陈奕诺 191220013

## 为什么在装载时要把内存中剩余的 p_memsz - p_filesz 字节的内容清零?

p_filesz 是段在文件中所占的长度，而 p_memsz 是段在内存中所占的长度。p_memsz 大于 p_filesz 说明其中可能包含可能包含.bss 部分，.bss 节在文件中不占用磁盘空间，但是在存储器中要分配给它大小相同的空间。将 p_memsz - p_filesz 字节的内容清零，有未初始化的全局变量，初值为 0，这是 EFL 的规范。