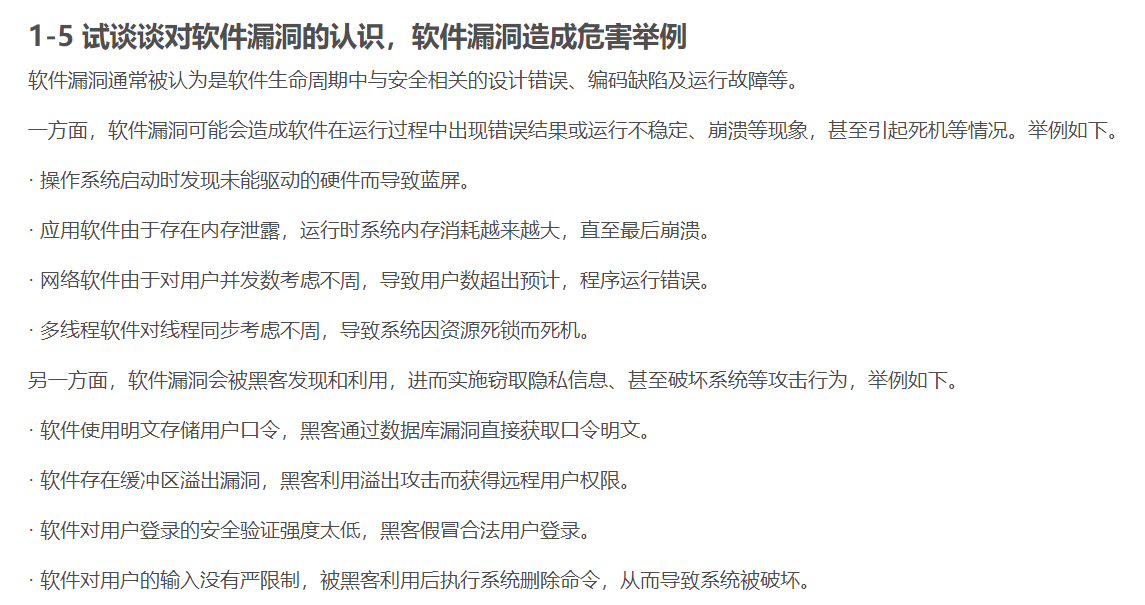
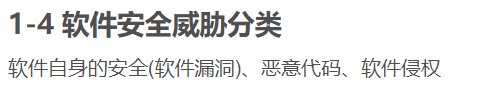
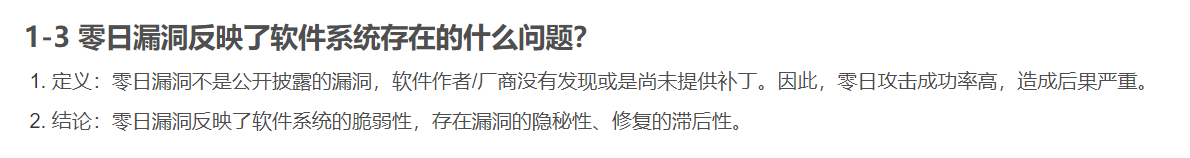
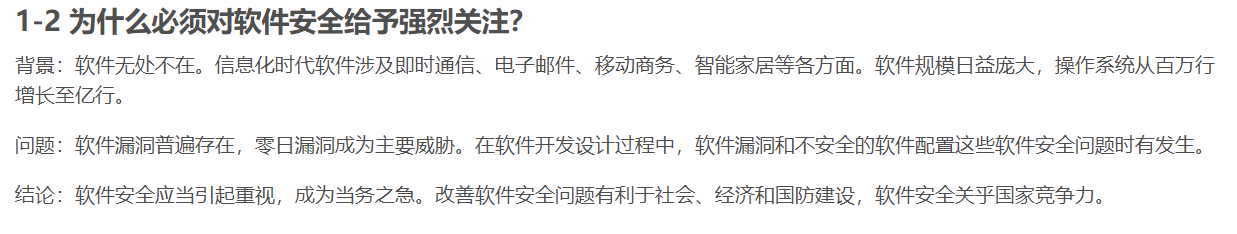
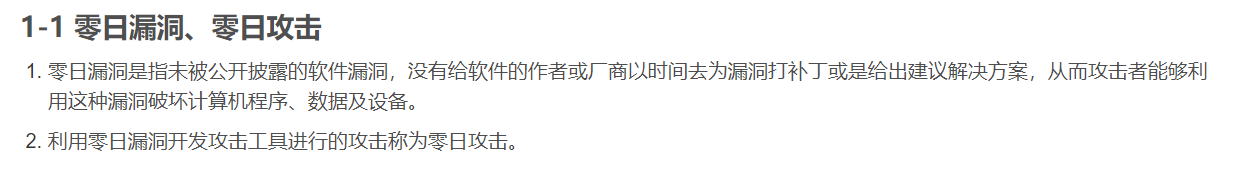
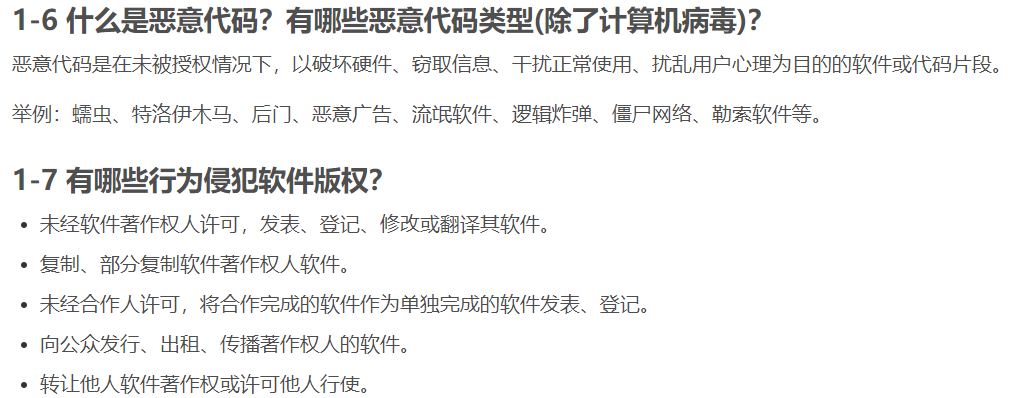
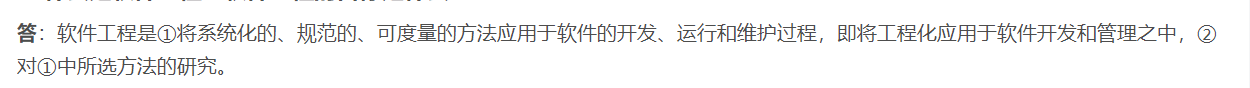
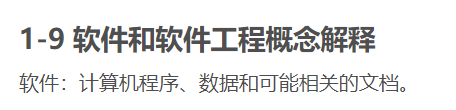
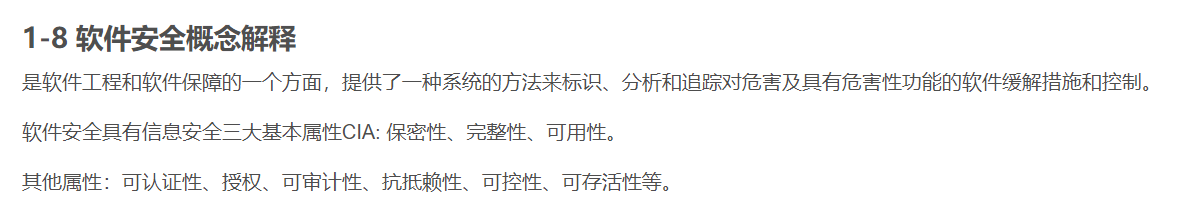
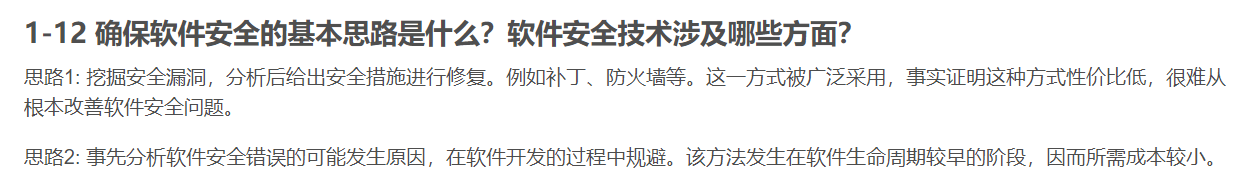
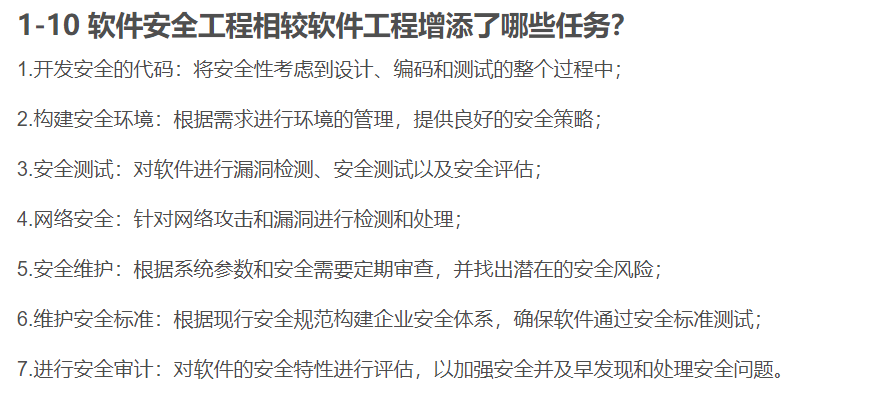
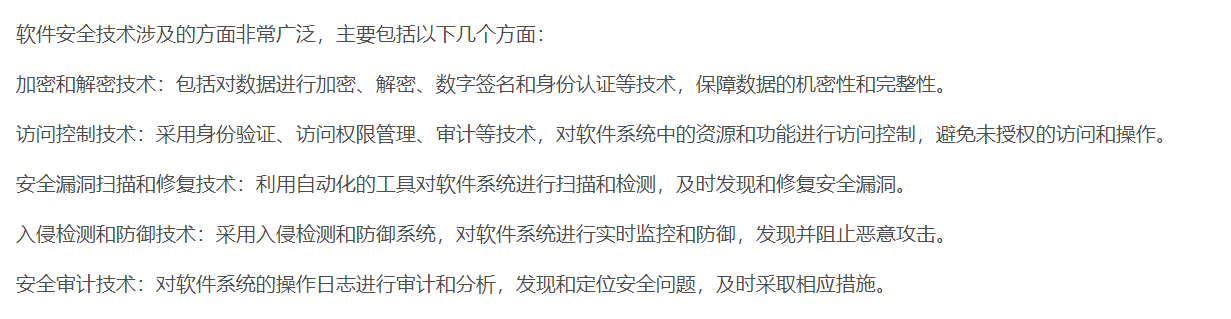
### 第一章



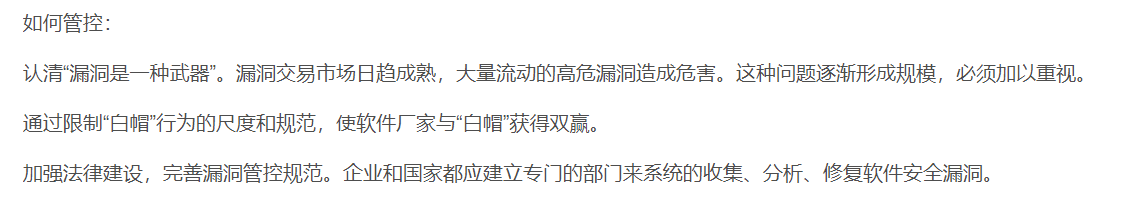
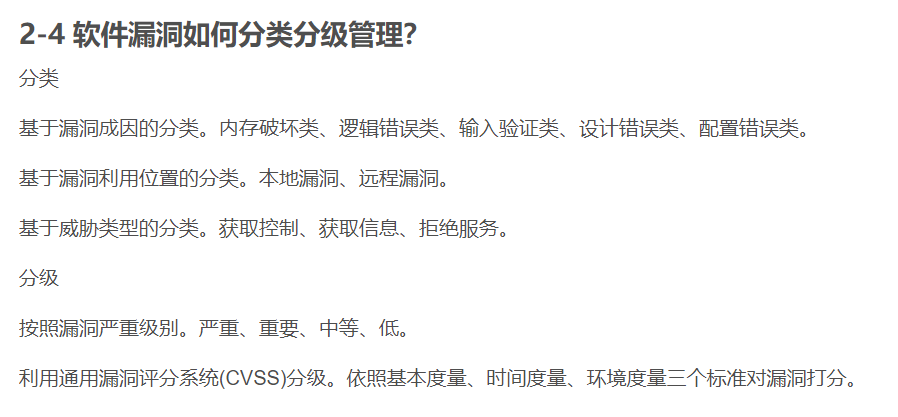
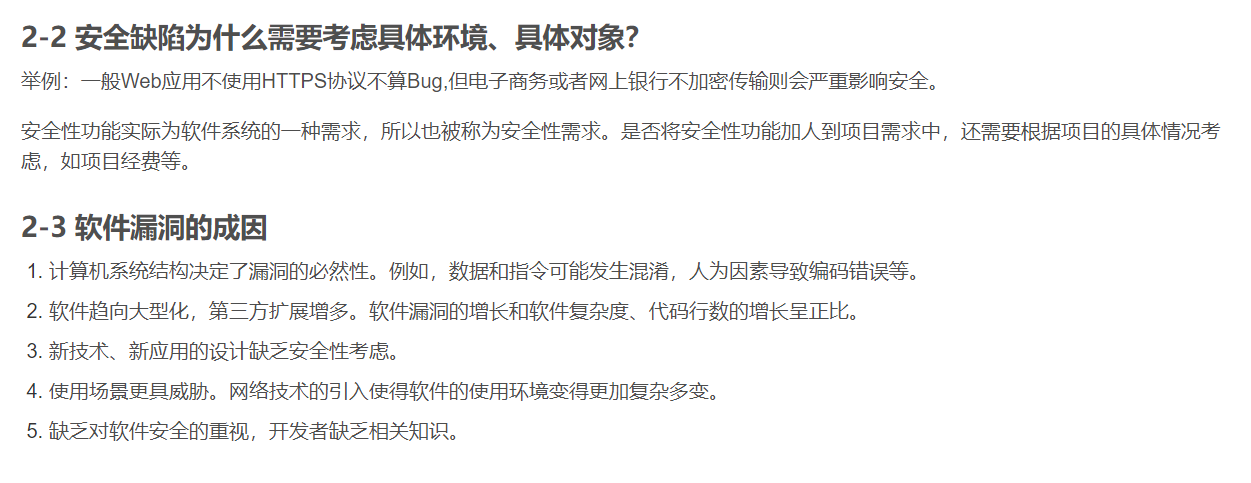
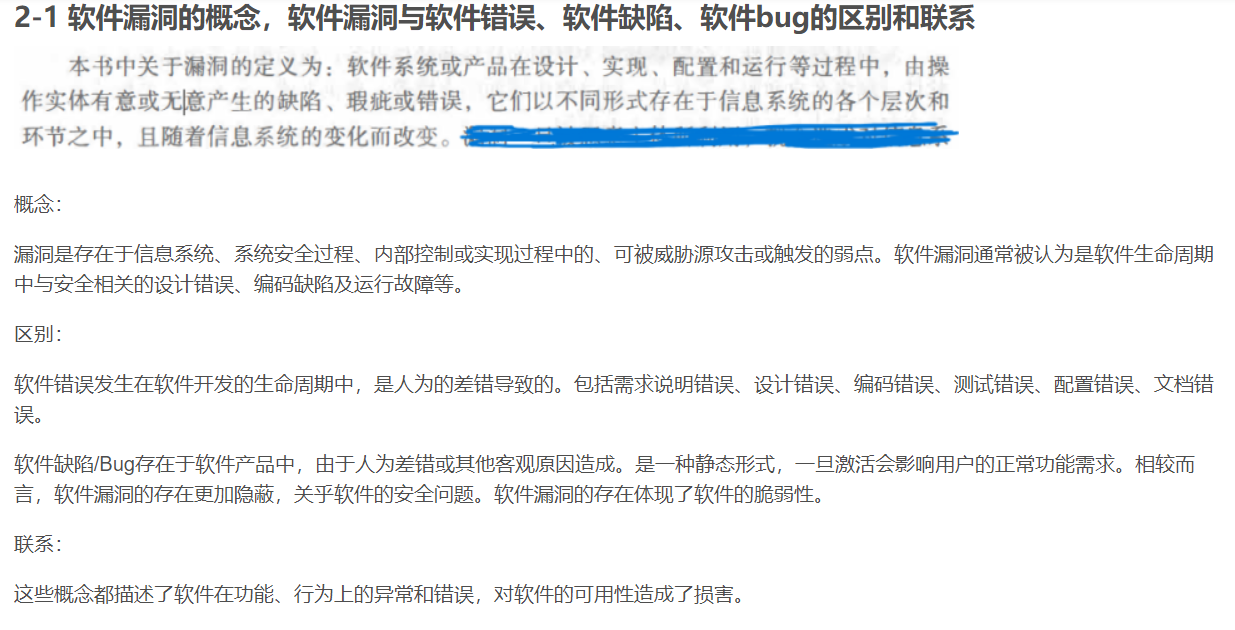






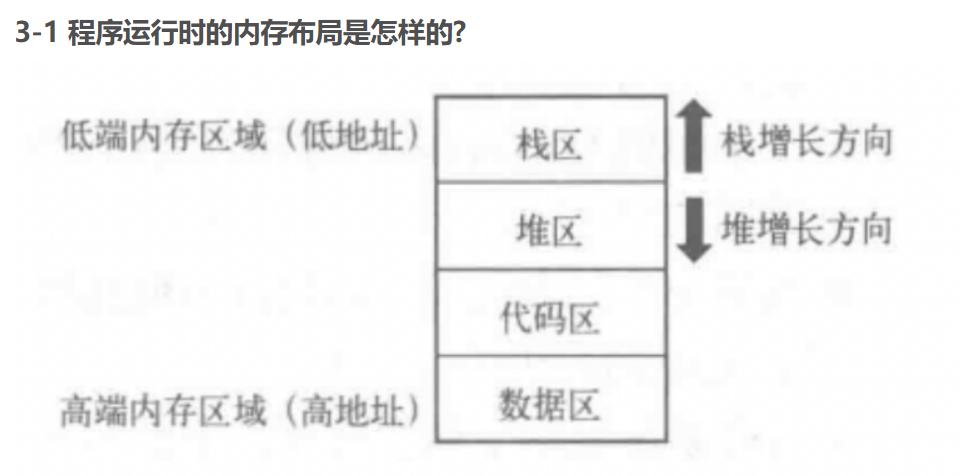
未添加：1-11：谈谈软件安全与软件危机、软件质量和软件质量保证、软件保障、软件可靠性、应用软件系统安全、可信软件和软件定义安全等概念的区别和联系

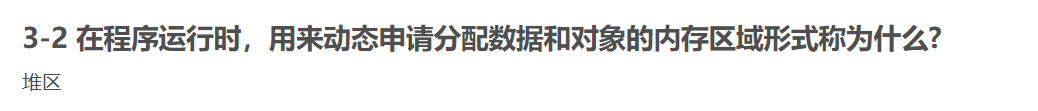
### 第二章

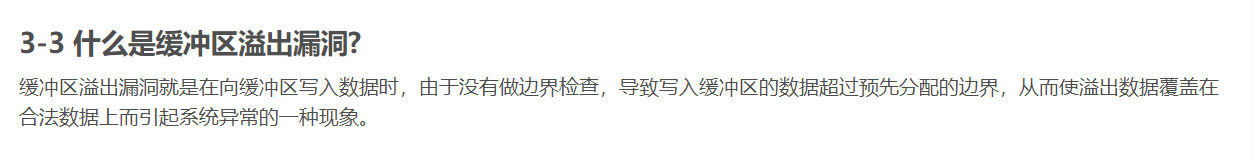


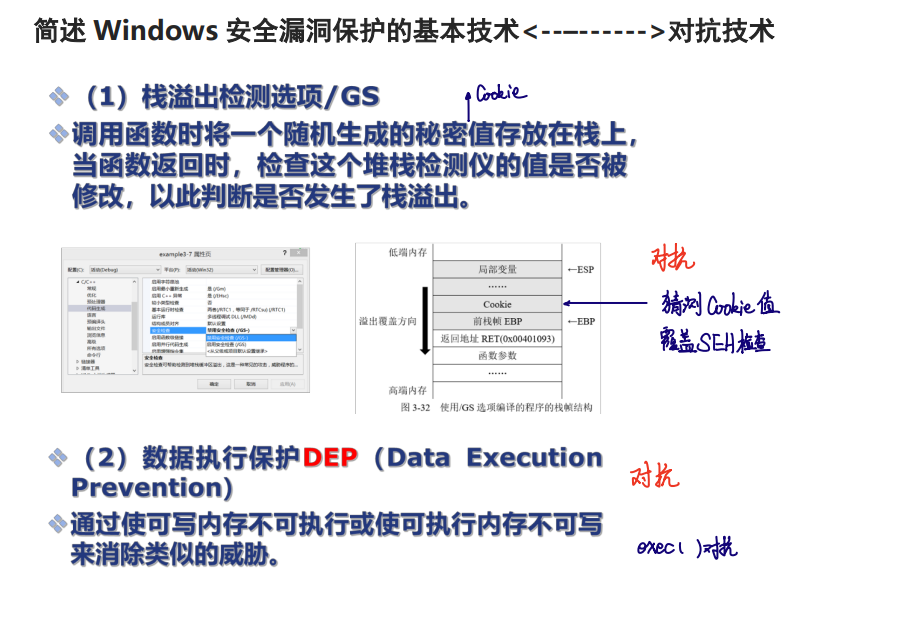


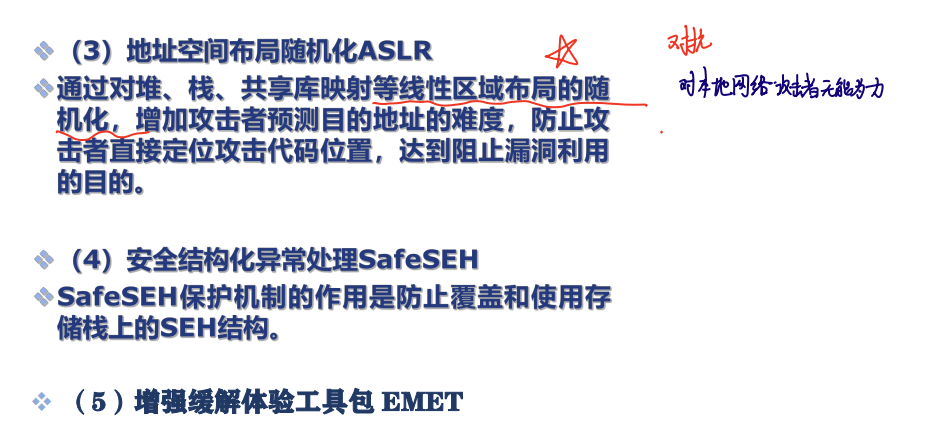
### 第三章













Address Space Layout Randomization Enhanced Mitigation Experience Toolkit

分别的问题：

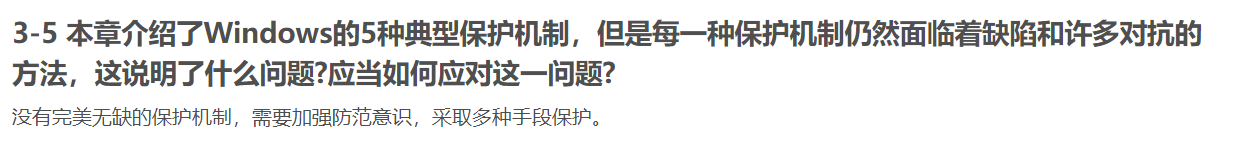
1.cookie值可以被猜测 2.Cookie可以被修改 3.覆盖SEH绕过Cookie检查 4.覆盖父函数的栈数据绕过Cookie检查。

可以执行已经加载的模块中的指令或利用栈上的数据作为函数/指令的参数

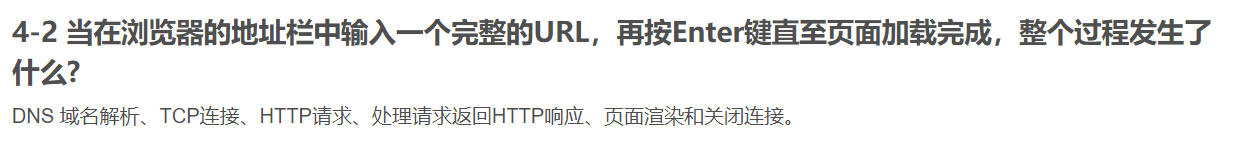
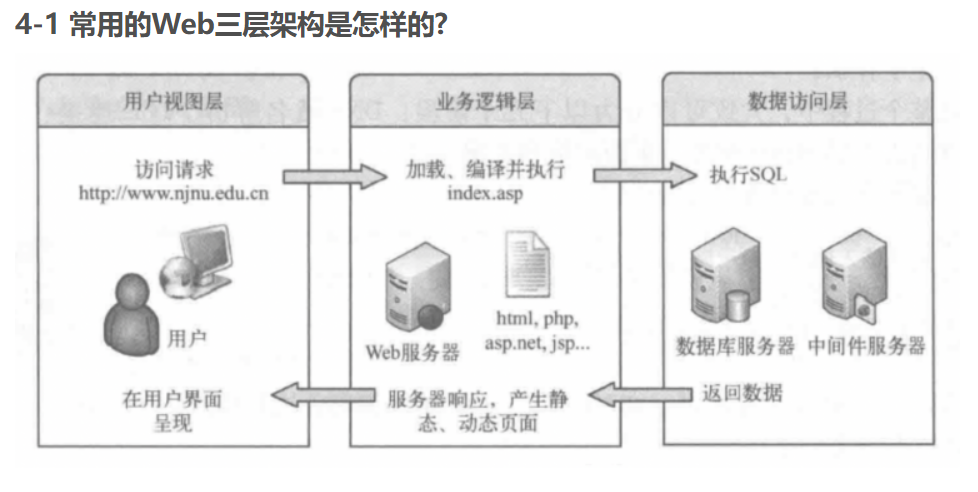
1. 对于本地网络攻击者无能为力 2.造成内存碎片增多

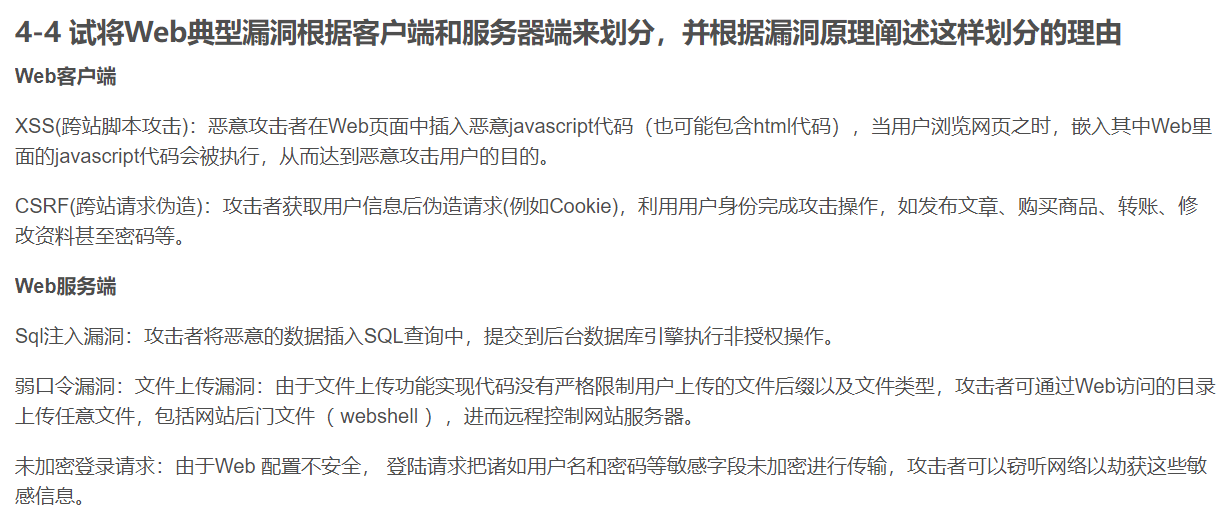
当进程中存在一个不支持SafeSEH的模块时，整个SafeSEH的机制就可能失效

EMET不是操作系统的一部分，会给操作系统的性能，可靠性以及会给其上运行的应用程序带来严重的副作用，且未跟上windows发展的步伐



### 第四章：

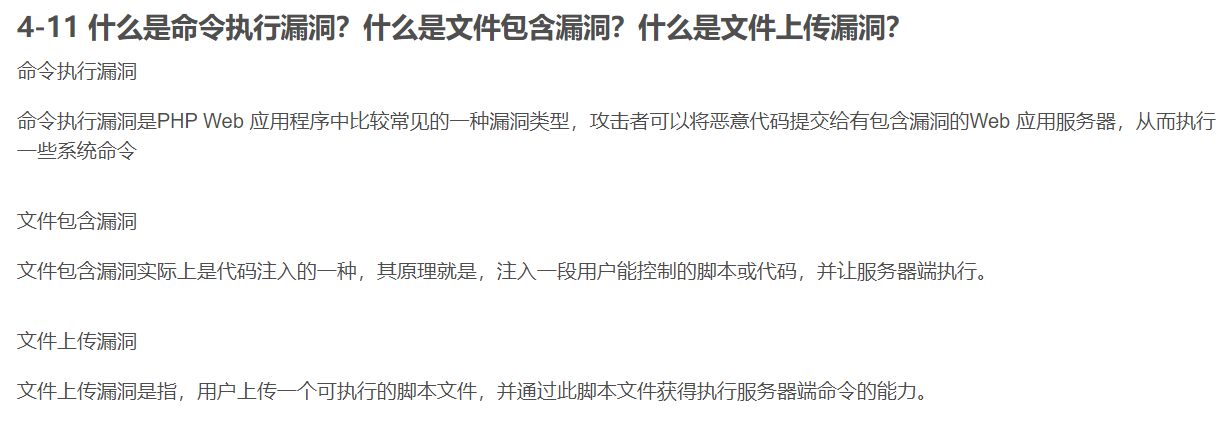
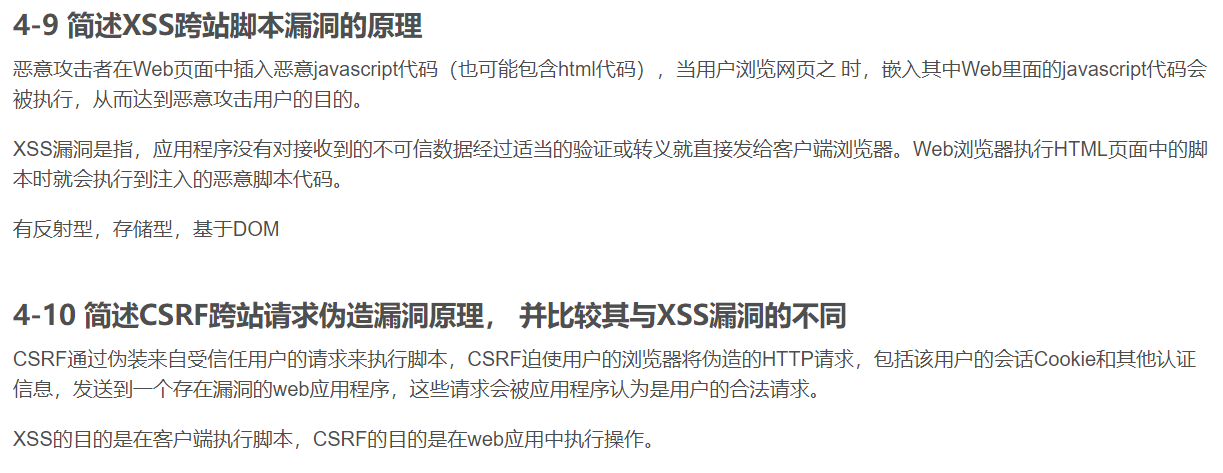
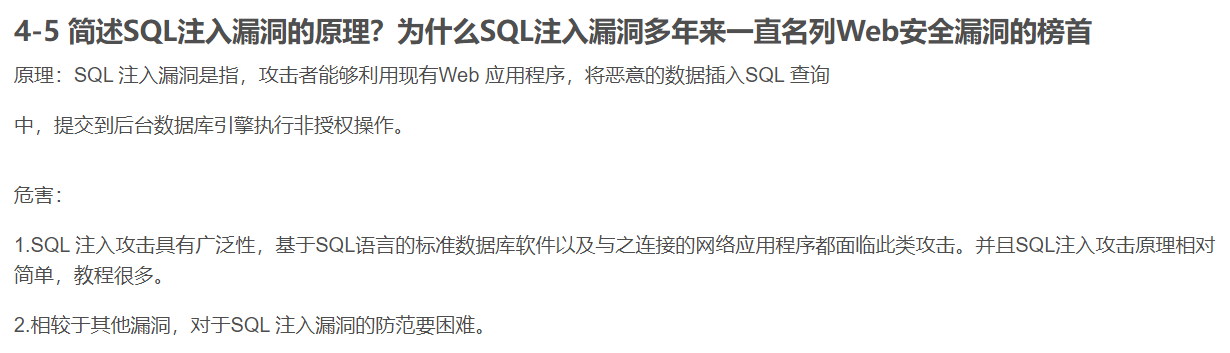




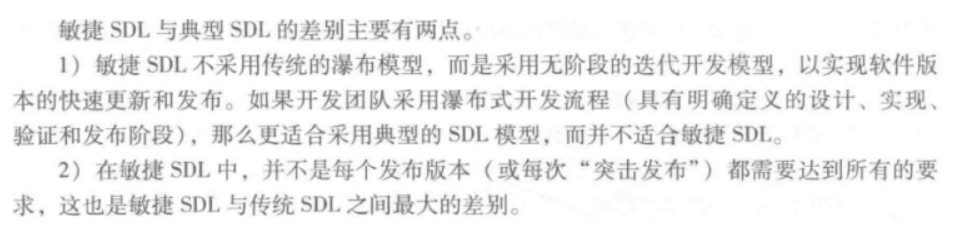
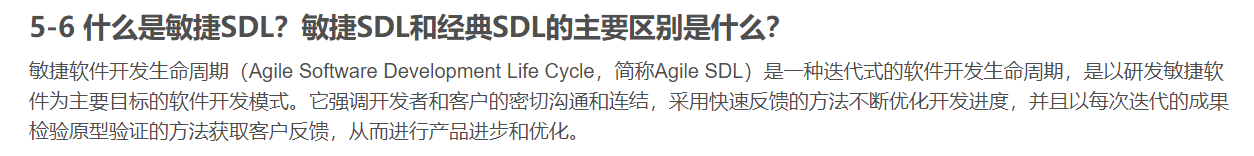
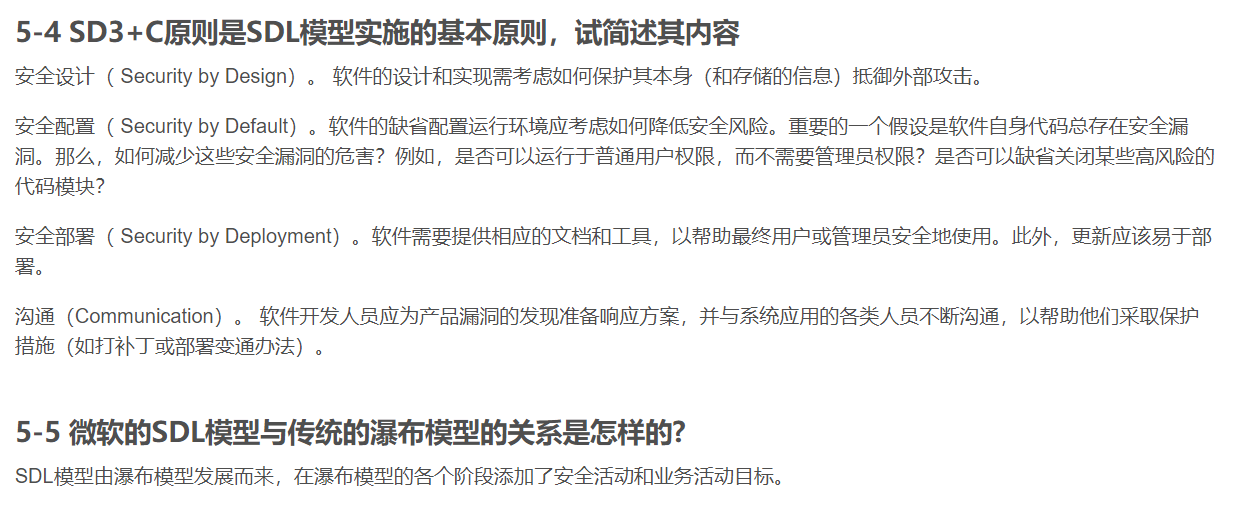
服务端：sql注入、命令执行漏洞、文件包含漏洞、文件上传漏洞

定义看下面的题目

Cross-Site Scripting Cross-Site Request Forgery



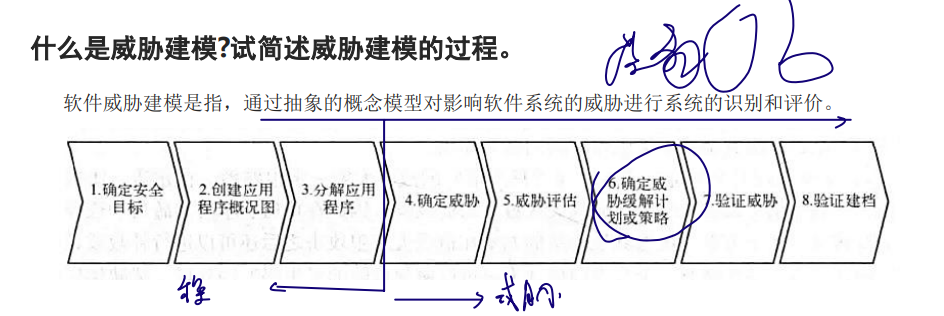
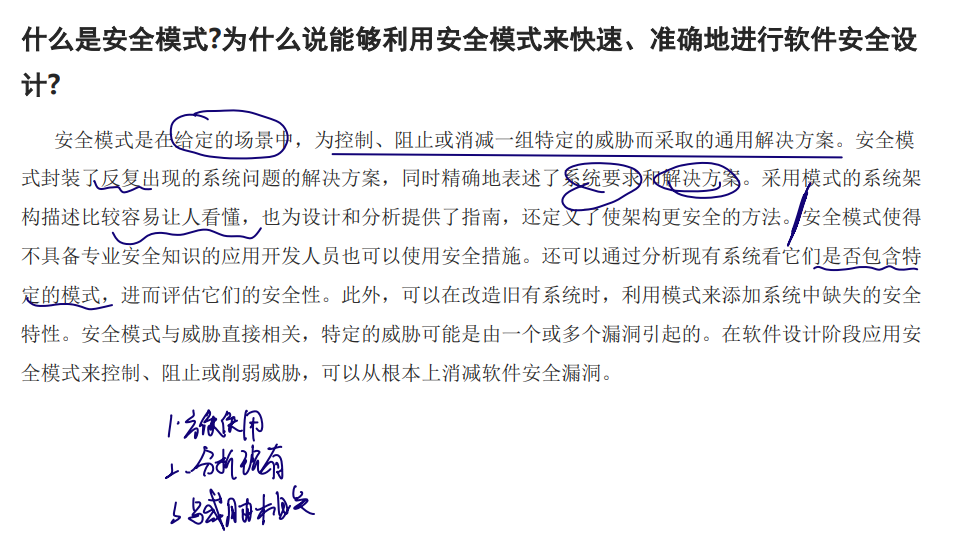
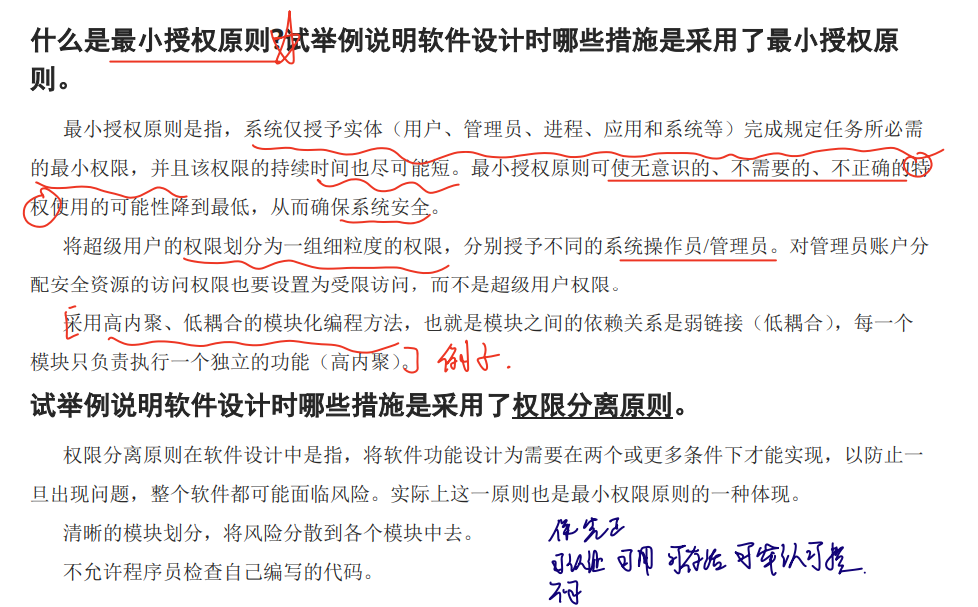
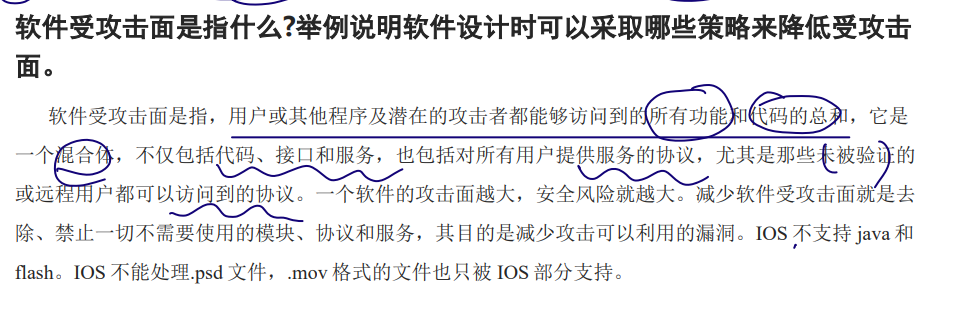
### 第五章



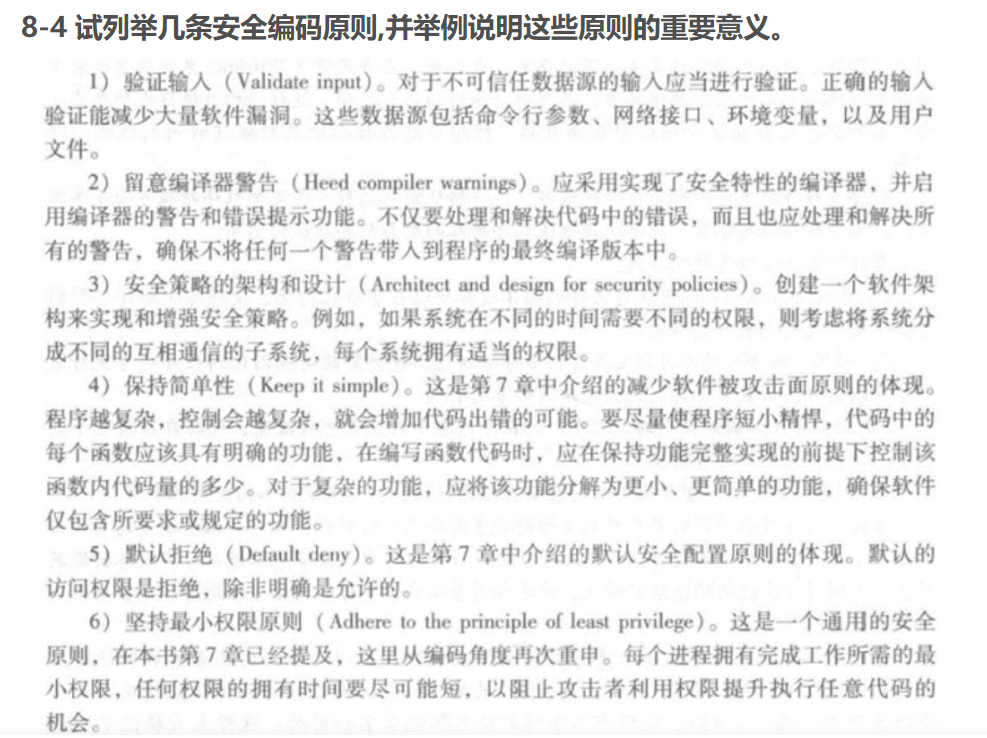
### 第六章

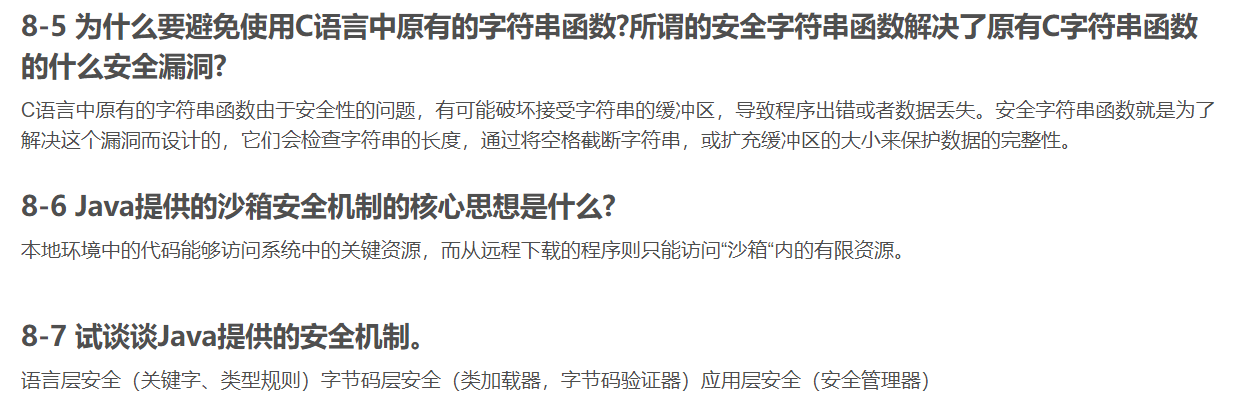


### 第七章

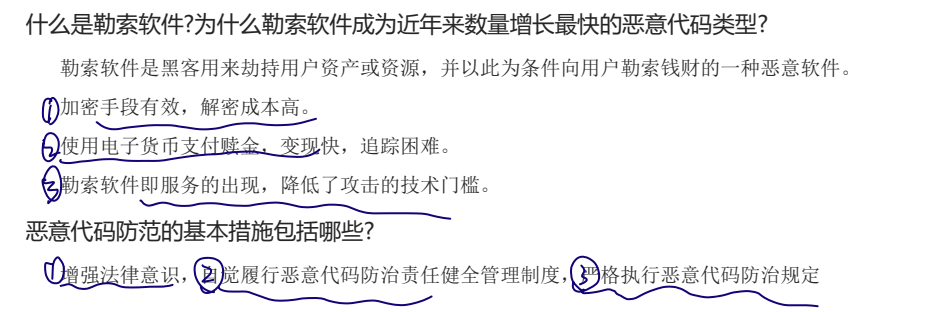
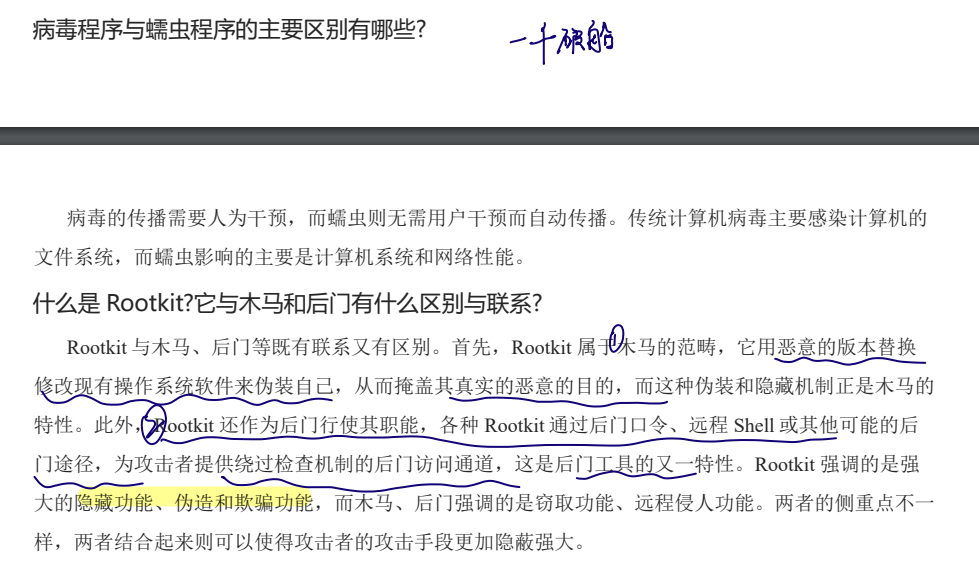


### 第八章





### 第十二章



### 第十四章

