第七章Web安全性

- Internet的脆弱性P226
  - 黑客入侵
  - TCP/IP通信协议
  - Unix操作
  - 电子信息
  - 电子邮件
  - 计算机病毒
- Web服务器的安全问题P227
  - 向公众提供了不应该提供的服务，导致在安全隐患
  - 把本应私有的数据敬妇到了公开访问区域，导致敏感息泄露
  - 信赖了来不可信赖数据源的数据，导致爱到攻击
- Web服务器的作用P228
  - Web服务器也称为WWW(World Wide Web)服务器
  - Web服务器的主要作用是提供网上信息浏览服务
  - 现在的服务器后台还包括数据库，用来更新前台的页面
  - Web可以提供将图形、音频、视频信息集合于一体的特性
- Web服务器存在的漏洞P228
  - 物理路径泄露
  - 目录遍历
  - 执行任意命令
  - 缓冲区溢出
  - 拒绝服务
  - SQL注入
  - 条件竞争
  - CGI漏洞
- IIS安全
  - IISP230
    - 即互联网信息服务，是由微软公司提供的基于运行Microsoft Windows的互联网基本服务。因其方便性和易用性，成为最受欢迎的b服务器软件之一
  - IIS安装注意事项P231
    - 不要安装在系统分区上
    - 修改默认安装路径
    - 打上Windows和IS的补丁
  - IIS的安全配置P231
    - 删除不必要的虚拟目录
    - 删除危险的S组件
    - 为IS文件设置权限
    - 删除不必要的应用程序映射
    - 保护系统日志
- 脚本语言的安全性
  - CGI程序的安全性P234
    - CGI(Commom Gate Interface)外部应用程序与Web服务器眩互的一个标准接口
    - CGI应用程序可以完成客户端与服务器的交互操作
    - 几乎所有的CGI漏洞均来自与用户的交互，这种交互性在给主页带来活力的同时，成为Web服务器的一个潜在危险。
  - ASP的安全性P235
    - ASP(Active Server Page)动态服务器网页，其实质是运行于服务器端的脚本
    - 黑客可以通过特殊的工具利用ASP存在的漏洞获得管理员的密码
    - 还可以通过ASP网站架设的论坛实行攻击。
- Web浏览器的安全性
  - 浏览器本身的漏洞P238
    - 搜狗浏览器：“缓冲区溢出”漏洞；
    - IE7.0浏览器：“0day”漏洞；
    - 360浏览器：“缓冲区溢出”漏洞：
    - 火狐浏览器：被攻击者远程控制的漏洞
  - ActiveX的安全性
    - ActiveX控件三大组成腰素P240
      - 属性
      - 方法
      - 事件
    - 控件的安全问题P240
      - 导出函数可能具有隐蔽的逻辑功能
      - 通过控件可以获取本地私密信息
      - 控件本身的一些函数在处理参数时由于未对参数长度进行检查而导致字符串缓冲区溢出、整数溢出、格式化字符串漏洞导致浏览器或系统异常
      - 一些恶意控件可以通过欺骗行为使用户访问恶意网页、下载恶意程序等
    - 漏洞检测与发现的方式P240
      - 使月Fuzz测试工具
      - 人工分析方法
    - 漏洞的安全防范P241
      - 使用特征安全的ActiveX控件
      - 使用ActiveX控件前进行漏洞检测
      - 安装补丁文件
      - 浏览器中的安全设置
      - 屏蔽所有非主动安装的控件
      - 使用安全软件
  - Cookie的安全性P243
    - Cookie指某些网站为了辨别用户身份、进行Session.跟踪而储存在用户本地终端上的数据（通常经过加密）
    - Cookie是由服务器端生成，发送给浏览器，浏览器将会把Cookie的key/value保存到某个目录下的文本文件内，下次请求同一网站时就发送该Cookie?给服务器
    - 尽管Cookie没有病毒那么危险，但它仍包含了一些敏感信息：用户名，计算机名，使用的浏览器和曾经访问的网站