# Web应用安全测试核对表--渗透版

信息收集：

□ 手工探索公开内容

□ 爬虫抓取隐藏内容 （Spider）

□ 域名收集（whois, 子域名, cdn, 真实ip, C段ip, 同服站点等）

□ 敏感文件（Robots.txt, Sitemap.xml, .DS\_Store, GIT, 备份文件等）

□ 搜索引擎信息发现和侦查Google Hack

□ 识别更改User Agent检查内容差异（XFF ClientIP等）

□ Web服务器（指纹 环境信息 脚本等）

□ 识别应用入口（普通用户/管理员入口）

□ 识别多个版本/通道（Web, Mobile Web, Mobile App Web服务等）

□ 识别所有主机和端口(弱点端口扫描等)

□ 识别第三方托管内容

□ 绘制应用架构图

配置管理

□ 检查旧版代码 备份文件和未被引用文件

□ 检查支持HTTP方法和跨站追踪（Cross Site Tracing）

□ 测试文件扩展名处理（解析漏洞）

□ 测试安全HTTP头（CSP,X-Frame-Options,HSTS）

□ 测试代码中敏感数据（API keys 用户凭证）

安全传输

□ 检查SSL版本，算法，密钥长度（心脏滴血）

□ 检查数字证书有效期（持续时间，签名和CN）

□ 检查仅通过HTTPS传递的凭据

□ 检查登陆表单是否通过HTTPS传输

□ 检查是否使用HTTP严格传输安全（HSTS）

认证

□ 测试用户枚举

□ 测试认证绕过（后台绕过, cookie欺骗, 万能密码）

□ 测试后台弱口令暴力破解

□ 测试验证码（爆破/固定/自动识别打码）

□ 测试HTTP上的缓存管理（Pragma , Expires, Max-age）

□ 测试账户锁定和更改密码成功的通知情况（密码找回绕过手机/邮箱认证等）

会话管理(Session)

□ 判断Web应用如何处理会话管理（Cookie中的Token，URL中的Token等）

□ 检查Cookie标志的会话标记（httpOnly和secure）

□ 检查会话Cookie作用域（Path, Domain）

□ 检查会话Cookie 存活期（过期时间等）

□ 测试会话Cookie随机性（固定session/Cookie）

□ 测试在用户登陆 切换用户 注销用户 是否更新会话token

□ 测试跨应用使用共享会话是否等同一致会话（跨应用登陆Session不变等）

□ 测试CSRF和点击劫持

授权

□ 测试目录遍历

□ 测试绕过授权模式（前端js注释授权代码）

□ 测试垂直越权访问（用户特权提升）

□ 测试水平越权访问（相同特权级别两个用户）

漏洞测试

□ 测试前端漏洞

□ 测试跨站脚本（XSS）

□ 测试反射型跨站脚本（Reflected XSS）

□ 测试存储型跨站脚本（stored XSS）

□ 测试基于DOM跨站脚本（DOM XSS）

□ 测试Flash跨站脚本（Cross Site Flashing）

□ 测试HTML注入

□ 测试跨站请求伪造（CSRF）

□ 测试LDAP注入（轻量级目录访问协议注入）

□ 测试ORM注入（Java ORM框架注入）

□ 测试XML注入（XML实体注入）

□ 测试XXE注入（XML外部实体注入Blind-XXE,DTD等）

□ 服务端漏洞

□ 测试远程命令执行/代码执行（Remote Command/Code Execute）

□ 测试SSI注入 （服务端包含注入）

□ 测试SSRF注入

□ 测试XPATH注入

□ 测试XQuery 注入

□ 测试IMAP/SMTP注入 （邮件服务器注入任意IMAP / SMTP命令）

□ 测试代码注入

□ 测试表达式注入

□ 测试命令注入

□ 测试溢出（堆栈 堆 整数）（Overflow (Stack, Heap and Integer)）

□ 测试字符串格式化漏洞

□ 测试HTTP 分割/伪造测试

□ 测试HTTP 方法更改

□ 测试HTTP参数污染（HPP）

□ 测试NULL/无效会话Cookie

□ 测试反序列化漏洞

□ 测试STRUCT2漏洞

□ 测试SQL注入

□ Orcale注入

□ MySQL注入

□ SQL Server注入

□ PostgreSQL注入

□ MS Access注入

□ NoSQL注入

□ 报错注入

□ 联合查询

□ 堆查询注入

□ 二阶注入

□ SQL盲注（布尔 时间 报错）

文件操作

□ 测试本地文件包含

□ 测试远程文件包含

□ 任意文件下载

□ 其他文件操作

□ 中间件漏洞 （nginx iis7.5 6.0）

□ 上传bypass检测（黑名单, 白名单+解析, 截断, htaccess）

□ 编辑器漏洞

其他漏洞

□

□

□

□

□

□

□

□

□