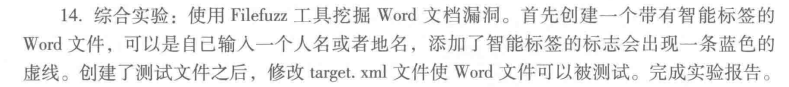
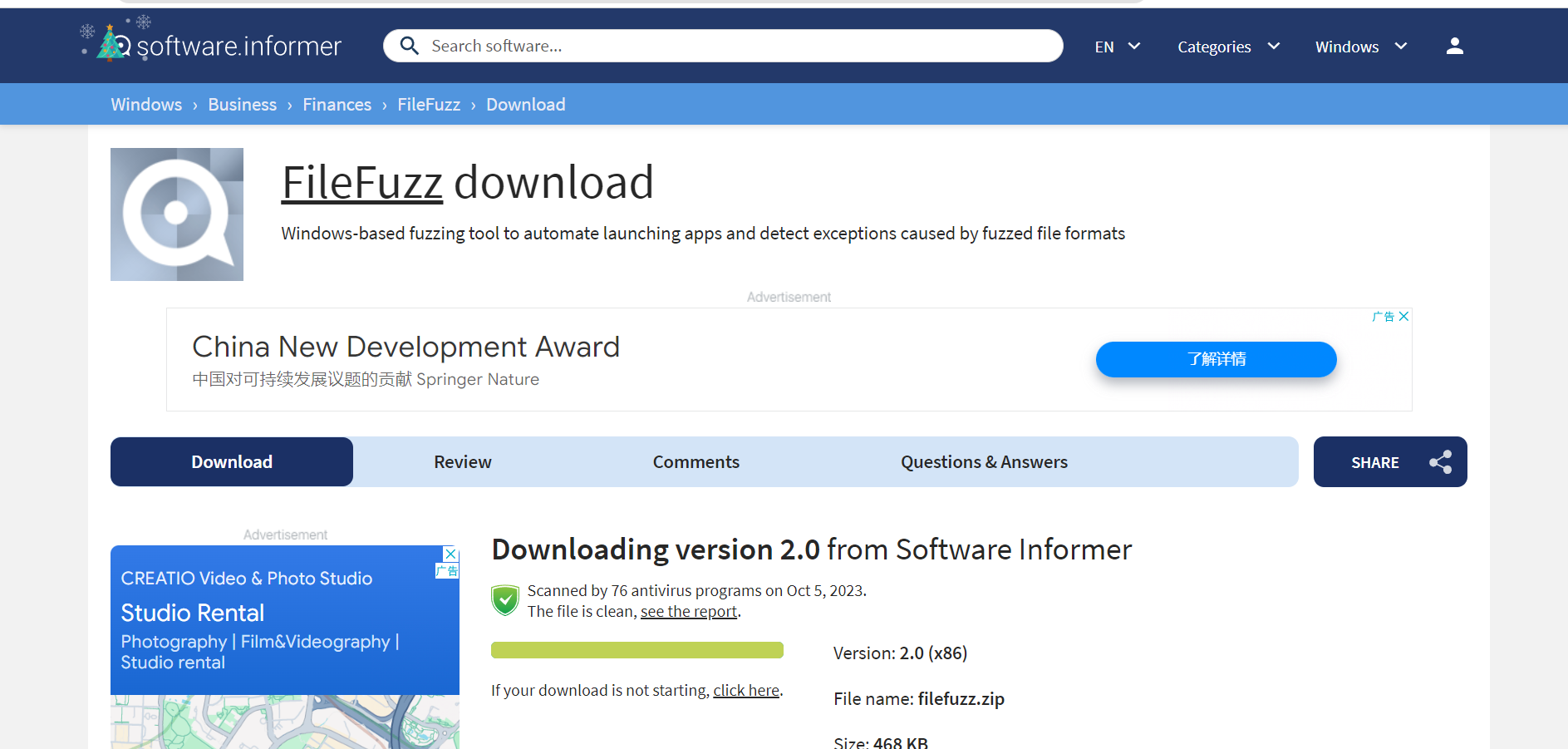
## 选取题目：

P239 14



## 软件安装：

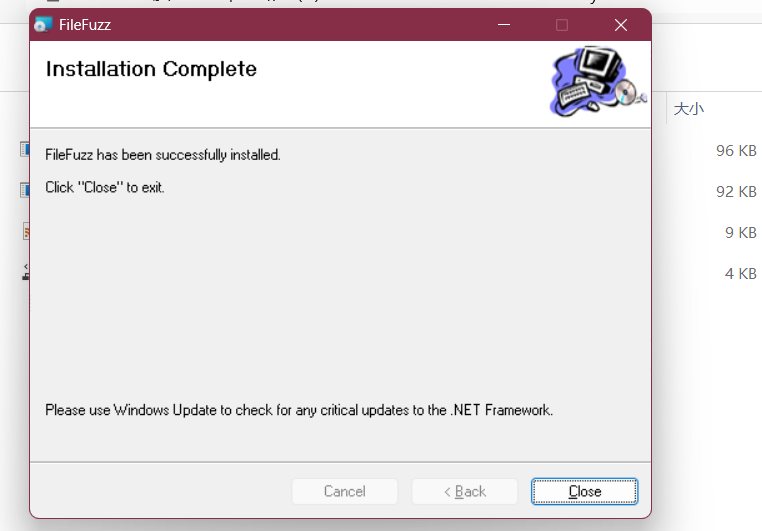
下载



解压

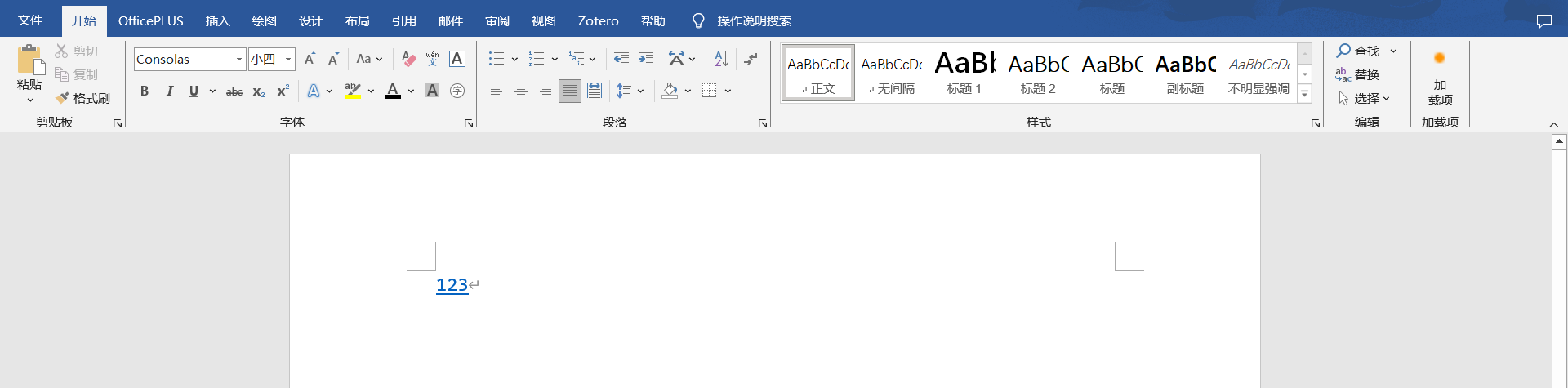


安装



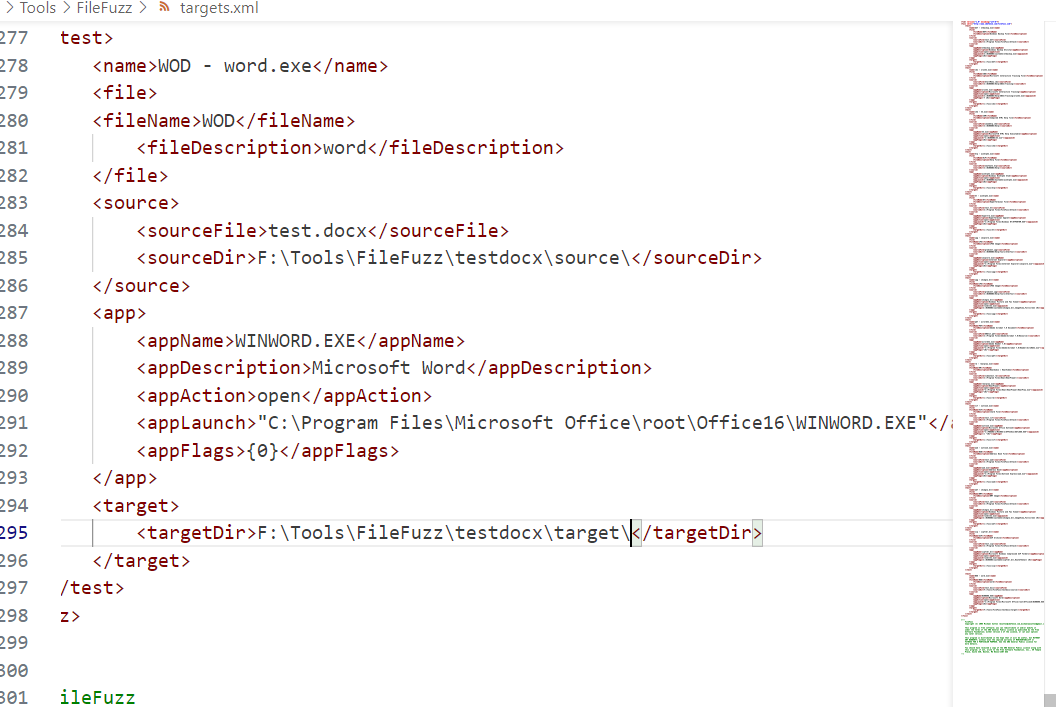
### 分析过程

测试用的word文档：

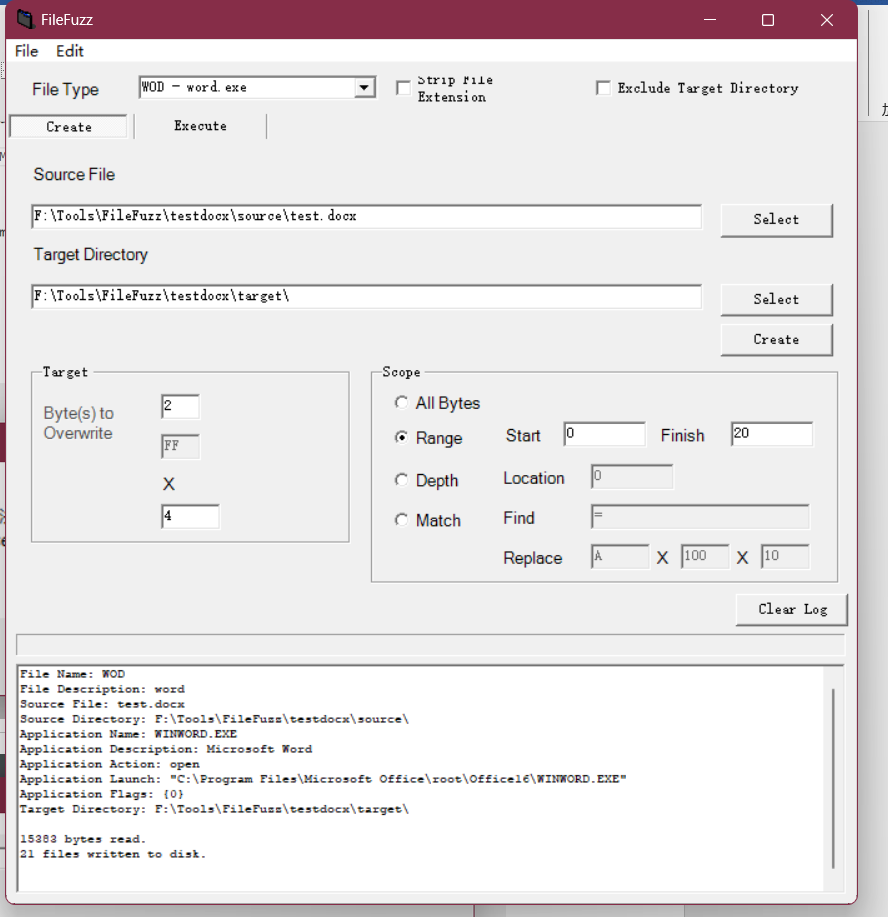


添加了一个智能标签

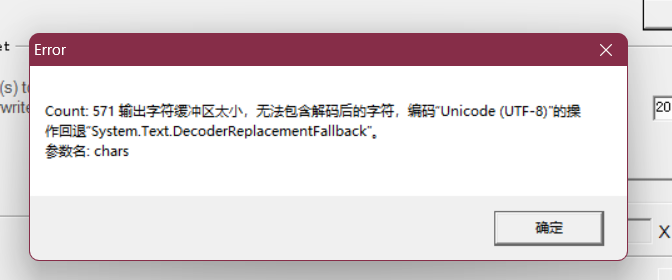
修改targets.xml:



打开filefuzz软件修改相关配置：

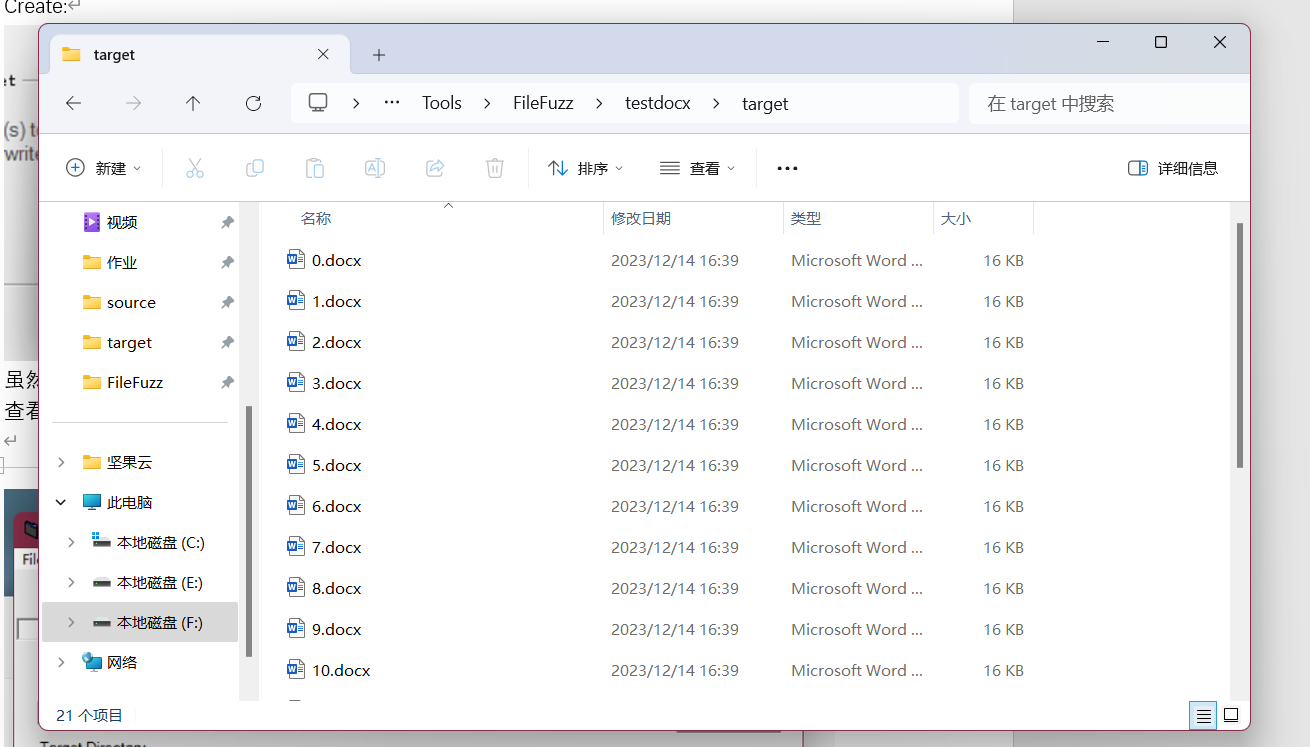


Create:



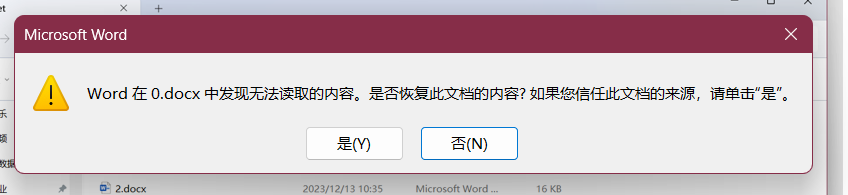
虽然爆了字符串缓冲区太小的错不过不影响实验流程

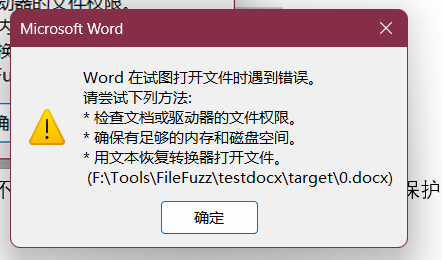
查看target目录：



可以看到有21个模糊测试文件产生

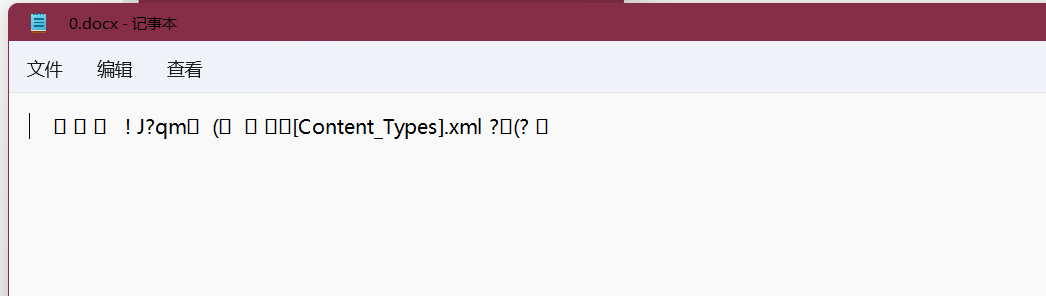
尝试打开这些文档：





Filefuzz产出的这些文档不可以用word正常打开，这是word自带的保护机制。

尝试使用记事本打开:



可以看到输入似乎是随机的乱码，但是也有些正常的英文单词。

新版的word打开这些文档已经不会被漏洞利用了，不过搜索发现word2003在打开一份测试文档时会使得shell被远程使用。

## 实验总结：

本次实验使用的filefuzz通过改变文档的内容进行模糊测试来发现word的潜在漏洞。

模糊测试是一种基于缺陷注入的自动软件测试技术。通过编写工具向目标程序提供某种形式的输入并观察其响应来发现问题，这种输入可以是完全随机的或精心构造的。模糊测试通常以大小相关的部分、字符串、标志字符串开始或结束的二进制块等为重点，使用边界值附近的值对目标进行测试。模糊测试不是测试软件正确性，而是一个漏洞发现工具。