白皮书

Akamai 如何增强您的安全实践以减轻 OWASP 的 10 大风险

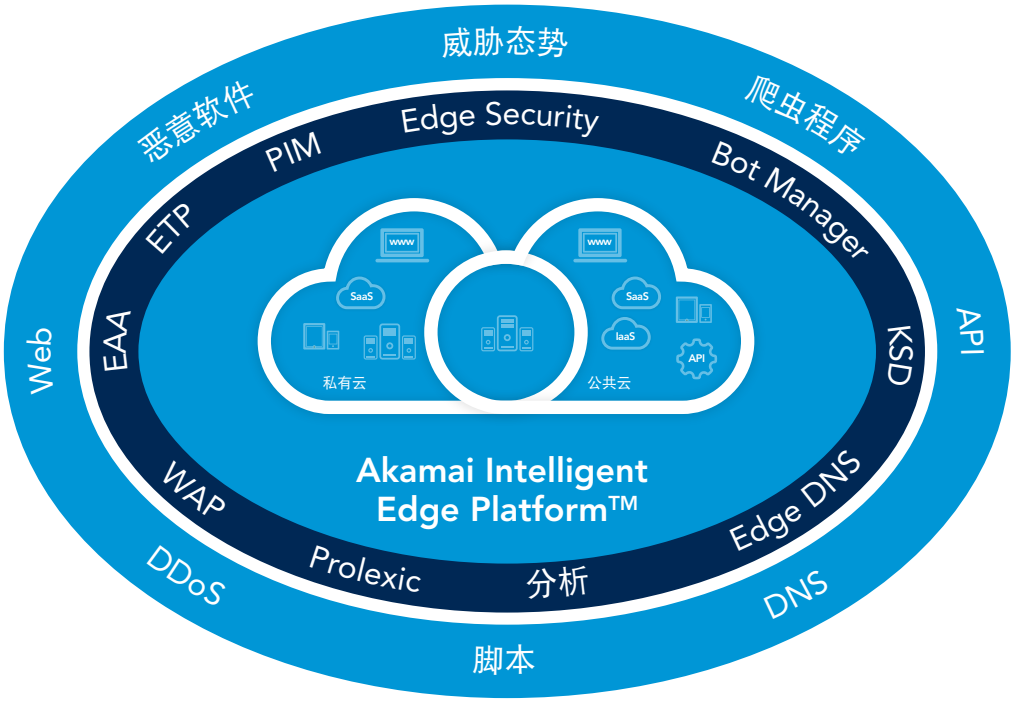
Akamai

简介

《OWASP 10 大漏洞》提供了 Web 应用程序中最常见的漏洞类型的列表。为了指出安全供应商经常会出现的常见误解，《OWASP 10 大漏洞》并不会提供可被 Web 应用程序防火墙 (WAF) 简单阻止的攻击向量清单。相反，它的目标是提高应用程序开发人员针对常见安全漏洞的认知，在一系列开发实践中不断加强此类认知，同时帮助培养安全开发文化。

要应对 OWASP 10 大漏洞，必须了解安全供应商和贵公司在保护 Web 应用程序方面所扮演的角色。某些风险领域只能由应用程序开发人员自己解决。许多安全供应商可在某些领域提供帮助，但通常无法提供针对漏洞的完整或最佳覆盖。更理想的解决方案会提供人员、流程和技术的组合，以减轻与 10 大漏洞相关的风险。

为了全面应对 OWASP 10 大漏洞，必须了解安全供应商可以在哪些方面、如何以及多大程度上帮助改进您自己的开发实践。以下内容介绍了 Akamai 在通过边缘安全解决方案[1]、托管服务[2] 和安全智能边缘平台[3] 为您提供支持方面所能发挥的作用。



漏洞 1：注入

影响：严重	普遍性：常见	可利用性：容易

在将不受信任的数据作为命令或查询的一部分发送到解释程序时会出现注入缺陷（例如 SQL、NoSQL、OS 和 LDAP 注入）。攻击者的恶意数据可能诱使解释程序在未经适当授权的情况下执行意外命令或访问数据。

Akamai 如何提供帮助

公司可以使用 WAF 安全解决方案来保护 Web 应用程序和 API 免受注入缺陷的影响。但是，公司应始终修补 Web 应用程序，以根据其开发生命周期解决发现的任何漏洞。

- Akamai WAF[4] 通过现有的开箱即用规则提供广泛的注入攻击防护。
- 通过使用自定义规则进行虚拟修补，可以帮助快速解决新出现的注入漏洞或应用程序更改带来的新漏洞，直至应用程序得到修补。利用 Akamai 的 OPEN API 功能，虚拟修补也可实现自动化并集成到 DevSecOps 流程中。
- Client Reputation[5] 为“Web 攻击者”类别中高度活跃的恶意客户端提供风险评分，以帮助识别和阻止基于注入的攻击。
- 还可以通过具有“受罚区警报模式”的 WAF，对基于注入的攻击执行进一步的分析。

漏洞 2：受损的身份验证

影响：严重	普遍性：常见	可利用性：容易

与身份验证和会话管理相关的应用程序功能经常出现实施不当的情况，以致于让攻击者可以趁机窃取密码、密钥或会话令牌，或者利用其他实施缺陷临时或永久地假冒其他用户的身份。

Akamai 如何提供帮助

公司必须修复其受损的身份验证过程才能完全解决此漏洞，而 Akamai 可以帮助检测并防范大量尝试利用此漏洞的攻击媒介：

- Akamai WAF 提供速率控制功能，可应对暴力破解攻击。
- 爬虫程序管理解决方案[6] 可以检测和管理撞库攻击中使用的自动化功能。
- HTTP Cookie 可在 Akamai 平台[7] 上进行加密，防止 Cookie 篡改和修改，进而增强身份验证流程。
- Enterprise Application Access (EAA)[8] 可以通过“最低权限访问模式”代理对应用程序的访问，从而缩减应用程序的攻击面，同时通过双重身份验证 (2FA) 和多重身份验证 (MFA) 功能来增强访问。

漏洞 3：敏感数据曝光

影响：严重	普遍性：广泛	可利用性：中等

许多 Web 应用程序和 API 未对财务、医疗和 PII 等敏感数据提供适当的保护。攻击者可能窃取或修改此类保护程度较弱的数据，以进行信用卡欺诈、身份盗窃或其他犯罪活动。敏感数据在缺乏额外保护（例如，静态加密或传输加密）的情况下可能会受到入侵；在通过浏览器交换这些数据时，需要采取特殊的预防措施。

Akamai 如何提供帮助

敏感数据泄露涵盖了数据传输、存储和共享过程的许多方面 - 包括无意中泄露来自未受保护网页的数据 - 无法单独通过任何一个安全解决方案实施全面保护。不过，各种各样的解决方案可以帮助应对此漏洞的不同方面。例如：

- Akamai 可以对传输中的敏感数据进行加密和保护，同时维护 PCI 合规性，方法是仅从带笼式机架的安全 CDN 提供服务，支持所有品牌的 SSL 证书并保护客户的私钥。
- Enterprise Application Access 可以通过加密通信和隐藏机密数据，防止他人窥探网络，从而保护远程访问。
- Enterprise Application Access 还可以与使用 ICAP 的数据丢失防护 (DLP) 解决方案集成，以进一步保护敏感数据免遭泄露。
- Enterprise Threat Protector (ETP)[9] 可帮助应对敏感数据泄露。

漏洞 4：XML 外部实体 (XXE)

影响：严重	普遍性：常见	可利用性：中等

许多较旧或配置不当的 XML 处理器会评估 XML 文档中的外部实体引用。外部实体可用于公开内部文件，在此过程中使用文件 URI 处理程序、内部文件共享、内部端口扫描、远程代码执行和拒绝服务攻击。

Akamai 如何提供帮助

- Akamai WAF 包括相关规则，可以在 XML 解析器处理危险的外部实体之前检测和阻止 XXE 攻击。
- Akamai WAF 包括 API 保护功能且存在 API 请求限制，可以根据预定义格式验证 XML 和 JSON 以阻止 XXE 攻击。

漏洞 5：受损的访问控制

影响：严重	普遍性：常见	可利用性：中等

对经过身份验证的用户可执行的操作的相关限制经常出现实施不当的情况。攻击者可以利用这些缺陷来访问未经授权的功能和/或数据 - 访问其他用户的帐户、查看敏感文件、修改其他用户的数据、更改访问权限等。

Akamai 如何提供帮助

公司必须修复其访问控制模式才能完全解决此漏洞，而 Akamai 可以帮助检测并防范一些尝试利用此漏洞的攻击媒介：

- Enterprise Application Access 针对企业用户启用了最低权限访问模式，仅允许经过身份验证的用户查看和访问经授权的应用程序 - 支持 Zero Trust 安全模式。
- API Gateway[10] 可对 API 实施身份验证以加强访问控制。
- Akamai WAF 可通过站点引用检查来帮助阻止强大的浏览器攻击。
- HTTP Cookie 可在 Akamai 平台上进行加密，进而增强访问控制。

漏洞 6：安全配置错误

影响：中等	普遍性：广泛	可利用性：容易

安全配置错误是最常见的问题。导致这种问题的原因通常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 标头或包含敏感信息的冗长错误消息。公司不仅要确保所有操作系统、框架、库和应用程序得到安全的配置，还要及时予以修补和升级。

Akamai 如何提供帮助

根据定义，安全配置错误 (a.) 涵盖应用程序安全的诸多方面，且 (b.) 要求公司适当地配置安全控件。Akamai 的解决方案虽不能替代正确的配置，但可以帮助防止数据泄露：

- Akamai WAF 包括一个出站异常攻击组，用于捕捉错误代码等信息泄露，以及安全配置错误即时产生的源代码。
- 通过使用自定义规则进行虚拟修补，可以帮助快速解决检测到的数据泄漏问题，直至应用程序得到修补。
- 使用默认凭据的暴力破解攻击可通过速率控制加以防范。
- “内容安全策略”标头上的弱安全配置可在 Akamai 平台上加强。

漏洞 7：跨站点脚本攻击 (XSS)

影响：中等	普遍性：广泛	可利用性：容易

如果应用程序 (a) 在新网页中包括不受信任的数据，但没有正确的验证或跳出，或者 (b) 通过可创建 HTML 或 JavaScript 的浏览器 API 更新现有网页中用户提供的数据，就会出现 XSS 缺陷。利用 XSS，攻击者可在受害者的浏览器中执行脚本来劫持用户会话、损坏网站或将用户重定向到恶意网站。

Akamai 如何提供帮助

公司可以使用 WAF 安全解决方案来保护 Web 应用程序免受 XSS 缺陷的影响。但是，公司应始终修补 Web 应用程序，以根据其开发生命周期解决发现的任何漏洞。

- Akamai WAF 产品具有现有的 XSS WAF 规则，可立即识别和阻止 XSS 攻击。
- 通过使用自定义规则进行虚拟修补，可以帮助快速解决新出现的 XSS 漏洞或应用程序更改带来的新漏洞，直至应用程序得到修补。
- Client Reputation 为“Web 攻击者”类别中的恶意客户端提供风险评分，以帮助阻止基于 XSS 的攻击。
- Akamai 平台可以动态设置安全响应策略标头，以防止 XSS 攻击。

漏洞 8：不安全的反序列化

影响：严重	普遍性：常见	可利用性：困难

不安全的反序列化通常会导致远程执行代码。反序列化缺陷即使不会导致远程执行代码，也可用于执行攻击，包括重放攻击、注入攻击和特权升级攻击。

Akamai 如何提供帮助

公司可以使用 WAF 安全解决方案来保护 Web 应用程序和 API 免受不安全的反序列化缺陷的影响。但是，公司应始终修补 Web 应用程序，以根据其开发生命周期解决发现的任何漏洞。

- Akamai WAF 规则可检测反序列化攻击。
- 通过使用自定义规则进行虚拟修补，可以帮助快速解决新的反序列化缺陷，直至应用程序得到修补。
- Akamai WAF 包括 API 保护功能且具有主动安全模型，可以定义可接受的 XML 和 JSON 对象格式，以便过滤掉恶意制作的 XML 和 JSON。

漏洞 9：使用具有已知漏洞的组件

影响：中等	普遍性：广泛	可利用性：中等

库、框架和其他软件模块等组件使用与应用程序相同的权限运行。此外，脚本还可以充当具备完整应用程序数据访问权限的受信任应用程序资源。如果利用易受攻击的组件，此类攻击可能会导致严重的数据丢失或服务器接管。如果应用程序和 API 使用具有已知漏洞的组件，可能会破坏应用程序防御并导致各种攻击和影响。

Akamai 如何提供帮助

尽管第三方组件很受欢迎且广泛用于减少开发时间和成本，但它们也是最常见的漏洞入口点 - 甚至可借此进入您大多数的专有应用程序。存在多种风险。通常，公司无法跟踪他们的应用程序中正在使用哪些第三方组件，而且安全团队往往都完全没有意识到这一点。此外，公司也控制不了第三方实体解决新发现的漏洞的速度或时间。因此，直接及时地修补应用程序可能极其困难或根本做不到，因而必须使用 WAF 和脚本保护等安全解决方案：

- Akamai WAF 包括多个旨在修复已知漏洞的规则 - 不论漏洞具体是在您的应用程序还是第三方组件中。
- 通过使用自定义规则进行虚拟修补，可以帮助快速解决新出现的漏洞或应用程序更改带来的新漏洞，直至应用程序得到修补。
- Akamai WAF 提供 API 保护功能来帮助第三方组件的 API 抵御利用已知漏洞进行的攻击。
- Client Reputation 为“Web 扫描”类别中的恶意客户端提供风险评分，以帮助防止利用新漏洞。
- Page Integrity Manager 通过检测可疑脚本行为并提供切实可行的见解来阻止恶意活动，从而帮助 Web 应用程序抵御新的威胁（例如 Web 窃取、表单劫持和 Magecart 攻击）。
- Page Integrity Manager 使用不断更新的常见漏洞和风险 (CVE) 数据库，阻止数据从第一方和第三方脚本泄露到具有已知漏洞的 URL。

漏洞 10：日志记录和监控不足

影响：中等	普遍性：广泛	可利用性：中等

日志记录和监控不足，再加上与事件响应的集成缺失或无效，让攻击者有机可乘，他们将能够进一步攻击系统，维护持久性，转向更多系统以及篡改、提取或销毁数据。大多数漏洞研究表明，检测漏洞的时间通常超过 200 天，而且此类漏洞通常是被外部方检测到的，而并非被内部的流程或监控功能检测到。

Akamai 如何提供帮助

日志记录和监控不足本身随不会构成漏洞，但是表明了公司在相关方面的能力不足，无法解决漏洞并阻止借此发起攻击的企图。Akamai 提供如下多种功能来帮助公司更好地了解攻击：

- Akamai 在 Akamai Luna Control Center[11] 图形用户界面中提供仪表板和报告工具。
- Akamai 支持与公司现有的 SIEM 基础设施集成，以便将 Akamai 检测到的事件与其他安全供应商检测到的事件关联起来。
- Akamai 管理的安全服务提供全天候分析和响应功能。
- Akamai WAF 包括一项“受罚区”功能，可以增加对可疑会话的日志记录，以便进一步深入分析。
- Akamai Enterprise Application Access 提供了集成的身份管理解决方案，支持验证和控制对所有企业应用程序的访问。与其身份识别代理功能结合使用时，公司可以更具体地了解用户操作，甚至包括监控每个 GET/POST 操作。
- 借助 Akamai Enterprise Threat Protector，您能够完全了解企业的所有外部 DNS 请求 - 恶意和善意请求。

结论

如果公司及其安全供应商能够协同工作，确保人员、流程和技术协调一致，就可以实现针对 OWASP 10 大漏洞的最佳防御。Akamai 提供行业领先的技术和经验丰富的人员，确保与您的流程协调一致。要了解有关 Akamai 边缘安全产品组合的更多信息，请查看我们网站上的详细信息。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，请联系您的 Akamai 销售代表。

资料来源

1. 边缘安全
2. 服务与支持
3. Akamai Intelligent Edge Platform™
4. Kona Site Defender (KSD) 和 Web Application Protector (WAP)
5. Client Reputation
6. Bot Manager
7. Secure CDN
8. Enterprise Application Access
9. Enterprise Threat Protector
10. API Gateway
11. Luna Control Center

Akamai Experience the Edge