1. 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?

否则若上一次装载时若旧的 p_filesz 大于新的 p_filesz, 位于它们之间的数据没有被覆盖而仍然存在，执行程序时，eip 指针可能会访问到新的 p_filesz 后面的内容，出现难以预料的效果。清零可以保证 p_filesz 与 p_memsz 之间均为安全值 0，防止这种情况发生。