AKAMAI 核对表

OWASP 10 大 API 安全风险

API 已成为构建和连接现代应用程序的事实标准，而越来越多的应用程序转向基于微服务的架构更是助推了这一趋势。正因如此，您有必要确保贵公司免受开放 Web 应用程序安全项目 (OWASP) 确定的最常见 API 安全风险的侵扰。我们来盘点一下 2023 年的最新版清单，帮您掌握更多相关信息，从而更好地完成 API 保护之旅。

Akamai 能够抵御 OWASP 十大 API 安全风险

- **API1:2023——失效的对象级授权 (BOLA)：**当客户端的授权没有经过正确验证便可访问特定对象 ID 时，就会出现 BOLA 漏洞。
- **API2:2023——失效的身份验证 (BA)：**身份验证过程中的大量漏洞均与 BA 有关，这种安全风险导致系统暴露在攻击者面前，使攻击者能够利用这些漏洞来破坏 API 对象防护机制。
- **API3:2023——失效的对象属性级授权 (BOPLA)：**在 BOPLA 这类安全漏洞中，API 端点公开的数据属性不必要地超过了其发挥功能所需的数量，违背了最小特权原则。
- **API4:2023——不受限制的资源消耗：**这类漏洞有时也称为 API 资源耗尽，API 不会限制给定时间内的请求数量或者所传输的数据量。
- **API5:2023——失效的功能级授权 (BFLA)：**在 API 端点的访问控制模型实施不正确时，就有可能发生 BFLA。
- **API6:2023——不受限制的敏感业务流访问：**在 API 公开关键操作（如业务逻辑）而又没有足够的访问控制措施时，就会出现这种风险。
- **API7:2023——服务器端请求伪造 (SSRF)：**通过 SSRF，攻击者可诱导服务器端应用程序向其选定的任意域发出 HTTPS 请求。
- **API8:2023——安全配置错误：**这是指安全控制措施设置有误，从而造成系统容易受到攻击。
- **API9:2023——不当的资产管理：**这是每个管理 API 的公司都面临的一项挑战。API 安全解决方案可以保护已知 API，但未知 API（包括弃用的、遗留的和/或过时的 API）可能没有得到修补，容易遭受攻击。
- **API10:2023——不安全的 API 使用：**此类风险涉及到在未实施适当的安全措施情况下使用第三方 API。

想要进一步了解 2019 年与 2023 年 OWASP 十大 API 安全风险清单之间的差异？请阅读这篇博客。

扫码关注 · 获取最新CDN前沿资讯

与我们合作

企业与其安全供应商必须紧密合作，在人员、流程和技术方面保持一致，以建立坚实的防御来应对 OWASP 十大 API 安全风险中概述的安全风险。

Akamai 简介

Akamai 提供出色的安全解决方案、经验丰富的专家和 Akamai Connected Cloud，每天从数以百万计的 Web 应用程序攻击、数以亿计的爬虫程序请求和数万亿的 API 请求中获取见解。借助 Akamai 的 Web 应用程序和 API 安全解决方案，您可确保贵企业能够抵御较为高级的 Web 应用程序攻击、分布式拒绝服务 (DDoS) 攻击以及基于 API 的攻击。

 | 支持 | 发布时间：2023 年 8 月