第一章：

1) 一些概念，需要理解什么是软件安全，软件安全都包含哪一些研究内容；进程内存分类，各类别内存的作用。
2) 栈的运行机制，函数调用时栈的变化机制。
3) 重点细节：可执行文件格式、函数调用栈结构、PE 文件结构，ELF 与 PE 文件格式差异

第二章：

4) 字符编码的知识，UTF-8 编码；字符串的概念，C/C++字符串的实现；
5) 常见的字符串操作错误；
6) 常见字符串漏洞的种类；缓冲区溢出深入理解；字符串处理函数；
7) 重点细节：Unicode 编码、UTF-8 编码格式、UTF-8 编码合法性；差一错误；安全字符串函数

第三章：

8) 指针分类；
9) 全局偏移表；.dtors 区；虚指针；
10) 异常处理与缓解方法；

重点细节：C++虚表机制、函数指针攻击目标、控制流劫持、strcpy 风险与安全替代方案、缓冲区溢出（strcpy 风险）、虚表攻击原因（指针未验证）、GOT 劫持（strcpy 调用劫持）、strcpy 风险与安全替代方案。

第四章：

11) 内存的用途；常见内存分配算法；基本的内存管理函数；常见的内存管理错误；
12) 基本 C/C++的内存管理错误；dlmalloc 机制：内存管理数据结构、unlink、

frontlink 导致的 dlmalloc 问题；RTLheap 机制：内存管理数据结构，相应的问题，比如双重释放漏洞等；

13) Fuzz 测试相关的步骤与流程；
14) 重点细节：calloc/malloc、变量存储位置、空闲块结构、RtlHeap 机制、动态内存管理未检查返回值、UAF 漏洞检测与防御、伙伴系统内存分配算法、篡改堆管理结构、dlmalloc 空闲块篡改、Windows 堆边界标志、双重释放、Windows SEH 链篡改。

第五章：

15) 整数的表示，原码、反码和补码，整数操作出错的情形；整数的回绕；整数的溢出；整数可能的漏洞。
16) 重点细节：补码表示与整数溢出、有符号数乘法溢出检测、整数截断与类型提升、后验检测法局限性、malloc 参数校验、符号错误导致溢出、strlen 返回值类型与截断风险;

第六章：

17) 变参函数原理：格式化字符串、变参函数的原理；
18) 格式化输出函数的漏洞；
19) 格式化的缓解策略都有哪一些？
20) 重点细节：格式化字符串漏洞利用、格式化字符串漏洞（%n 覆写返回地址）、变参函数宏详细含义、格式化字符串漏洞原因、%n 转换指示符作用、格式化字符串漏洞利用、ASLR 防御目标。

课堂作业

实验