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。