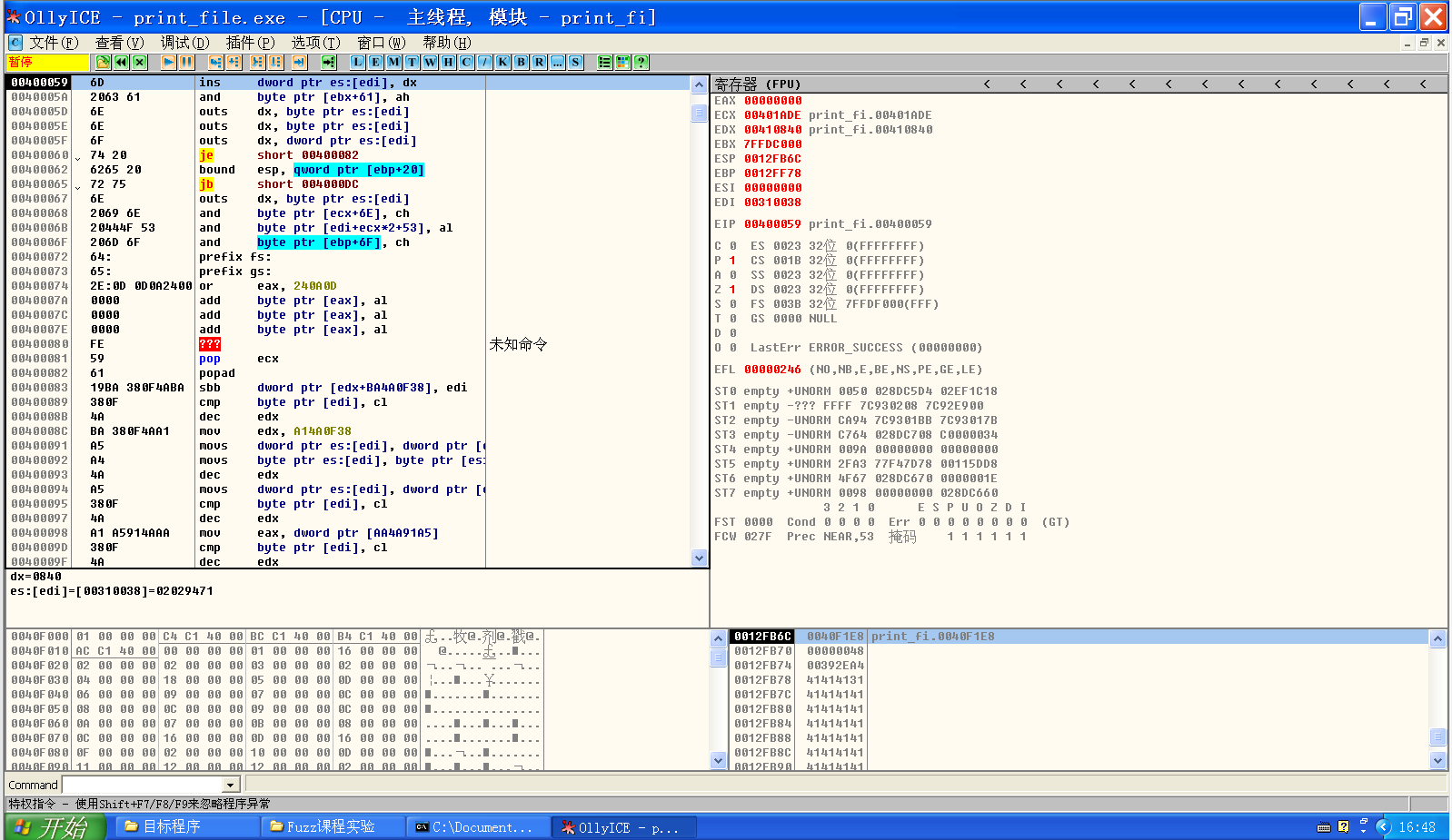
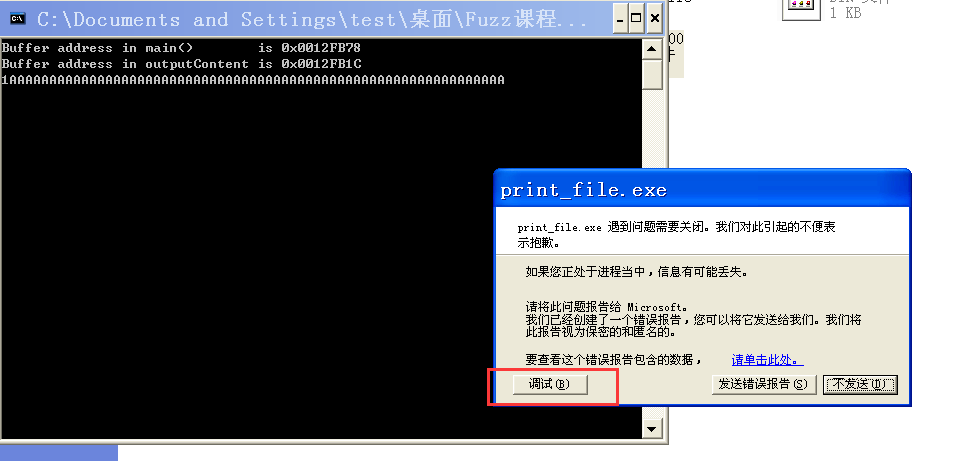
1. **根据异常日志，使用OllyICE调试print\_file程序：**

****

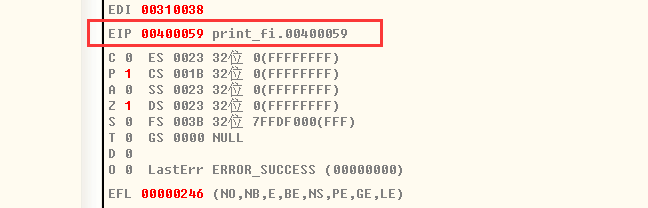
将000000000.bin拖到print\_file程序上以运行：



程序报错，这时点击调试即可打开OllyICE进行调试：

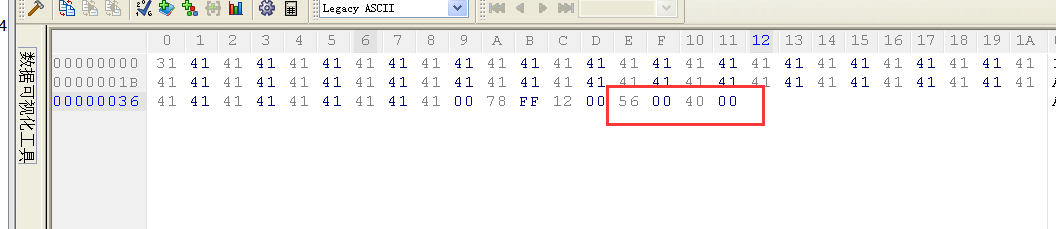


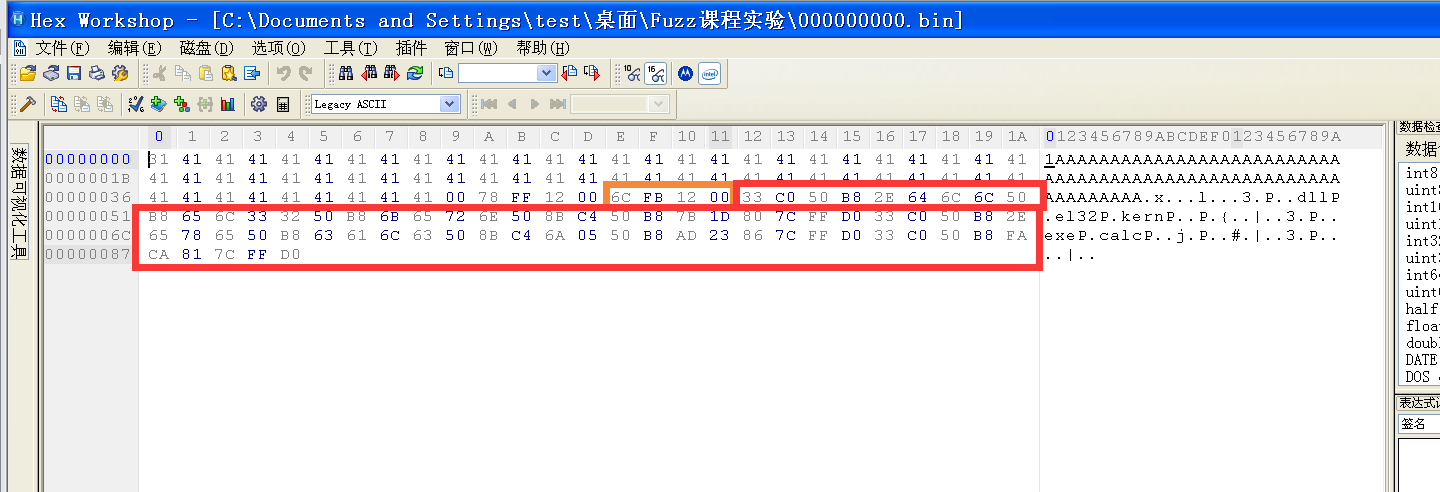
左上角为反汇编窗口、左下角为数据窗口、右上角为寄存器窗口和右下角为堆栈串口，此时观察寄存器串口，可以发现EIP寄存器指向地址0x00400059，而这是不可访问区，因此程序报错。EIP寄存器是x86架构中的指令指针寄存器，用于存储下一条要执行的指令的地址。EIP寄存器在计算机体系结构中扮演着核心角色，它确保了程序的正确执行顺序，并为程序员提供了实现复杂逻辑控制的手段。



修改样本000000000.bin中的返回地址，将其修改为可访问地址，并添加上计算器代码：



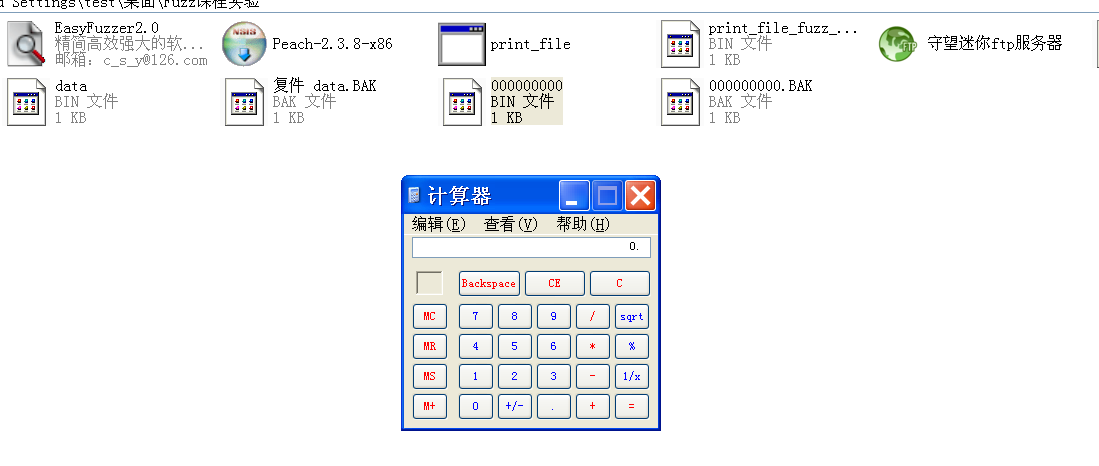




1. **构建缓冲区溢出样本后完成弹出计算器的利用：**

在4）中，我们构建了溢出样本，其原理为：首先填充buf数组字节，接着覆盖保存的返回地址，这个地址应该指向将要执行的恶意代码（通过调试信息来确定），最后注入可以执行计算器程序的机器码。

将修改后的样本拖到print\_file程序上运行，可见成功打开计算器：



1. **实验思考及心得**

通过本次实验，我深刻理解了模糊测试（Fuzz Testing）的重要性和实际应用。通过向程序输入非预期数据，我成功地识别并利用了软件中的缓冲区溢出漏洞，这不仅增强了我的调试技能，也让我更加了解了软件安全性的重要性。