白皮书

巧用对策防范 OWASP 十大 API 安全风险

Akamai 如何助您应对常见的 API 漏洞和威胁

OWASP 十大 API 安全风险		Akamai 能否提供帮助?
API1:2023	失效的对象级授权	✓
API2:2023	失效的身份验证	✓
API3:2023	失效的对象属性级授权	✓
API4:2023	不受限制的资源消耗	✓
API5:2023	失效的功能级授权	✓
API6:2023	不受限制的敏感业务流访问	✓
API7:2023	服务器端请求伪造	✓
API8:2023	安全配置错误	✓
API9:2023	不当的资产管理	✓
API10:2023	不安全的 API 使用	✓

API 是企业数字产品、服务和云环境的核心。随着企业越来越多地采用基于微服务的架构来开发应用程序，API 也成为了构建和连接应用程序的标准。然而，由于 API 会持续访问数据和关键系统，它在帮助企业提升收入的同时，也会带来运营风险。

暴露或配置错误的 API 非常普遍，很容易遭到入侵，而且往往缺乏必要的安全保护。仅仅是一个遭到入侵的 API 就会导致数百万条记录被窃取。

78% 的企业报告称他们在一年内遇到过 API 安全事件，显然保护 API 应该成为企业的首要任务。但 API 攻击面已快速上升为攻击者的目标，并且速度之快让大多数企业来不及清楚了解以下情况：

API 风险

API 攻击方法

API 安全控制措施和功能

API 攻击面都包含什么？简单来说，这远超出了很多企业的认知范围。企业可以并且应该扩大对 API 的传统理解范畴，例如机器间的 API 或第三方 API，将移动和 Web 应用程序服务纳入到基于微服务的架构中。换言之，微服务架构中的 Web 请求也是一种 API，它们在一系列针对不同微服务发出的调用中充当着 API 的角色。

78%

的企业报告称他们在一年内遇到过 API 安全事件。显而易见，保护 API 应该成为企业的首要任务。

2023 年 6 月 5 日，备受推崇的开放全球应用程序安全项目 (OWASP) 发布了对其 2019 年第一版十大 API 安全风险列表的首次重大更新。更新后的列表主要针对不同的 API 调用可能给企业带来的安全漏洞和隐私风险问题，其中包括：

数据验证不完善

配置错误

实施缺陷

安全组件之间的集成问题

继续阅读，了解 OWASP 已识别的主要风险以及 Akamai 的 API 安全解决方案如何帮助您抵御这些风险。

问题在于，即便是声称拥有 API 完整清单的企业也存在严重不足：

只有**四成**的企业知道哪些 API 会在被调用时返回敏感数据。

API1:2023——失效的对象级授权

当客户端的授权未经过正确验证即可访问特定对象 ID 时，就会产生失效的对象级授权 (BOLA) 漏洞。此漏洞为攻击者直接访问资源敞开了方便之门，让他们能够绕过预期的应用程序工作流并对敏感数据进行未授权访问。为降低此风险，企业应该避免单纯地依赖于客户端在请求中传递的对象 ID，可改为使用不可猜测的随机对象 ID，从而确保对每个对象进行强力验证。在适当的时候，掩藏对象的真实 ID 可以提供一层额外的安全保护。

Akamai 如何为您提供帮助

Akamai 灵敏的监控系统会跟踪威胁并针对攻击者尝试过的 BOLA 漏洞利用生成告警，从而确保能够让用户立即注意到相关情况并采取相应措施。

Akamai 可以通过下列操作来抵御风险：

- 识别 BOLA 漏洞利用尝试
- 根据收到的输入（例如，可枚举参数）以及 API 对象与属性之间的关系，对容易受到 BOLA 漏洞利用入侵的 API 端点进行分类
- 针对攻击者尝试过或已成功的 BOLA 漏洞利用生成告警

API2:2023——失效的身份验证

失效的身份验证指的是身份验证过程中的大量漏洞，这些漏洞会将系统暴露在攻击者面前，而攻击者能够利用这些漏洞来破坏 API 对象防护机制。通常，攻击者会利用失效的身份验证漏洞来操纵系统中的漏洞，例如弱密码或会话重播。为了防范失效的身份验证漏洞，企业可以建立强大的身份验证和密钥管理机制，例如高强度密码策略、密钥轮换、强令牌签名和加密密钥。在企业中强制实施这些严格的策略会显著降低风险。

Akamai 如何为您提供帮助

Akamai 可以识别并纠正弱身份验证点，抵御自动攻击并且针对攻击方尝试过的漏洞利用主动发出告警，从而增强 API 安全性。

Akamai 可以通过下列操作来抵御此风险：

- 识别不需要身份验证或者未遵循身份验证最佳实践的 API 端点，例如弱令牌签名或弱加密密钥以及接受过期的身份验证令牌
- 通过我们的爬虫程序管理功能来防范自动字典或撞库攻击
- 通过我们的 API Gateway 功能，使用强令牌签名来处理 JSON Web 令牌的授权
- 针对攻击者尝试过的 BUA 漏洞利用生成告警

API3:2023——失效的对象属性级授权

失效的对象属性级授权 (BOPLA) 是一种安全漏洞。在此漏洞中，API 端点不必要地公开很多数据属性，超过了该端点发挥其功能所需的数量，进而导致忽视最低权限原则。

此漏洞会在无意中为攻击者提供过多的数据，然后攻击者会利用这些数据找到更多漏洞或挖掘敏感数据。这包括未授权用户可以操纵管理员级别访问权限的专有属性，进而破坏系统完整性的情形。为了确保安全性并阻止攻击者获取或操纵多余的信息，提供适当的访问权限级别和数据暴露至关重要，这可以阻止潜在攻击者利用这些疏漏。

Akamai 如何为您提供帮助

利用 Akamai 的全面策略，企业能够识别 API 端点及其关联属性并进行分类，从而抵御 BOPLA 的风险。

Akamai 可以通过下列操作来抵御此风险：

- 识别所有端点及其所公开的 API 属性并进行标记，例如个人身份信息 (PII)
- 识别没有文档记录的或影子 API 端点、对象和属性以及异常属性
- 应用与可接受的和已定义的参数及属性相关的安全策略，以确保进行数据清理
- 应用基于完整 OpenAPI/Swagger 规范的安全策略，并且仅允许定义完善的 API 端点和方法访问 API 对象和属性
- 针对攻击者尝试过的 BOPLA 漏洞利用生成告警

API4:2023——不受限制的资源消耗

不受限制的资源消耗（有时称为“API 资源耗尽攻击”）也是漏洞的一种类型，在此类漏洞中，API 不会限制给定时间内的请求数量或者其所提供的数据量。此漏洞会为寻求进行拒绝服务 (DoS) 攻击的攻击者敞开大门，进而导致系统对合法用户不可用。此类漏洞会产生严重的业务影响，导致出现服务可用性下降、客户不满意和潜在收入损失等问题，具体取决于服务中断的持续时间和范围。采取恰当的措施来限制 API 请求速率和数据返回大小以避免服务中断至关重要。

Akamai 如何为您提供帮助

Akamai 可以通过下列操作来保护您的 API 免受不受限制的资源消耗威胁的侵扰：

- 识别存在风险的端点，并针对攻击者尝试过的容量耗尽型攻击提供实时告警
- 发现有过多的错误、登录尝试或异常行为表明存在风险

Akamai 可以通过下列操作来抵御此风险：

- 识别缺少速率限制或者正在遭受大容量字典攻击或撞库攻击的 API 端点
- 启动相应的工作流以减缓或阻止容量耗尽型攻击
- 针对攻击者尝试过的容量耗尽型攻击生成告警

API5:2023——失效的功能级授权

当错误地实施 API 端点的访问控制模式时，将会出现失效的功能级授权 (BFLA) 漏洞。不正确或过时的访问控制方法无法充分限制未经授权的访问，使攻击者能够访问敏感信息或整个系统。要抵御此风险，企业可以采用最低权限原则，确保只有具备相应权限的用户才能访问所有功能，特别是管理功能。

Akamai 如何为您提供帮助

Akamai 将会追踪行为时间表、对敏感功能应用安全策略、管理密钥轮换和撤消，并在检测到任何可疑尝试时立即发出告警，从而帮助企业增强 BFLA 防范能力并强化响应策略。

Akamai 可以通过下列操作来抵御此风险：

- 通过获取用户、API 密钥、访问令牌、会话 ID 等，识别 API 端点访问的行为时间表
- 通过 Akamai API Gateway 应用密钥轮换或撤销已泄露的密钥
- 针对访问管理功能的可疑尝试生成告警

API6:2023——不受限制的敏感业务流访问

如果某个 API 在缺少足够的访问控制措施时公开关键操作（如业务逻辑），就会出现不受限制的敏感业务流访问漏洞。这会导致出现未经授权的访问和利用，进而对企业造成严重的损害。这种利用通常涉及了解由 API 提供支持的业务模式、识别敏感业务流以及利用这些流程中的漏洞。这会产生阻止合法用户购买产品等各种影响。

Akamai 如何为您提供帮助

Akamai 全面的 API 防护解决方案可提供敏感端点识别、实时漏洞利用告警以及专家咨询服务，在保障关键数据安全和运营安全的同时为您的企业保驾护航。

Akamai 可以通过下列操作来抵御此风险：

- 识别敏感 API 端点，例如处理 PII 的支付流程或端点
- 针对各种潜在的漏洞利用（包括数据外泄和数据操纵，以及对这些敏感 API 端点的可疑尝试）生成告警

API7:2023——服务器端请求伪造

通过服务器端请求伪造 (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。在典型的 SSRF 攻击中，攻击者会诱骗服务器对内部资源发出请求，从而绕过防火墙并获得对内部服务的访问权限，这可能会导致数据泄露或远程代码执行。要抵御此风险，验证、过滤或清理用户输入并限制服务器建立的出站连接数至关重要，这可以确保它仅与关键服务进行通信。

Akamai 如何为您提供帮助

Akamai 可以提供对可信 API 连接的异常检测、有效密钥管理，并在发现 SSRF 漏洞利用尝试时立即发出通知，从而增强您的安全态势。

Akamai 可以通过下列操作来抵御此风险：

- 通过针对 SSRF 攻击的 Web 应用程序和 API 保护策略实施防护
- 通过 API Gateway 应用密钥轮换或撤销已泄露的密钥

API8:2023——安全配置错误

安全配置错误是指安全控制措施设置有误，从而导致系统容易受到攻击。这可能包括不安全的默认配置、不完整或临时的配置、开放式云存储、配置错误的 HTTP(S) 标头或包含敏感信息的详细错误消息。要抵御这些风险，企业必须确保在应用程序和 API 的各个方面都正确地配置了自己的安全控制措施。这包括定期更新、全面测试以及进行持续监控以识别并立即纠正任何配置错误。

Akamai 如何为您提供帮助

Akamai 会帮助您识别影子、恶意或僵尸 API 端点，并帮助您遵循安全最佳实践、进行稳健的 HTTPS 实施，还会在发现安全配置错误时接收即时告警，以此增强您的洞察能力。

Akamai 可以通过下列操作来抵御此风险：

- 识别可能会暴露低级别环境（例如，测试和暂存环境）的影子 API 端点
- 根据安全配置最佳实践和标准，识别并匹配 API 端点、对象和属性
- 通过 API 安全最佳实践（例如，格式正确的 HTTPS 请求和响应）应用安全策略，配置或移除正确的 HTTP 标头，以及确保完全控制跨源站资源共享 (CORS) 和缓存控制标头
- 通过 SSL/TLS 应用正确的 HTTPS 实施，包括正确安全的密码套件
- 针对配置错误或不符合 API 安全最佳实践和标准时生成告警

API9:2023——不当的资产管理

对于每个管理 API 的企业来说，不当的资产管理都是一项挑战。API 安全解决方案可以保护已知 API，但未知 API（包括影子 API）可能得不到修补，因此很容易受到攻击。这可能会导致出现过时组件、未使用的页面或 API，以及不必要地暴露敏感信息。未加维护的服务管理可能会导致系统容易受到威胁侵扰，并且攻击者有可能通过连接到同一数据库的未知 API 获得对敏感数据甚至是服务器的访问权限。必须实施访问控制和定期审计，以避免企业服务中存在不断改变的组件。

Akamai 如何为您提供帮助

Akamai 会持续监控 API 流量以发现隐藏的 API 端点以及具有潜在风险的 API，为企业提供安全数据存储、实施高级威胁分析并在发现潜在漏洞利用时立即发出告警。

Akamai 可以通过下列操作来抵御此风险：

- 持续监控流经您环境的暴露 API 流量，包括以可公开访问的 API 为目标的南北向 API 端点以及东西向内部 API 端点
- 识别可能会暴露低级别环境（例如，测试和暂存环境）的影子 API 端点或者没有文档记录的和/或已弃用的 API 版本
- 根据风险评分和数据分类创建最新的 API 清单
- 针对各种潜在的漏洞利用（包括数据外泄和数据操纵，以及对这些敏感 API 端点的可疑尝试）生成告警

API10:2023——不安全的 API 使用

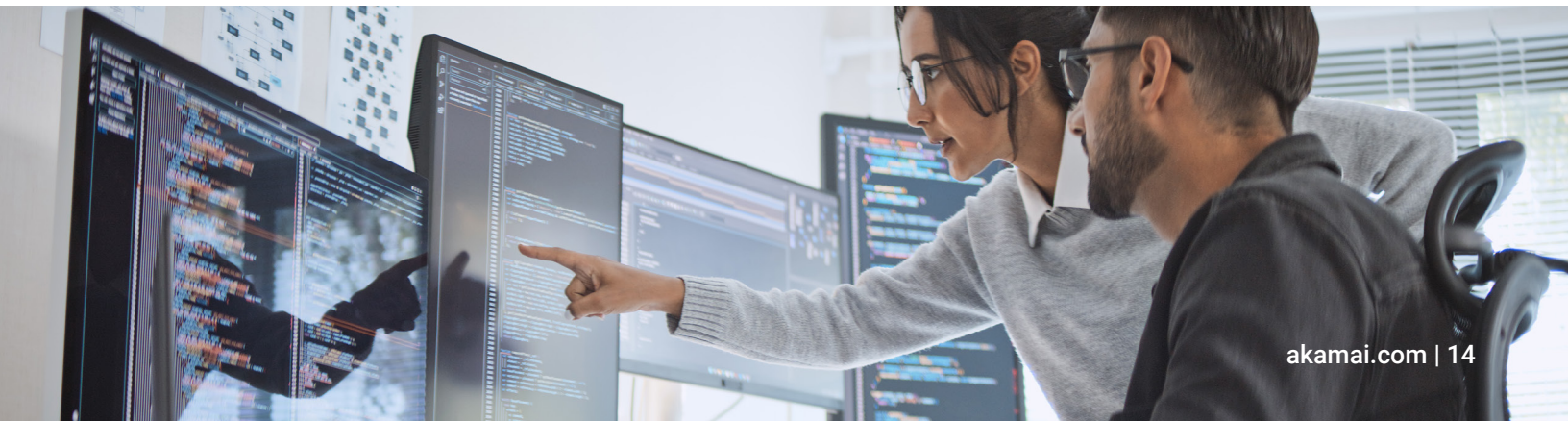
不安全的 API 使用风险涉及在未实施适当安全措施的情况下使用第三方 API。企业越来越多地依靠第三方 API 来扩展服务和功能，因此通常情况下会默认这些 API 是可信的。这可能会导致严重的安全漏洞。未实施适当的加密、数据验证、清理和资源消耗限制会导致企业中存在验证漏洞。要抵御这些风险，企业可以对通过网络传输的所有数据实时加密，验证和清理所有数据输入，并且对资源消耗设置合理的限制。

Akamai 如何为您提供帮助

利用 Akamai 的监控、告警和咨询服务，监控和验证您的服务以确保安全性，从而持续保护您的系统。

Akamai 可以通过下列操作来抵御此风险：

- 持续监控所有流经您环境的暴露 API 流量，包括用于帮助实现 B2B 和/或第三方集成的东西向 API 和出站 API
- 针对各种潜在的漏洞利用（包括数据外泄和数据操纵，以及对这些敏感 API 端点的可疑尝试）生成告警
- 通过针对攻击组中所收集的各种 API 攻击的 Web 应用程序和 API 保护策略实施防护



OWASP 识别的其他安全风险

2023 版的 OWASP 十大 API 安全风险是 2019 年以来该非营利组织对其列表进行的首次重大更新。不过，我们不妨回顾一下最初的列表，其中讨论了在当今的环境中仍然有意义的其他安全风险，例如注入攻击。

Akamai 可以通过下列操作来抵御此安全风险：

- 通过签名匹配和异常检测来识别容易受到 API 注入攻击的端点和注入尝试
- 通过对 API 请求进行 JSON 和 XML 检查来应用安全策略，并扫描各种注入攻击，例如 SQLi、XSS、CMDi、RFI 和 LFI
- 针对注入漏洞利用生成告警

OWASP 还发布了其他十大安全风险列表，例如 OWASP 十大 Web 应用程序安全风险。Akamai 的安全产品组合也能够帮助抵御这些安全风险。

我们将随时为您提供帮助！

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 提供出色的安全解决方案、经验丰富的专家和强大的平台，每天会从数百万次 Web 应用程序和 API 攻击、数十亿次爬虫程序请求和多达数万亿次的 API 请求中获取见解。

Akamai 的 Web 应用程序和 API 安全解决方案为您提供安心保护，帮助您的企业抵御较为高级的 Web 应用程序攻击、DDoS 攻击和基于 API 的攻击形式。此外，Akamai Managed Security Service 提供全天候监测、安全管理和威胁抵御。

要详细了解 Akamai 的安全产品组合，请查看我们的网站。如果您想更详细地讨论和了解我们如何合作，从而为您的业务构建最佳防御屏障，请立即联系您的 Akamai 销售代表。

Akamai

Akamai Security 可为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2024 年 9 月。

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯