Web攻击及防御技术

- Web安全
  - 三方面
    - 服务器
      - 利用Web服务器的漏洞
      - 利用网页自身的安全漏洞
      - 实例
        - 服务器程序编写不当导致缓冲器溢出
        - 针对服务器系统的拒绝服务攻击
        - 脚本程序编写不当，SQL注入
        - 乐观的相信用户的输入，导致跨站脚本攻击
    - 客户端
      - 网页木马
      - XSS
    - 通信信道
      - 拒绝服务攻击
        - 网络嗅探
        - 拥塞信道
        - 耗费资源
  - 安全问题
    - 未验证参数
    - 访问控制缺陷
    - 账户及会话管理缺陷
    - 跨站脚本攻击
    - 缓冲区溢出
    - 命令注入
    - 错误处理
    - 远程管理
    - Web服务器及应用程序配置不当
  - 指纹识别
    - 流程
      - 对指纹进行收集和分类
      - 将未知的指纹同被存储在数据库中的指纹进行比较，找出做符合的。
    - Web服务Banner信息获取
      - 对目的主机80端口发送一个请求，查看Header的Server字段就可以看到Banner
      - 防御
        - 自定义Banner头信息
    - 发送畸形的HTTP请求，不同的服务器产生不同的响应
    - 攻击
      - Httprint
  - 页面盗链
    - 通过网页源码的分析，找出可能存在于代码、注释或者设计中的关键缺陷和脆弱点
    - 方法
      - 逐页手工扫描
      - 自动扫描
    - 防御方法
      - 提高代码质量
      - 监视访问日子中快速增长的GET请求
      - 设置garbage.cgi脚本
  - 跨站脚本攻击
    - XSS
      - 在Web页面里面插入恶意html代码，当用户浏览该网页时，嵌入其中的HTML代码会执行。
    - 危害
      - 修改用户账户，盗取Cookie，做虚假广告，查看主机信息。
    - 先决条件
      - 有跨站脚本漏洞的Web应用程序
      - 需要用户点击链接或者是访问某一页面
    - 流程
      - 寻找XSS漏洞
      - 注入恶意代码
      - 欺骗用户访问
  - SQL注入
    - 原因
      - 程序员的水平经验不够
      - 对输入的参数不进行检查和过滤
    - 过程
      - 寻找可能存在SQL注入漏洞的连接
      - 测试该网站是否存在SQL注入漏洞
      - 猜管理员账号表
      - 猜测管理员表中的字段
      - 猜测用户和密码的长度
      - 猜测用户名
      - 猜测密码
  - Google Hacking
    - 利用Google的一些语法搜索功能去搜索有漏洞的URL等。
  - 网页验证码
    - 区分人机交互问题
    - 防御
      - 自动灌水机
      - 广告机
      - 自动注册机
      - 用户密码破解机
    - 类型
      - 文本验证码
      - 手机验证码
      - 邮件验证码
      - 图片验证码
    - 防范验证码攻击
      - 不应该使用安全性很差的文本验证码
      - 尽量不使用手机验证码、邮件验证码，以避免手机/邮件DOS攻击
      - 使用安全性较高的图片验证码
  - 防御Web攻击
    - Web服务器的安全配置
      - 主机系统的安全配置
        - 简单性
        - 超级用户权限
        - 本地和远程访问控制
        - 审计和可审计性
        - 恢复
      - Web服务器的安全配置
        - Windows
          - IIS
            - 删除不必要的虚拟目录
            - 删除微信的IIS组件
            - 为IIS中的文件分类设置权限
            - 删除不必要的应用程序映射
            - 保护日志安全
        - Unix/Linux
          - 不用root运行Web服务器
          - 限制Web服务器开账户，定期删除一些用户
          - 对Web服务器上面的账户定期修改口令
          - 尽量与其他的FTP，Mail服务器分开。
          - 定期查看日志
          - 对不同目录设置不同的属性
    - Web浏览者的安全措施
      - 经常对操作系统打补丁、升级
      - 使用漏洞较少的浏览器
      - 经常对浏览器进行升级
      - 不要因为好奇而打开一些不信任的网站
  - 五个误区
    - 使用了SSL加密，所以很安全
      - SSL只是在通信信道上
    - 使用了防火墙所以很安全
      - 防火墙并不是不可突破的
    - 漏洞扫描工具没有发现问题很安全
      - 扫描工具永远落后于漏洞
    - 安全问题是程序员的造成的
      - 有些一问题，程序员也不可控
    - 我们每年都对Web做安全评估所以很安全
      - 当代码变动的时候，就有可能出问题