Top 10 Privacy Risks

王强
OWASP中国·海南区域负责人
海南神州希望网络有限公司红队负责人
E-mail:wangqiang@owasp.org.cn

目录

- 项目背景
- 项目介绍
- 项目内容
- 交流探讨

项目背景

- 当前许多Web应用程序包含隐私风险；
- 应用程序所在国家的法律对隐私保护没有足够的重视；
- 过分关注应用程序的合规性而忽视了真正的现实隐私风险；
- 没有关于Web应用程序中隐私风险的现有指南或统计数据

项目背景

- 2017年6月实施《网络安全法》；
- 2018年5月出台GDPR；
- 2019年5月发布网络安全等级保护2.0；
- 自身工作原因

项目介绍

- 2014年发布Top 10 Privacy Risks v1.0;
- 2015年发布德语版;
- 2016年发布Countermeasures v1.0 published;
- 2019年开始v2.0版本的开发
- 2020年发布v1.0中文版，中文翻译由王强负责翻译、王颉博士进行审查
- OWASP十大隐私风险项目提供了Web应用程序中的隐私风险和相关对策的前十名。它涵盖了关注现实生活风险的技术和组织方面，而不仅仅是法律问题。
- 该项目提供了有关如何通过设计在Web应用程序中实现隐私的技巧，旨在帮助开发人员和Web应用程序提供商更好地理解和改善隐私。
- 该项目由Florian Stahl，Stefan Burgmair主导，并由近百名安全和隐私专家参与
- 原项目地址： https://owasp.org/www-project-top-10-privacy-risks/
- 中文项目地址： http://www.owasp.org.cn/owasp-project/OWASP_Top_10_Privacy_Countermeasures_v1.0.pdf

项目内容

P1 Web 应用程序脆弱点

P2 运营商端的数据泄露

P3 数据泄露响应不足

P4 个人数据删除不足

P5 不透明的政策、条款和条件

P6 收集除主要目的需要之外的额外数据

P7 与第三方共享数据

P8 过期的个人数据

P9 会话超时缺失或不足

P10 不安全的数据传输

P1 Web应用程序脆弱点

Web应用程序的脆弱点仍是隐私风险引发的重灾区

- 开发阶段是否遵循安全开发生命周期？
- 运营阶段是否有相应的安全测试？
- 是否使用了过时的软件？（服务器、数据库、框架等）

P1 应对措施

- 遵循安全开发生命周期，对开发人员进行培训；
- 定期进行安全测试
- 跟踪发现的脆弱点并及时修复
- 定期安装更新、补丁等程序

P2 运营商端的数据泄漏

内部程序或工作人员是数据泄露的重要原因之一

- 访问控制管理不足
- 不安全的存储
- 缺乏安全意识

P2 应对措施

- 加强身份与访问控制管理（最低权限原则）
- 对数据进行分类并加强数据处理策略
- 加强安全意识并定期进行培训
- 个人数据匿名化

P3 数据泄露响应不足

数据泄露很可怕，更可怕的是缺乏响应机制

- 是否制定了隐私数据泄漏相关的安全事件响应预案？
- 是否定期演练该预案？
- 是否具备计算机应急响应小组？
- 是否对安全事件进行了跟踪？

P3 应对措施

事前：

- 建立并维护安全事件响应预案；
- 定期演练该预案；
- 建立计算机应急响应小组；

事后响应：

- 验证泄露事件；
- 派遣负责人进行调查；
- 组建应急小组；
- 对事件进行评估（如范围、是否涉密等）
- 通报数据所有者；
- 决定如何处理、如何调查；
- 。。。。。。

P4 个人数据删除不足

完成某项操作后，应根据要求及时删除个人数据。

- 数据保留或删除的策略是否恰当？
- 数据保留或删除是否具有透明性？

P4 应对措施

- 制定恰当的数据保留或删除策略
- 因技术受限，无法删除的数据应进行安全锁定。
- 加强数据访问的权限控制

P5 不透明的政策、条款和条件

- 隐私政策、条款、条件等不是最新的、不准确的、不完整的，或难以找到的
- 数据处理解释不足
- 条款太长，用户难以阅读

P5 应对措施

- 制定恰当准确的隐私条款，且显目
- 准确解释数据的使用和处理
- 条款应简单明了，使非专业人士能容易理解

P6 收集除主要目的需要之外的额外数据

未经用户同意，收集多余数据

- 非系统所需的描述性数据、公民信息、及其他多余的用户相关数据
- 未经用户允许，收集额外数据

P6 应对措施

未经用户同意，收集多余数据

- 对个人数据的目的进行定义
- 仅收集必要的个人数据
- 向用户明确收集数据的目的和用途

P7 与第三方共享数据

个人数据泄露常因第三方内容导致

第三方:

- 广告商
- 外包商
- 视频集成
- 地图商
- 社交网络.....

问题:

- 未经用户知情和同意，数据被传输或出售给第三方
- 完全失去控制

P7 应对措施

- 仅在需要的时候使用第三方内容
- 仅收集必要的个人数据
- 与第三方共享数据前，应考虑使用标记化或匿名化策略
- 制定严格的第三方监控策略（如黑白名单、政策条款制定、用户投诉情况等）

P8 过期的个人数据

- 伪造或绕过身份验证
- 过期数据遭受非法利用

P8 应对措施

- 在特定时间执行特定程序过程中以通过用户输入数据对用户数据进行更新
- 当用户触发“关键”操作时，应对数据进行授权
- 以表单形式使用户能够更新自身的数据

P9 会话超时缺失或不足

- 无法有效强制终止会话
- 用户不知情的情况下被额外收集信息

P9 应对措施

- 应设置自动会话超时
- 会话超时应根据用户需要进行设置
- 提示用户未进行注销动作

P10 不安全的数据传输

- 传输信道未加密
- 未能实施限制泄露的机制

P10 应对措施

- 采用加密的传输信道
- 对敏感信息禁止使用弱协议
- 避免在URL中包含个人信息
- 采用密码技术对个人信息进行加密处理

交流探讨


OWASP
Open Web Application
Security Project