# Web应用安全测试核对表

信息收集：

□ 手工探索网站

□ 爬虫抓取隐藏内容 （Spider）

□ 检查公开内容文件（Robots.txt, Sitemap.xml, .DS\_Store等）

□ 搜索引擎Google Hack

□ 识别更改User Agent检查内容差异（XFF ClientIP等）

□ 识别Web应用指纹

□ 识别脚本语言，Web环境信息

□ 识别用户角色

□ 识别应用程序登入点

□ 识别客户端代码

□ 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

□ 识别第三方托管内容

配置管理

□ 检查常用应用程序和管理者URLs

□ 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

□ 测试安全HTTP头（CSP,X-Frame-Options,HSTS）

□ 测试策略（Flash Silverlight ,Robots）

□ 测试非生产数据于生产环境中

□ 测试客户端代码中敏感数据（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阉割传输安全性设置（HSTS）

认证

□ 测试用户枚举

□ 测试认证绕过

□ 测试暴力破解

□ 测试密码质量规则

□ 测试记住密码功能

□ 测试是密码表单/输入自动填充

□ 测试密码重置/密码找回

□ 测试验证码（爆破/固定/自动识别打码）

□ 测试多因素认证

□ 测试注销功能

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

□ 测试默认登陆

□ 测试用户可访问认证记录

□ 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）

□ 测试使用共享身份/SSO跨应用验证密码（微博使用qq登陆等）

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）

□ 检查会话在最长生命周期后终止情况

□ 检查会话在相对超时后终止情况

□ 检查会话在注销后终止情况

□ 测试用户是否有多个同时运行的会话

□ 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）

□ 测试会话复杂程度

□ 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）

□ 测试不存在授权认证

数据验证

□ 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（HTML Inject）

□ 测试SQL注入 （SQL Inject 盲注等）

□ 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）

□ 测试SSI注入 （服务端包含注入）

□ 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

□ 测试潜伏式漏洞

□ 测试HTTP 分割/伪造测试

□ 测试HTTP 方法更改

□ 测试重定向

□ 测试本地文件包含

□ 测试远程文件包含

□ 测试比较客户端和服务器验证规则

□ 测试NOSQL注入

□ 测试HTTP参数污染（HPP）

□ 测试自动绑定

□ 测试质量分配

□ 测试NULL/无效会话Cookie

拒绝服务

□ 测试反自动化

□ 测试账户锁定

□ 测试HTTP协议DOS

□ 测试SQL通配符DOS

业务逻辑

□ 测试功能误用

□ 测试缺乏不可否认性

□ 测试数据完整性

□ 测试权限分离

加密

□ 检查是否加密数据

□ 检查上下文是否存在错误算法使用情况

□ 检查弱算法使用情况

□ 检查是否使用salt

□ 检查随机性功能

文件上传

□ 测试可接受文件类型是否列入白名单

□ 测试已经定义了上传文件大小限制，上传频率和总文件数量

□ 测试文件内容是否与定义文件类型匹配

□ 测试所有文件上传是否进行反病毒扫描

□ 测试不安全文件名是否被清理

□ 测试上传的文件不能在Web根目录直接被访问

□ 测试上传的文件不在相同的主机/端口上

□ 测试文件和其他媒体是否与身份验证/授权模式相匹配

卡支付

□ 测试Web服务器和Web应用已经漏洞和配置问题

□ 测试默认霍克猜测的面膜

□ 在生产环境测试非生产数据

□ 测试注入漏洞

□ 测试缓冲区溢出

□ 测试不安全的密码存储

□ 测试传输层保护不足

□ 测试不正确的错误处理

□ 测试既有漏洞

□ 测试身份验证和授权问题

□ 测试CSRF

HTML5

□ 测试Web消息

□ 测试Web存储SQL注入

□ 测试CORS实施情况

□ 测试离线Web应用