****

青岛理工大学

**《恶意代码分析》项目课报告**

**项目题目：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |
| --- | --- | --- |
| **项目组成员** | **姓名** | **姓名** |
| 组长：\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |
| --- | --- |
| **学 院：** | 信息与控制工程学院 |
| **专 业：** |  |
| **指导教师：** |  |
| **起讫日期：** | 2025.3.17 至 2025.6.1 |

# 模糊测试项目报告

### 项目源码分析（50分）

整体流程

关键代码与技术

### 现有项目总结（10分）

### 项目改进（20分）

### 测试效果（10分）

环境构建

下载并构建

首先为Fuzz目标创建一个新目录：

cd $HOME

mkdir fuzzing\_xpdf && cd fuzzing\_xpdf/

下载Xpdf 3.02：

wget https://dl.xpdfreader.com/old/xpdf-3.02.tar.gz

tar -xvzf xpdf-3.02.tar.gz

构建Xpdf：

cd xpdf-3.02

sudo apt update && sudo apt install -y build-essential gcc

./configure --prefix="$HOME/fuzzing\_xpdf/install/"

make

make install

现在可以开始测试Xpdf。首先，需要下载一些 PDF 示例：

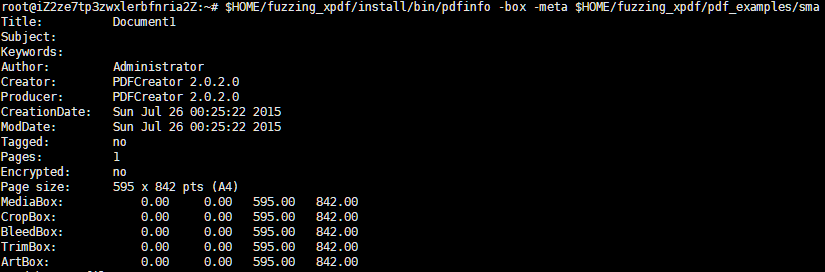
cd $HOME/fuzzing\_xpdf

mkdir pdf\_examples && cd pdf\_examples

wget https://www.melbpc.org.au/wp-content/uploads/2017/10/small-example-pdf-file.pdf

$HOME/fuzzing\_xpdf/install/bin/pdfinfo -box -meta $HOME/fuzzing\_xpdf/pdf\_examples/ small-example-pdf-file.pdf

结果如下：



安装AFL

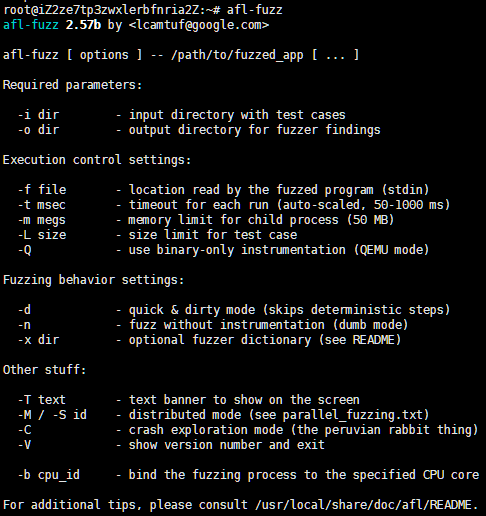
tar -xvzf GA\_Fuzz.tar.gz

make

make install

afl-fuzz

结果如下：



开始Fuzz

首先，清理所有以前编译的目标文件和可执行文件：

rm -r $HOME/fuzzing\_xpdf/install

cd $HOME/fuzzing\_xpdf/xpdf-3.02/

make clean

现在将使用afl-clang-fast编译器构建 xpdf ：

CC=$HOME/Ga\_Fuzz/afl-gcc

CXX=$HOME/Ga\_Fuzz/afl-g++

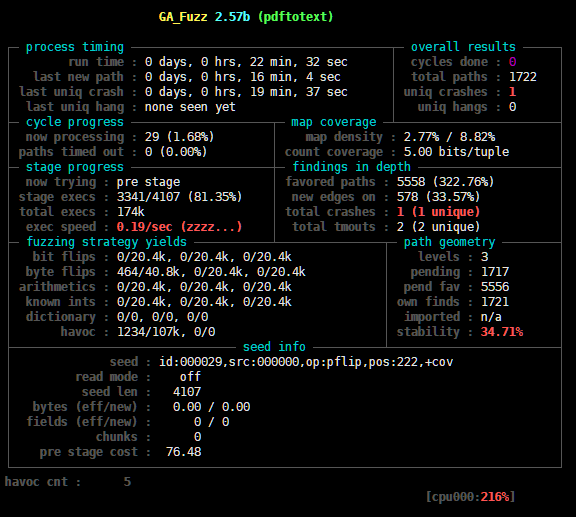
./configure --prefix="$HOME/fuzzing\_xpdf/install/"

make

make install

现在可以使用以下命令运行Fuzz：

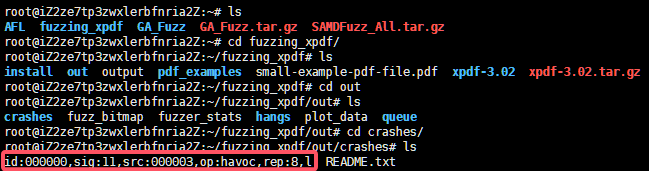
afl-fuzz -i $HOME/fuzzing\_xpdf/pdf\_examples/ -o $HOME/fuzzing\_xpdf/out/ -- $HOME/fuzzing\_xpdf/install/bin/pdftotext @@ $HOME/fuzzing\_xpdf/output



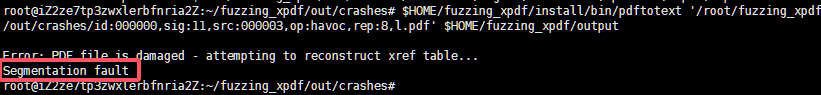
可以看到红色的uniq crashes值，显示找到的唯一崩溃的数量。可以在$HOME/fuzzing\_xpdf/out/目录中找到这些崩溃文件。一旦发现第一个崩溃，就可以使用control+c停止 fuzzer。

复现崩溃和修复漏洞

在$HOME/fuzzing\_xpdf/out/目录中找到崩溃对应的文件



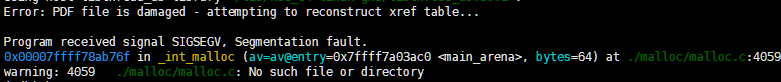
将文件名称改为xxx.pdf后将此文件作为输入传递给 pdftotext 二进制文件



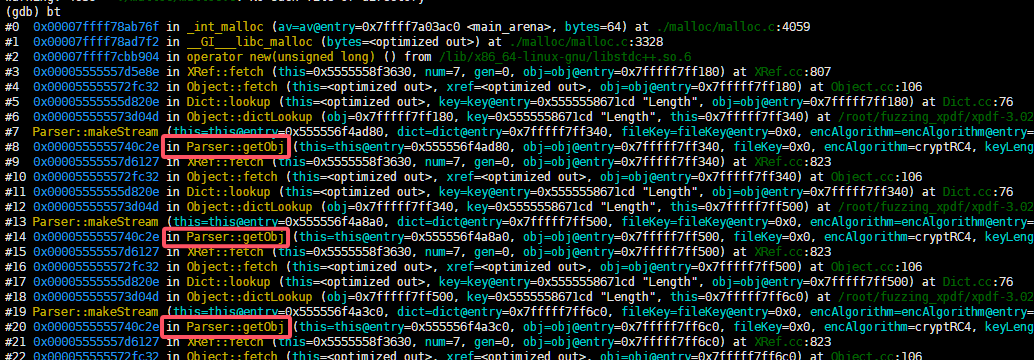
使用 gdb 找出程序因该输入而崩溃的原因

gdb --args $HOME/fuzzing\_xpdf/install/bin/pdftotext $HOME/fuzzing\_xpdf/out /crashes/ id:000000,sig:11,src:000003,op:havoc,rep:8,l.pdf $HOME/fuzzing\_xpdf/output

run



然后输入bt以获取栈回溯：



滚动调用堆栈，将看到Parser::getObj方法的许多调用，这些调用似乎表示无限递归

### 分工明细

**项目总结（10分）**

# 测试用例生成项目报告

### 项目源码分析（50分）

整体流程

关键代码与技术

### 现有项目总结（10分）

### 项目改进（20分）

### 测试效果（10分）

### 分工明细

**项目总结（10分）**

# XXX（自选）项目报告

### 项目简介（5分）

### 项目的目标（5分）

### 相关项目调研与代码分析（40分）

### 项目设计（30分）

项目设计思路，创新性、安全性体现。

### 效果（10分）

### 分工明细

**项目总结（10分）**