Web应用程序安全测试备忘录

legend / 2017-12-15 14:51:00 / 浏览数 3211 安全技术 资源分享 顶(0) 踩(0)

Web应用程序安全测试备忘录
介绍
此备忘录提供了在Web应用程序的黑盒安全测试期间要执行的检查列表。

目的
此列表旨在用作经验丰富的测试人员的备忘录，并建议与OWASP测试指南一起使用。

清单
信息收集
网站审查
手动探索网站
蜘蛛/抓取错误或隐藏的内容
检查Web服务器文件以查找泄露内容的信息，例如robots.txt，sitemap.xml，.DS_Store
利用搜索引擎发现 / 侦察检测信息泄露
根据用户不同页面检查内容的差异（例如，移动网站，利益搜索引擎爬虫访问）
检查信息泄漏的网页评论和METADATA数据

目标发展历史
检查Web应用程序框架
检查 Web应用程序指纹识别
确定使用的技术
识别用户角色
确定应用程序入口点
识别客户端使用的代码
识别多个版本/渠道（例如网络，移动网络，移动应用程序）
业务托管平台审查
确定Web服务
确定共同托管和相关的应用程序
确定所有主机名称和端口
识别第三方托管的内容
配置管理
检查常用的应用程序和管理网址
检查旧的，备份和未被引用的文件
检查支持的HTTP方法和跨站点跟踪（XST）
测试文件扩展名处理
测试RIA跨域策略
测试HTTP headers信息（例如CSP，X-Frame-Options，HSTS）
测试配置策略（例如Flash，Silverlight，robots）
检查客户端代码中的敏感数据（例如API密钥，相关认证信息）
安全传输
协议和加密

检查SSL版本，算法，密钥长度
检查数字证书有效期（持续时间，签名）
检查仅通过HTTPS传递的凭据
检查登录表单是否通过HTTPS传送
检查仅通过HTTPS传递的会话令牌
检查是否使用HTTP严格传输安全（HSTS）
测试伪造请求的能力
测试Web消息（HTML5）
检查CORS跨域信息（HTML5）
Web服务和REST
测试Web服务问题
测试REST
认证
应用程序密码功能
测试密码质量规则
测试记住我的功能
测试密码重置/找回功能
测试密码更改过程
测试CAPTCHA
测试多因素认证
测试存在注销的功能

测试默认登录
测试帐户锁定和成功密码更改的消息
使用共享身份验证模式/ SSO和备用渠道测试跨应用程序的身份一致性验证
测试弱安全问题/答案
额外的认证功能
测试用户枚举
测试旁路验证
测试暴力破解保护
测试通过加密通道传输的凭证
在HTTP上测试缓存管理（例如Pragma，Expires，Max-age）
测试用户可访问的认证历史
会话管理
确定如何在应用程序中处理会话管理（例如，Cookie中的令牌，URL中的令牌）
检查会话令牌的cookie标志（httpOnly和secure）
检查会话cookie作用域（路径和域）
检查会话cookie持续时间（过期和最大限度）
在最长使用期限后检查会话终止
检查会话超时后会话相对终止
注销后检查会话终止
测试用户是否可以同时进行多个会话
测试会话cookie的随机性
确认在登录，角色更改和注销时发出新的会话令牌
使用共享会话管理测试跨应用程序的一致会话管理
测试会议令人困惑
测试CSRF和点击劫持
鉴权
测试路径遍历
测试垂直访问控制问题（也称为权限提升）
测试水平访问控制问题（在相同级别的两个用户之间越权）
测试缺少的鉴定机制
测试不安全的直接对象引用
加密
检查应该加密的数据是否加密
根据上下文检查错误的算法使用情况
检查弱算法的使用情况
检查是否正确使用盐分
检查随机性功能
数据验证
注入
测试HTML注入
测试SQL注入
测试LDAP注入
测试ORM注入
测试XML注入
测试XXE注入
测试SSI注入
测试XPath注入
测试XQuery注入
测试IMAP / SMTP注入
测试代码注入
表达式语言注入测试
测试命令注入
测试NoSQL注入
其他
测试反射跨站点脚本
测试存储的跨站脚本
测试基于DOM的跨站点脚本
测试跨站点闪烁
测试溢出（堆栈，堆和整数）
测试格式字符串
测试组合攻击的漏洞
测试HTTP拆分
测试HTTP Verb Tampering
测试打开重定向
测试本地文件包含
测试远程文件包含
比较客户端和服务器端验证规则
测试HTTP参数污染
测试自动绑定

测试Mass Assignment
测试NULL /无效会话Cookie
测试数据的完整性
测试工作流程的规避
测试防止应用程序被误用
测试一个功能或特性不能用于限制之外
测试过程时间
Web存储SQL注入测试（HTML5）
检查离线Web应用程序
拒绝服务
测试反自动化
测试帐户锁定
测试HTTP协议DoS
测试SQL通配符DoS
特定的风险功能
文件上传

测试可接受的文件类型是否列入白名单，并且是否列入非白名单类型将被拒绝
测试文件大小的限制，上传频率和总文件数量的定义和执行
测试文件内容是否与定义的文件类型匹配
测试所有文件上传是否具有反病毒扫描。
测试上传的恶意文件
测试不安全的文件名是否被清理
测试上传的文件能不能直接在Web根目录下访问
测试上传的文件在不在相同的主机名/端口上
测试文件和其他媒体是否与身份验证和授权模式集成
支付
在Web服务器和Web应用程序上测试已知的漏洞和配置问题
测试默认或可猜测的密码
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CVSS v2得分> 4.0的所有漏洞
测试身份验证和授权问题
测试CSRF
错误处理
检查错误代码
检查堆栈
其他备忘录
https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

上一篇：Redis和SSRF 下一篇：Linux下pwn从入门到放弃
1. 1 条回复


legend 2017-12-15 14:52:22

脑图也发上去啦
新版编辑器用的不太溜大家见谅下····

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板