OWASP 隐私风险 Top 10
—应对措施

OWASP 中国

2020 年 7 月

P1 Web 应用程序脆弱点	在任何保护用户敏感数据或需对用户敏感数据进行操作的系统中，脆弱点都是一个关键问题。由于未能正确设计和开发应用程序，或虽检测到问题却无法及时修复应用程序（包括安装补丁），可能都会导致隐私受到侵犯。该风险也包括《OWASP Top 10》中所述 Web 应用程序脆弱点所引发的风险。
如何检查？ • 是否针对隐私风险进行了常规渗透测试？ • 开发人员是否接受过 Web 应用程序安全相关的培训？ • 是否使用了安全的编码规范？ • 是否使用了过时的软件？（包括：服务器、数据库、框架及其他基础架构组件）	**应对措施** • 由第三方安全专家定期进行渗透测试。 • 追踪发现的补救措施。 • 对应用程序开发人员和架构师进行安全培训。 • 采用安全开发流程（如：安全开发生命周期 SDL）。 • 定期安装更新、补丁等修补程序。
示例 • 注入漏洞：攻击者可通过诸如 SQL 注入类的攻击对数据进行复制或操作。 • 敏感数据泄露：由于未采用加密技术，导致攻击者可通过诸如中间人攻击收集敏感信息。 • 使用不安全的直接对象引用：攻击者可猜解并访问敏感信息，特别是在缺少访问控制的情况下。 • 使用含有已知漏洞的组件：如未修复的软件缺陷和错误的安全配置、未加固的应用程序。 • 一般来说，攻击者可能通过权限滥用输入恶意代码或窃听通信来访问、操作或删除应用程序正在处理的个人数据。	**参考资料** • OWASP Top 10 Project • OWASP ASVS • Open SAMM • OWASP Proactive Controls • Security Development Lifecycle（SDL） • OWASP Secure Application Design Project • 在 CVE 和 NVD 找到已知的漏洞列表 • ISMS of the German Federal Office for Information Security（BSI）

P2 运营商端的数据泄露	由于恶意破坏或无意错误（如：访问管理控制不足、存储不安全、数据重复或缺乏意识），导致未能防止任何与用户数据相关的信息及数据本身泄露给任意未授权方，进而导致丧失数据机密性。
如何检查？ • 调查运营商的声誉及可靠性： ▫ 曾经是否有与运营商有关的违规行为？ ▫ 运营商是否主动展示保护隐私安全的能力？如果是，如何展示？ ▫ 是否有漏洞奖励计划来报告漏洞？ ▫ 运营商是否经过 ISO 27001 或 ISO 27018（云供应商）认证？ ▫ 运营商是否设置在隐私标准较高的国家？ • 审查运营商： ▫ 关于隐私的最佳实践是否到位？ ▫ 所有员工是否都必须进行意识培训？ ▫ 是否有隐私工作团队？ ▫ 个人数据如何匿名化？ ▫ 个人数据是否加密处理？ ▫ 谁有权访问数据（需要了解访问规则）？ • 审核方法： ▫ 纸质审计（基础） ▫ 访谈式审计（良好） ▫ 现场审计和系统检查（最佳）	**应对措施** • 恰当的身份与访问管理（包括物理和逻辑的）： ▫ 最低权限原则。 • 对所有存储个人数据（静态数据）的设备进行强加密，尤其是移动媒介上（如：U 盘、笔记本电脑硬盘、平板电脑和手机中的本地存储、备份磁盘、移动硬盘等）。 • 对所有员工进行有关个人数据处理的意识培训。 • 实行数据分类和数据处理策略。 • 监测和检测机密数据从终端、门户网站、云服务等地方的泄露（如通过 SIEM 进行数据泄露防护）。 • 通过设计实现隐私保护。 • 个人数据匿名化：个人数据用于其他目的（如测试或推广）时，个人数据匿名化是一种常见的作法。但匿名化并不容易实现（如 aol 搜索数据泄露），并且许多匿名理论非常复杂。 • 假名化，这意味着数据只能在了解某人并在相应假名的第三方协助下才能与该用户进行连接。
示例 • Handbook for Safeguarding Sensitive PII	**参考资料** • Article 29 Working Party on Anonymization • IT-Grundschutz-Catalogues

P3 数据泄露响应不足	因恶意或无意事件可能导致的数据泄露未告知受影响人员(数据主体);未能通过补救措施进行纠错;未尝试限制数据泄漏。

如何检查?

常规问题:

- 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(提供证明,如演练附件等)?
- 是否具备计算机应急响应小组(或中心)或隐私保护小组?
- 是否对安全事件(如 SIEM)进行了跟踪?

如果存在隐私问题,您是否?

- 及时发现到了吗?
- 及时通报相关人员了吗?
- 在响应或调查过程中是否保护了证据和剩余数据?

您的事件响应是:

- 及时向受影响方披露信息,以避免额外损害?
- 是否以真实、准确、通俗易懂的方式地披露事件?遭受隐私泄露的组织有责任向所有受影响的人清楚地传达泄露的性质和范围。
- 是否在整个公司范围内建立安全漏洞通报机制(或策略)?

应对措施

前置措施:

- 建立并维护安全事件响应预案。
- 定期进行安全事件响应演练。
- 安全事件响应演练中包含隐私相关的事件。
- 建立计算机应急响应小组(CERT)。
- 建立隐私保护小组。
- 持续监控个人数据泄露和丢失。

对数据泄露的响应:

- 验证泄露事件。
- 一旦确认违规行为,应立即指派事件负责人对其进行调查。
- 组件事件响应小组。
- 确定泄露的范围和类型(如:涉法、涉密)。
- 通报数据所有者。
- 决定是否通报主管单位(视实际情况而定)。
- 决定怎样调查数据泄露事件,确保证据得到适当处理。
- 确定受影响个人的通知是否适当,如果是,在什么时候以什么方式通知。
- 收集并审查所有数据泄露事件响应的文档记录和分析报告。

示例

- AICPA 隐私安全事件响应预案模板(AICPA Privacy Incident Response Plan Template)
- ENISA 严重性评估建议(ENISA recommendations for severity assessment)

参考资料

- Key Steps for Organizations in Responding to Privacy Breaches (Privacy Commissioner of Canada)
- Data Breach Response Checklist (PTAC)

P4 个人数据删除不足	在指定目的达成后，未根据要求及时删除或有效删除个人数据。
如何检查？ • 检查数据保留和删除策略。 • 评估这些策略是否恰当。 • 要求检查删除的过程。 • 检查是否提供透明性（何时删除哪些数据以及不删除哪些数据并提供原因）。	**应对措施** • 部署具有良好隐私实践的系统，可最大限度减少个人数据泄露。 • 在达到指定目的后或在恰当时限（如一个月）后，必须删除个人数据。 • 必须根据正确的用户请求删除个人数据。 • 如果由于技术限制而无法删除，则可以选择安全锁定（对数据进行访问限制）。 • 但最好是删除数据以将风险降至最低。 • 针对数据留存，须遵循归档和删除策略，且过程应记录在案。 • 应收集证据以验证是否根据策略删除数据。 • 须考虑备份，包括其他副本和第三方共享的所有数据。 • 在法律要求保留的情况下，可以例外。在这种情况下，访问权限应非常有限，并应有相应的协议。 • 删除云中数据时，应注意存储在旧快照中的历史数据。 • 长时间不活动后删除用户个人资料。
示例 客户数据在一段时间不活动后（如：当用户一年未使用，Hotmail 将删除其用户个人资料）或合同终止后（法律不要求保留所有客户信息用于会计或其他目的），自动删除。	**参考资料** • https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/ • German DIN standard 66398

P5 不透明的政策、条款和条件	没有提供足够的信息来描述如何处理数据（如：数据的收集、存储、处理和删除等），并且未能使不是作为律师的人员容易获取和理解这些信息。

如何检查？

检查政策、条款和条件：

- 容易找到。
- 全面描述如何处理数据：
  - 是谁在处理数据
  - 包括数据传输
  - 执行的数据分析
  - 保留时间
  - 使用的元数据
  - 有什么权利
  - ……
- 不是律师的人员也可理解。
- 完整且简单明了（保持简短）。
- 如果条款、政策或条件发生变化，请包含获取用户同意的过程。
- 以用户的语言提供这些政策、条款和条件。
- 说明收集个人数据的目的
- 使用如 https://readability-score.com/等可读性测试器检查文本是否难以阅读。
- 隐私条例是否主动告知或建议用户采取措施。

应对措施

- 《使用条款和条件（T&Cs）》应专用于网站的使用和数据处理。
- 对于不是律师的人而言，这些条款应易于理解，且阅读时间不应过长。
- 提供一份易于阅读的条款或条件的摘要以及一份长版本。
- 象形图可用于视觉辅助。
- 使用独立的 T&Cs 进行使用和数据处理。
- 使用发布说明来识别条款、条件、策略、通知等时间的更改历史记录。
- 追踪哪些用户允许哪个版本，以及他们可以选择使用新版本的任何其他时间。
- 在服务端部署“不追踪”服务。
- 收集信息时，应明确为什么需要收集该信息。还应尝试预判未来是否会使用这些信息用于其他事物，并告知用户是否有这样的计划。
- 提供 cookies、部件等清单，并解释其用途，如共享数据或广告等。
- 为用户提供“选择退出按钮”。

示例

- 易于阅读的摘要：
  - http://www.avg.com/privacy
  - 500px.com
- 解释 cookies、部件等，包括选择退出按钮（如果存在）：
  - http://www.kaspersky.com/third-pa-rty-tracking
- 象形图实例：
  - http://netdna.webdesignerdepot.com/uploads/2014/03/iubenda.jpg

参考资料

- ICO 的隐私声明行业规程，还包含了一系列实例：https://ico.org.uk/media/for-organisations/documents/1610/privacy_notices_cop.pdf
- HTTPA（HTTP with Accountability）
- Biggest lie 项目曾反对复杂的 T&Cs，并证明其他项目也试图改变它。

P6 所收集数据非主要目的需要	所收集的数据为非系统所需的描述性数据、人口统计数据或任何其他与用户相关的数据。也指用户未提供同意的数据。

如何检查？

- 列出由应用程序收集的个人数据。
- 收集请求的目的说明。
- 如果收集的数据非主要目的所需，那么检查是否同意收集和处理此数据，并将其记录在案。
- 是否通知个人并询问是否更改目的或流程？
- 是否存在关于收集个人数据和用户同意的定期合规性检查？

应对措施

- 对收集个人数据的目的进行定义。
- 仅收集目的实现所需的个人数据。
- 除非用户另行选择，否则默认设置为收集尽可能少的数据（数据最小化）。
- 向数据主体提供关于自愿提供额外资料以改善服务（如：产品推荐、个性化广告）的选择，并且可选择不提供。
- 对需要收集的个人数据进行收集目的的及时明确，而不是在收集数据的时候明确。
- 有条件的收集：只有在所使用功能确实需要个人数据时才收集这些数据。

示例

正面示例：

- 电子商城会收集电子邮件地址，进而向买家发送订单确认。除非用户主动选择此选项，否则所述电子邮件地址不会被用于发送关于产品的新闻消息（或其他目的）。

反面示例：

- 亚马逊能够向其用户提供个性化广告。默认设置已勾选该功能，不过用户可以禁用此选项。但是，从隐私保护的角度来看，默认设置应该是禁用它，并且用户应该选择加入以接收个性化的产品推荐。

参考资料

- Article 29 Working Party Opinion on Purpose Limitation

隐私设计策略：

- M. Colesky, J.-H. Hoepman, and C. Hillen. **A Critical Analysis of Privacy Design Strategies.** In 2016 International Workshop on Privacy Engineering - IWPE'16, San Jose, CA, USA, May 26 2016. （to appear）.
- J.-H. Hoepman. **Privacy Design Strategies.** In **IFIP TC11 29th Int. Conf. on Information Security （IFIP SEC 2014）**, pages 446-459, June 2-4 2014.

P7 与第三方共享数据	在未得到用户同意的情况下，私自向任何第三方提供用户相关数据。基于获得金钱回报的目的，向第三方转移或交换用户信息，或由于不适当地使用了来自网站的第三方资源，诸如小部件（如：地图、社交网络按钮）、网站漏洞与分析（如：导航标）而导致其信息被第三方获取。
如何检查？ • 个人数据是否被传输给第三方？ • 是否正在使用来自第三方的部件（插件、按钮、地图、视频文件、广告等），并且使用的是哪种类型的部件？ • 是否披露了第三方数据跟踪（第三方是谁？是关于什么数据的）？ • 能否提供一份能够包括所有第三方的列表？ • 对照本文档中的每个标准检查每个第三方。 • 你在隐私方面对它们进行评级了吗？ • 隐私以及个人数据处理是否是条款的一部分？如果是，那么存在什么限制？ • 您是否使用对隐私友好的第三方内容实现（如果有）？ • 是否使用出于隐私考虑而被禁止的第三方黑名单成员？ • 是否对第三方进行审查？ • 如果将数据传输给第三方或使用第三方处理，是否具有关于用户同意共享数据的内容？	**应对措施** 个人数据通常会与第三方内容（如用户跟踪代码、广告、社交网络按钮或视频以及第三方托管的 JavaScript 和样式表库等）相集成，进而与第三方共享。 为保护隐私，对第三方内容的使用，应考虑采取以下措施： • 将默认设置为仅在需要的时候使用第三方内容。 • 使用自己的服务器作为所需内容的“代理”。 • 部署完全“不跟踪”，符合最新的 W3C 标准。与任何非官方 EFF 标准相比，推荐 W3C 标准。 • 在与第三方共享数据之前，应考虑使用标记 化或匿名化（数据屏蔽）。 • 制定在线监控第三方战略： ▫ 第三方内容（白名单或黑名单）的发布关卡。 ▫ 有关政策、数据使用等相关合同条款的制定。 ▫ 用户投诉情况的监控。
示例 • 在没有点击社交网络按钮的前提下，数据不会被传送到第三方：https://github.com/heiseonline/shariff • YouTube 为用户提供了启动隐私增强模式的选择，并且只在点击的情况下才会传输个人数据。	**参考资料** • W3C Working Draft Tracking Compliance and Scope 基于属性的信任凭据： • https://abc4trust.eu/ • https://en.wikipedia.org/wiki/Do_Not_Track

P8 过期的个人数据	使用过期、错误或伪造的用户数据。未能更新或更正数据。
如何检查？ • 询问操作员如何确保个人数据为最新。 • 检查是否需要对应用程序中的个人数据进行更新。 • 是否会进行定期检查以验证数据是否为最新状态（如：“请核实您的送货地址”）？ • 询问数据能够保持最新的时间，以及通常多长时间更新一次。	**应对措施** • 在特定一段时间后，执行特定过程以通过用户输入数据来更新用户个人数据。 • 如果用户正在触发“关键”操作，则其应该对数据进行授权。 • 提供表单以使用户能够更新其个人数据。 • 在更新个人数据时，确保将该信息转发给之前接收到用户数据的任何第三方或子系统（如果有的话）。
示例 • 网站提供更新表以便用户可以在需要时更新其个人数据。 • 亚马逊首先会询问您的地址和账户数据是否正确，然后您才能完成订单（CRM 结算）	**参考资料** • UK ICO on keeping personal data up to date

P9 会话超时缺失或不足	无法有效强制终止会话。这可能会导致在没有得到用户同意或在不知情的情况下，额外收集用户数据。
如何检查？ • 检查注销按钮是否易于找到和点击。 • 检查自动会话超时是否小于 1 周时间（对于关键应用程序是否小于 1 天时间）。 • 会话超时时长是否适合于完成事务所需的时长（应足够长），是否同意适合于会话访问的数据敏感度（越短越敏感）。 • 单个服务可以支持会话敏感度和时长的多种组合。应评估每种组合下的可用会话类型。	**应对措施** • 应设置自动会话超时。会话超时时间不尽相同，具体取决于应用程序和数据的重要程度。 • 会话超时不应超过一周，对于重要应用使用情形，会话超时时间应短得多。中等重要程度（例如，网络邮件程序、网络商店、 社交网络）的最佳默认设置为一天。 • 会话超时应由用户根据其需要进行设置。 • 如果用户上次未使用注销按钮完成其会话，则下次登录时用户应会看到一条消息提醒。 • 如果用户无法注销，或者注销未能完全终止会话，则可能会被继续收集数据（如，跟踪用户在其他地方访问的站点）。
示例 • 当用户忘记从 web.de（德国邮件提供商）注销下线时，下次登录时会自动弹出一个窗口以提示处于安全原因注销非常重要。 • Facebook 没有自动会话超时功能。因此用户必须手动注销。如果用户没有主动注销，并且其他人随后使用了该设备，则后者就可以访问或操作前用户的配置文件。	**参考资料** • OWASP Session Management Cheat Sheet • Carnegie Mellon Guidelines for Data Protectionrecommends automatic session timeout besides other controls

P10 不安全的数据传输	在未加密或不安全的信道上提供数据传输，从而无法排除数据泄露的可能性。未能实施限制泄漏面的机制，例如，允许在 Web 应用程序操作机制之外推断任何用户数据。
如何检查？ • 检查是否存在保护传输中数据的策略？ • 数据在传输过程中是否经过加密处理？ • 是否使用安全协议和算法？ • 隐私友好协议是否适用于数据传输？ • 在适当的情况下是否强制执行隐私协议？（如，只能通过 HTTPS 登录，敏感记录只能通过 TLS 或 SFTP 访问）	**应对措施** • 始终使用安全协议发送个人数据，也就是说，不要使用不安全的协议，如：普通电子邮件、即时消息客户端、FTP 等。 • 配置传输协议，确保传输数据类型足够安全。 • 在可能的情况下，允许使用可用的最佳安全协议进行连接。 • 对于敏感信息不允许使用弱协议。 • 避免在 URL 中包含个人信息，特别是在数据传输未加密的情况下。 • 激活协议中的隐私（如，IPv6 中的隐私扩展）。 • 支持 TLS/DTLS，不支持 SSLv3。 • 使用 ECDHE 和 GCM 密码，不支持静态 RSA 密钥交换和基于 CBC 的密码。
示例 • 对服务进行配置，以禁用损坏的安全协议，如，SSLv3。 • 对服务进行配置，以启用最新的安全协议。 • 对整个 Web 应用程序会话强制执行 HTTPS，从登录页面首次访问到完成注销。 • 在文件服务器上禁用易受攻击的文件传输服务（例如 Telnet 和 FTP）。改为启用安全传输协议。 关于当前互联网技术不安全以及建立新技术的倡议： http://youbroketheinternet.org/	**参考资料** • http://security.stackexchange.com/questions/7790/guidance-for-implementors-of-https-only-sites-server-side • Jim Manico 在 OWASP AppSec EU 2015 的演讲： HTTPS is better than ever before - Now it's your turn • Privacy Extensions in IPv6 • Background information: IEEE 802 Tutorial about Designing Privacy into Internet Protocols (July 2014)

感谢以下人员的贡献

感谢以下编制《OWASP Top 10 Privacy Countermeasures》的主要贡献者：：

- Stefan BurgmairR
- Jason Cronk
- Edward Delaporte
- Tim Gough
- Prof. Hans-Joachim Hof
- Lukasz Olejnik
- Florian Stahl

感谢以下参与本中文版本《OWASP Top 10 Privacy Countermeasures》的 OWASP 中国成员。

- 翻译：王强
- 审查：王颉

由于项目组成员水平有限，存在的错误敬请指正。如有任何意见或建议，可联系我们。邮箱：project@owasp.org.cn