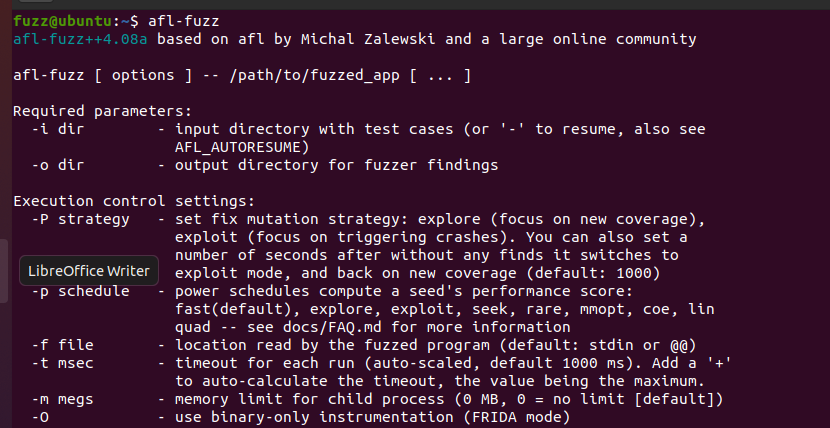
下载并构建Xpdf

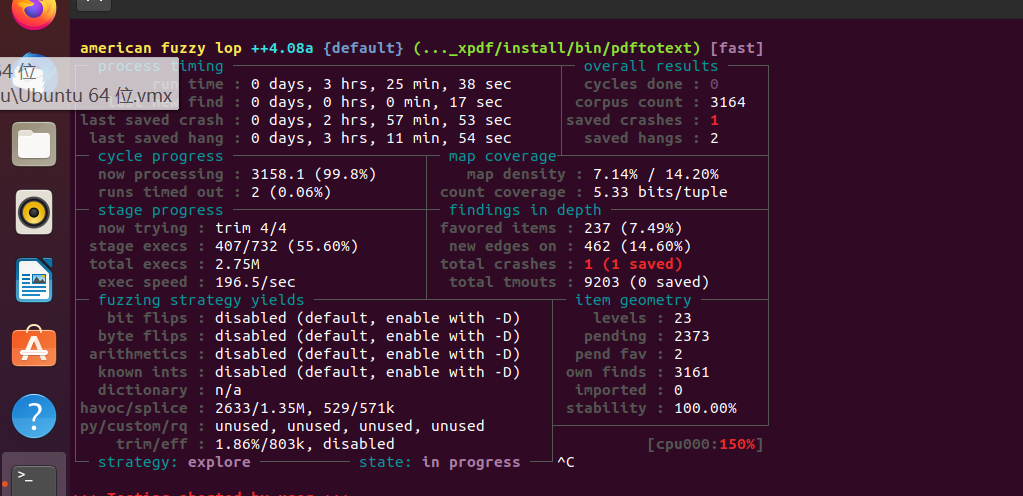
下载afl++



使用 afl-clang-fast 编译器构建 xpdf

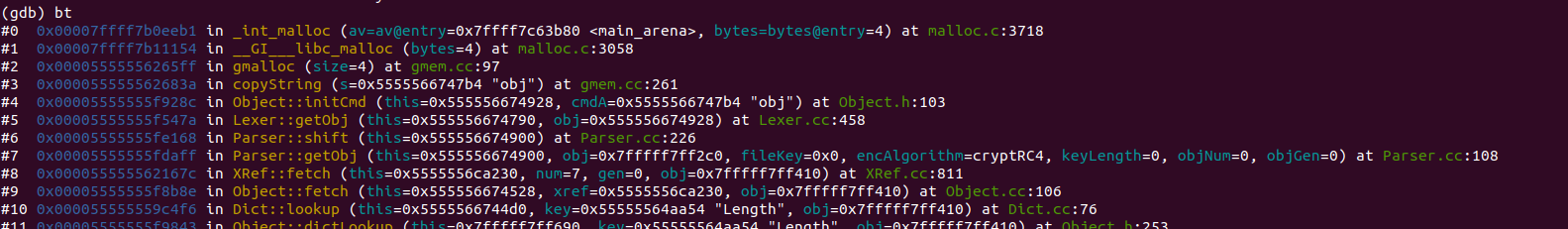
使用命令运行模糊程序

* afl-fuzz -i $HOME/fuzzing\_xpdf/pdf\_examples/ -o $HOME/fuzzing\_xpdf/out/ -s 123 -- $HOME/fuzzing\_xpdf/install/bin/pdftotext @@ $HOME/fuzzing\_xpdf/output
* *-i* 表示我们必须放置输入案例的目录（又名文件示例）
* *-o* 表示 AFL++ 将存储突变文件的目录
* *-s* 表示要使用的静态随机种子
* *@@*是占位符目标的命令行，AFL 将用每个输入文件名替换该命令行



运行gdb找出crash的原因

gdb --args $HOME/fuzzing\_xpdf/install/bin/pdftotext $HOME/fuzzing\_xpdf/out/default/crashes/<your\_filename> $HOME/fuzzing\_xpdf/output



报错信息Program received signal SIGSEGV, Segmentation fault，存在内存泄漏

报错位置 \_int\_malloc (av=av@entry=0x7ffff7c6bb80 <main\_arena>, bytes=bytes@entry=4) at malloc.c:3718

执行流信息，可以看出调用过程是循环的.

下载xpdf4.02，对比发现只是添加了一个限制循环次数的变量。限制次数为500.