BQConf ThoughtWorks

ThoughtWorks® | IT大咖说 知识分享平台

OWASP MOBILE SECURITY TOP 10

齐磊

2016 OWASP TOP 10

ThoughtWorks® | IT大咖说 知识分享平台

- 平台使用不当
- 不安全的数据存储
- 不安全的通信
- 不安全的身份验证
- 加密不足
- 不安全的授权
- 客户端代码质量问题
- 代码篡改
- 逆向工程
- 无关的功能

不安全的数据存储

- SQL 数据库；
- 日志文件；
- XML 数据中存储；
- 二进制数据存储；
- Cookie 存储；
- SD 卡；
- Cloud 同步。

移动端数据存储-安全控制与设计原则

- 在设计阶段，按照敏感程度和应用的访问策略对数据存储区域分类(如密码、用户数据、位置信息、错 误日志等等)，并检查调用这些敏感数据的 API 是否安全。 日志文件；
- 敏感数据应安全保存在服务端，而不应存储在客户端。

- 数据存储时应采用操作系统提供的文件加密函数或其它权威的加密函数。

- 个人敏感信息必须设置最大保存时间，超过时间必须删除（以防止数据还在无限期缓存）。
- 假设共享的存储区是不可信的，数据很容易以各种方式泄露。(如地址簿，摄像头等)

不安全的通信

不安全的通信

- 缺乏证书检查
- 脆弱的握手协议

- 当应用程序需要传输敏感信息时，应该强制使用加密的（如 SSL/TLS）点对点传输方式，保证机密性和完整性保护。这里敏感信息包括用户证书或类似的认证信息。
- 采用权威的加密算法（如 AES，DES），并且选择适当的密钥长度

- 服务端证书签名必须由权威 CA 提供，不要采用自签名的方式生成证书。

不安全的身份验证

不安全的身份验证

- 当被要求时，没有对所有用户进行身份识别；
- 当被要求时，没有保持对用户身份的确认；
- 会话管理中的漏洞。

不安全的身份验证-安全控制与设计原则

- 一个有关身份验证的常见风险是向未识别身份的用户暴露数据或提供服务。匿名用户可以调用 Web 服务。而 Web 服务的本意是只允许已注册的或已识别身份的用户执行该操作。
- 应用程序请求访问敏感数据或接口时，尽可能地增加其他身份鉴别因素。
- 仅客户端登出

加密不足

加密不足

- 弱密码；
- 短密钥；
- 错误类型的加密算法（如：对称加密算法比不对称加密算法适用）；
- 众所周知的密码分析攻击漏洞（如：选择明文攻击）

- 可预测的密钥，解决这个问题的方法将涉及到生成一个强密钥，并安全地在服务器和客户端之 间进行通信，或者使用非对称加密技术。
- 容易伪造的完整性检查。到生成独一无二的签名，且难以伪造。

ThoughtWorks® | IT大咖说 知识分享平台

客户端代码质量问题

客户端代码质量问题

- C 语言的缓冲区溢出、或在 Webview 移动 应用程序中基于 DOM 的 XSS，都是代码质量的问题
- 在代码质量事件中，风 险往往来自于使用了错误的 API、使用了不安全的 API、使用了不安全的语言结 构或其他一些代码级的问题。

客户端代码质量问题-安全控制与设计原则

- 利用静态扫描及早的发现代码存在的问题。
- 采用成熟的架构，及早的修复发现的安全问题。

逆向工程

逆向工程

- 通过逆向工程，攻击者可以枚举或绕过业务逻辑、绕过安全控制、促进源代码 盗用和篡改代码。
- 攻击者可以重新打包应用程序，并通过各种方式发布给公众。

- 通过代码混淆方式，增加代码被反编译的难度。

代码篡改

代码篡改

- 对应用程序包的直接修改；
- 系统 API 的重定向或更换；
- 对后端服务器的直接攻击。

- 攻击者要么 可以直接修改代码、动态修改内存中的内容、更改或替换应用程序使用的系统 API，要么可以修改应用程序中的数据和资源。系统 API 的重定向或更换；

- 可以检测应用程序内的在线购买是否成功，从而使不付钱但想获得内容的终端用户无法成功

无关功能

无关的功能

- 在应用程序中启用了在发布时并不打算发布的功能。
- 如果开发人员将恶意代码片段注入任何保险应用程序中，那么，窃取包含所有个人信息在内的客户数据是有很可能的。

- 进行代码走查，尽早发现以及降低这种风险。