Akamai

电子书

OWASP 10 大漏洞

Akamai 如何帮助防范常见漏洞

前言

开放 Web 应用程序安全项目 (OWASP) 10 大漏洞列表涵盖了 Web 应用程序中最常见的漏洞，旨在增强企业的安全意识。为了全面应对 OWASP 10 大漏洞，您有必要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。以下将详细分析 OWASP 10 大漏洞，介绍每种漏洞类别，并阐述 Akamai 如何通过边缘安全解决方案、托管服务以及全球领先的智能边缘平台来为企业提供支持。

Akamai 产品

OWASP 10 大漏洞		Account Protector	Akamai Guardicore Segmentation	App & API Protector	Bot Manager	Enterprise Application Access	Enterprise Threat Protector	Identity Cloud	Managed Security Services	Akamai MFA	Page Integrity Manager
权限控制失效	A01			✓	✓	✓		✓		✓	
加密机制失效	A02			✓		✓	✓				✓
注入	A03			✓							
不安全的设计	A04			✓		✓					
安全配置错误	A05		✓	✓	✓						
危险或过旧的组件	A06		✓	✓							✓
认证及验证机制失效	A07	✓		✓	✓	✓		✓		✓	
软件和数据完整性失效	A08		✓	✓			✓				✓
安全日志记录和监控失效	A09		✓	✓		✓	✓		✓		
服务器端请求伪造	A10		✓	✓							

OWASP 10 大漏洞是风险类别，而不是单一风险。Akamai 的解决方案将通过多种方式来应对这些风险类别。阅读白皮书以了解更多信息。

A01：权限控制失效

> “权限控制会实施相关策略，确保用户无法执行其预期权限以外的操作。权限控制失效通常会导致未经授权的信息泄露、修改或破坏所有数据，或执行超出用户限制的业务功能。”
>
> —— 来源：owasp.org

Akamai 如何提供帮助

虽然企业必须修复访问控制模式才能完全修复“权限控制失效”漏洞，但 Akamai 凭借在 WAAP 领域的深厚专业能力，可以帮助您检测并防范尝试利用此漏洞的一些攻击媒介：

- **Enterprise Application Access** 为企业用户启用了最小权限访问模式，仅允许通过身份验证的用户对授权应用程序进行查看和访问——支持 Zero Trust 安全模式。
- **Akamai MFA** 基于可防范网络钓鱼的 FIDO2 技术标准提供强大的身份验证服务。
- **App & API Protector**（Akamai WAAP 解决方案）可通过检查“引用站点”标头来阻止强力浏览器攻击，并实施 API 身份验证来加强基于 Akamai API Gateway 的访问控制。
- **Identity Cloud** 可提供对最终用户数据的精细访问控制，为每个内部用户或系统启用最小权限访问。
- **Bot Manager** 可防止自动化工具攻击和登录攻击。

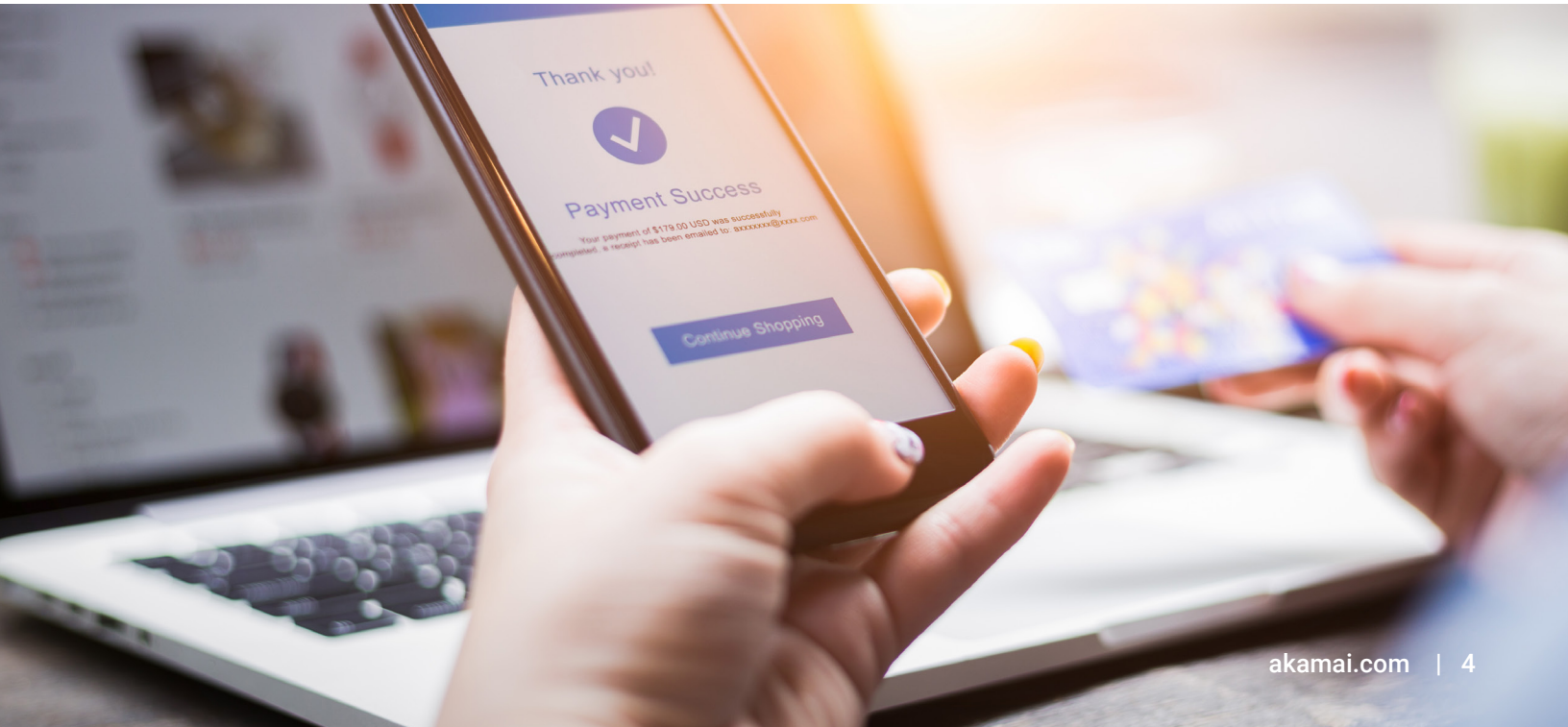
A02：加密机制失效

> “重点是与加密机制相关的失效（或缺乏加密机制）。这通常会导致敏感数据泄露。…例如，密码、信用卡号、健康记录、个人信息和商业机密需要得到额外的保护，主要是为符合隐私法的相关数据提供保护。”
>
> —— 来源：owasp.org

Akamai 如何提供帮助

企业无法使用任何一种安全解决方案来彻底防止加密机制失效。不过，结合使用各种不同的解决方案有助于应对此漏洞在部分方面的问题。例如，Akamai 的：

- **App & API Protector** 使用最新版本的 TLS 和强密码来为传输中的敏感数据提供加密和保护。它还有助于：
  - 仅通过安全 CDN 来提供服务，从而确保符合 PCI 标准。该安全 CDN 支持所有品牌 TLS 证书并且将保护客户的私钥。
  - 提供受操作和物理安全机制（例如笼式机架和运动检测器）保护的 CDN，确保只有授权人员才能访问服务器。
  - 通过 API PII 学习来定位和防止敏感数据泄漏。
- **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 Threat Protector** 可以帮助防止敏感数据泄露。
- **Page Integrity Manager** 还可以检测基于 JavaScript 代码滥用的 PII 数据泄漏，这可能是由加密机制失效引起的。



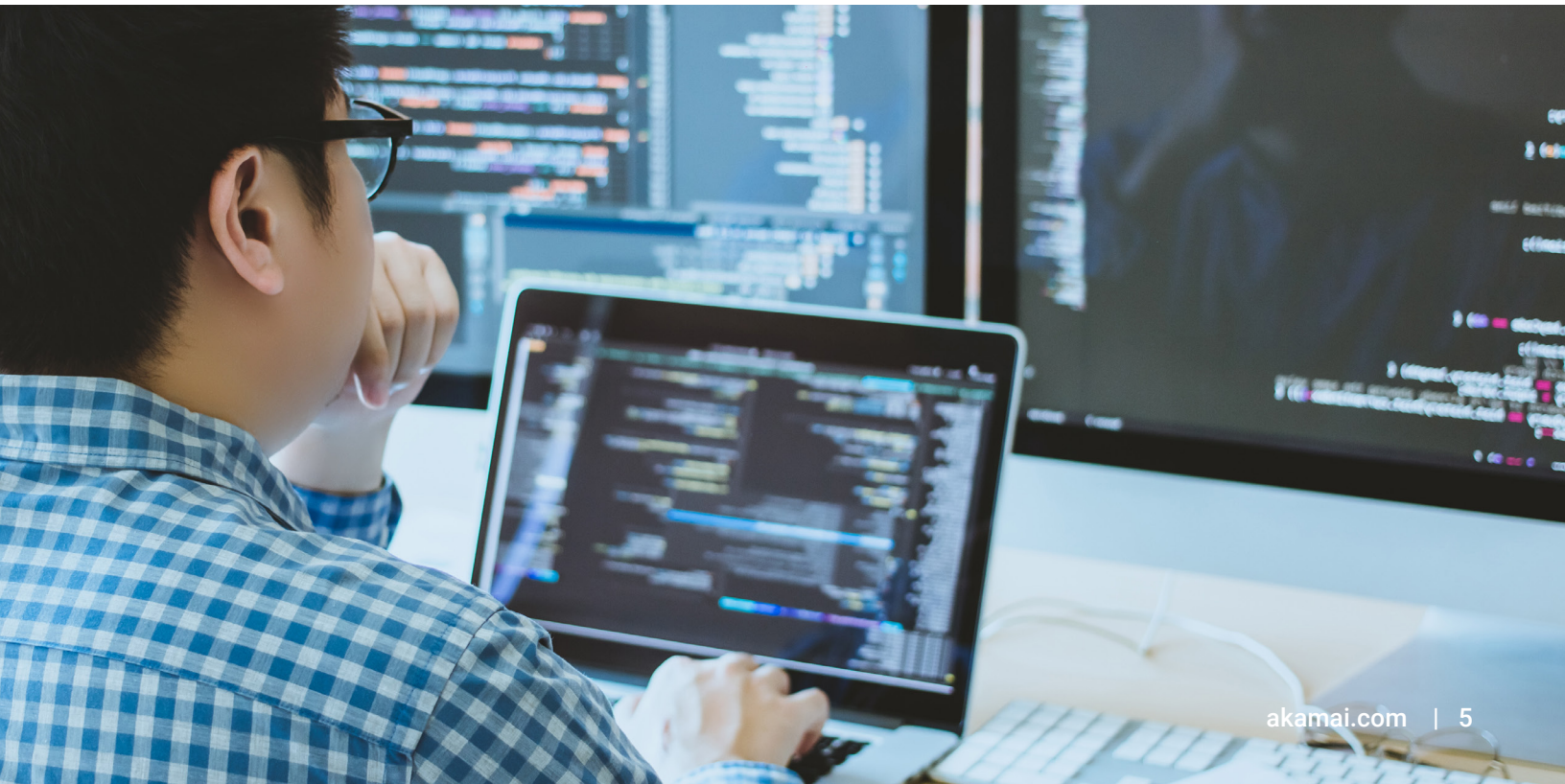
A03：注入攻击

> “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。”
>
> —— 来源：Akamai

Akamai 如何提供帮助

您可以使用 WAAP 来缓解来自 Web 应用程序和 API 注入缺陷的风险。但是，企业应始终修补 Web 应用程序，以根据其各自的开发生命周期来解决发现的任何漏洞。

- **App & API Protector** 提供行业领先、配备自适应安全引擎 (ASE) 的 WAAP 解决方案，可通过现有的开箱即用规则提供广泛的注入攻击保护。ASE 受罚区可以暂时阻止来自最近尝试使用 WAAP 进行注入攻击的客户端的所有流量。
- 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。安全部门还可以利用 Akamai 的 API 功能实现自动化虚拟修补，并将其集成到 DevSecOps 流程中。
- **Client Reputation** 可以帮助识别和阻止基于注入的攻击，并为 Web 攻击者类别中高度活跃的恶意客户端提供风险评分。



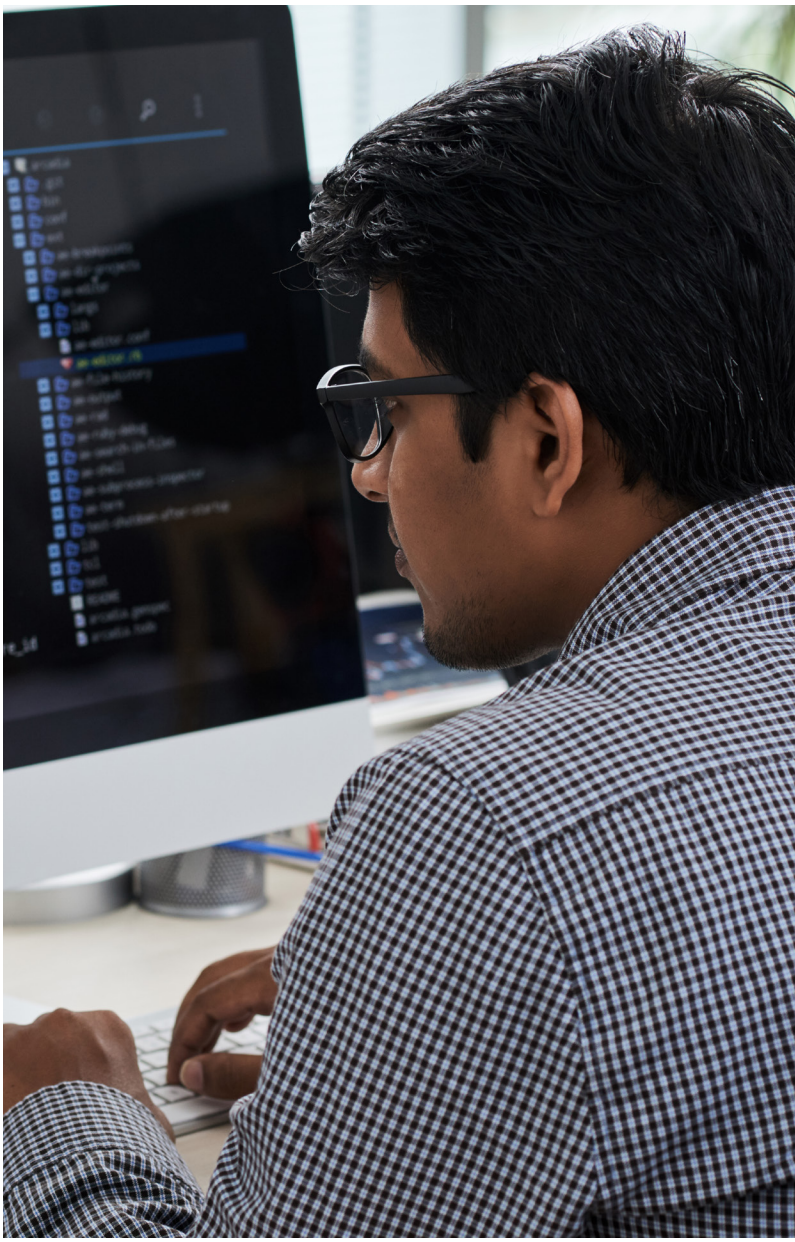
A04：不安全的设计

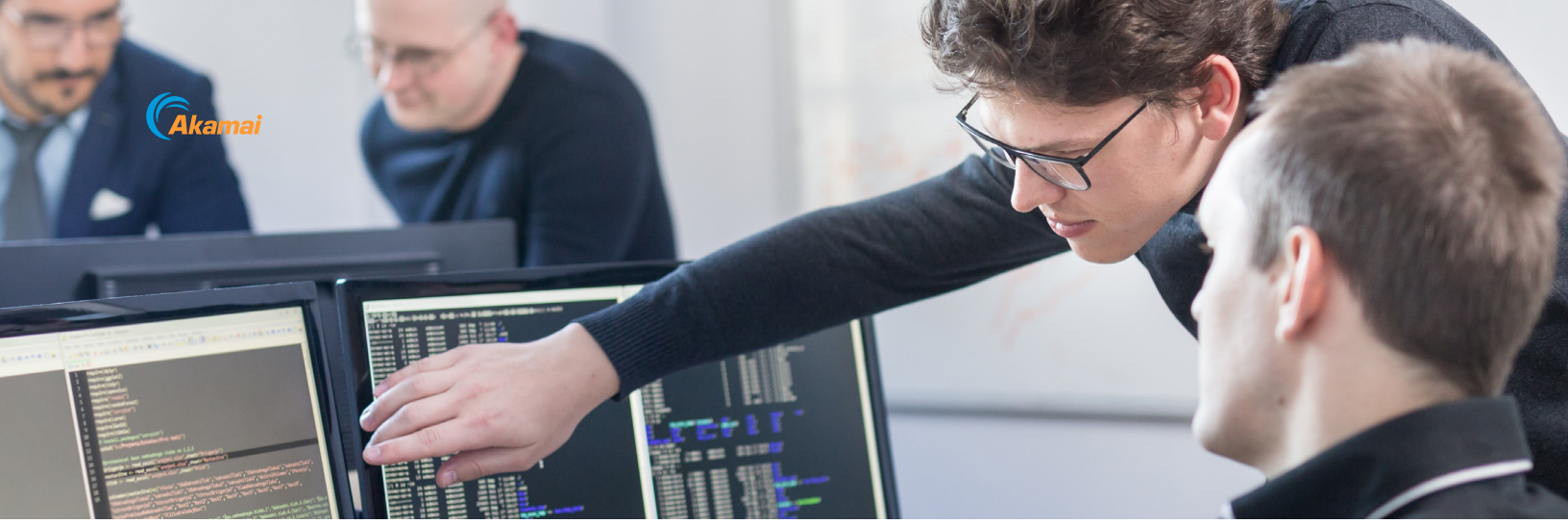
> “不安全的设计是一个广泛的类别，代表许多不同的弱点，其具体表示是‘控制设计缺失或无效’。不安全的设计与不安全的实施是有区别的。安全的设计仍然可能存在实施缺陷，并可能会导致被攻击者利用的漏洞。完美实施也无法解决不安全的设计问题，因为根据定义，不安全的设计从未创建所需的安全控制来防范特定攻击。”
>
> —— 来源：owasp.org

Akamai 如何提供帮助

企业应该在设计之初便将安全性考虑在内。但是，如果安全性整合难度较大，开发团队可能无法实现这一目标。Akamai 产品可以帮助企业加快“左移”，以防止任何设计不安全因素影响其应用程序和 API。

- **App & API Protector**（包括我们的 WAAP 解决方案和 ASE）也可以检测和修复要投入到生产环境中的一些设计缺陷。它还利用自动化来分流和简化日常任务，并将需要人工分析的任务留给人类。这种自动化包括自动更新、自主调优、API 发现、简化的可编程性和用户体验。
- **Enterprise Application Access** 可确保只有授权用户才能访问应用程序。这种最小权限方法可以防范针对其他应用程序的横向移动攻击，而一些网络访问解决方案（如 VPN）就很容易发生这样的攻击。





A05：安全配置错误

> “自上一版以来，90% 的应用程序都针对某种形式的错误配置进行了测试，其平均安全事件发生率为 4%，并且此风险类别在常见缺陷列表 (CWE) 中出现了 20.8 万次。如果未建立协同一致、可重复的应用程序安全配置流程，系统将面临更高的风险。”
>
> —— 来源：owasp.org

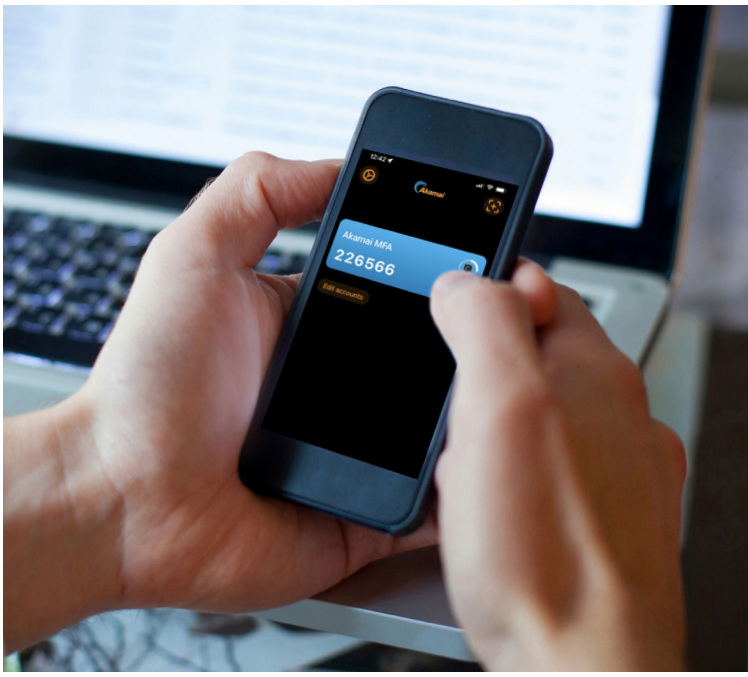
Akamai 如何提供帮助

根据定义，安全配置错误涵盖应用程序安全的多个方面。它还要求企业正确配置安全控制。Akamai 的产品可以通过以下方式提供帮助：

- 尽管不能替代正确的配置，但 **App & API Protector** 可以提供以下帮助：
  1. 使用出站异常攻击组来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。
  2. 实施相关规则，可在 XML 解析器处理危险的外部实体之前检测和阻止 XXE 攻击。
  3. 实施相关规则，可检测对开发人员在生产服务器上留下的已知敏感文件的访问。
- **Akamai Guardicore Segmentation** 可以监测和精细控制应用程序与互联网之间任何未经授权或计划外的通信，从而帮助防范因配置错误而导致的数据泄漏。
- 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，直至您的团队能够修补应用程序。
- **App & API Protector** 和 **Bot Manager** 可以通过速率控制来防范使用默认凭据的暴力攻击。
- 内容安全策略和其他与安全相关的 HTTP 标头上的弱安全配置可在 Akamai 平台上加强。
- 借助 **App & API Protector** 中的自动 API 发现功能，您可以自动持续地发现和分析您的 API，包括端点、定义以及资源和流量特征。

A06：危险或过旧的组件

> “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。”
>
> —— 来源：Akamai



Akamai 如何提供帮助

企业通常无法跟踪（而安全团队通常完全不知道）他们的应用程序中包含哪些第三方组件。此外，企业无法控制第三方修复新发现漏洞的速度（如果有的话）。如果要应对这种缺乏可见性和确定性的问题，企业就需要要使用适当的安全解决方案，比如以下 WAAP 和脚本保护解决方案：

- **App & API Protector** 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。它还提供 API 保护功能，即使 API 中整合的第三方组件会因开放而导致滥用，也能为 API 提供保护。
- 借助 **Akamai Guardicore Segmentation** 洞察模块，您可以查询网络中可能易受攻击的任何资产。不仅如此，借助内置精细实施，您还可以在应用补丁之前对任何受影响的资产进行隔离。
- 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。
- **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** 可持续分析真实用户会话中的脚本执行行为，以识别可疑或明显的恶意行为。它还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。

A07：认证及验证机制失效

> “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。”
>
> —— 来源：Akamai

Akamai 如何提供帮助

企业需要解决其内部缺陷才能完全修复此漏洞。尽管如此，下面列出的 Akamai 解决方案可以帮助检测和防范许多尝试利用认证及验证机制失效的攻击媒介：

- **Bot Manager** 可以检测和抵御自动攻击，例如撞库攻击中使用的攻击方式。
- **Account Protector** 可抵御帐户接管攻击，防范冒名顶替者在未经授权的情况下获取用户帐户的访问权限。
- **Enterprise Application Access** 可以通过“最小权限访问模式”代理对应用程序的访问，从而减小应用程序的攻击面并增强访问权限。
- **Akamai MFA** 使用可防范网络钓鱼的 FIDO2 技术提供强大的身份验证。
- **App & API Protector** 提供速率控制功能，可应对暴力破解攻击。
- **Identity Cloud** 提供对最终用户凭据和配置文件信息的安全管理，并通过双重身份验证和基于风险的身份验证功能提供安全保护。

A08：软件和数据完整性失效

> “软件和数据完整性失效与无法防止完整性违规的代码和基础架构有关。这方面的一个示例是应用程序依赖来自不受信任的来源、代码库和内容交付网络 (CDN) 的插件、库或模块。不安全的 CI/CD 管道可能会导致未经授权的访问、恶意代码或系统破坏。”
>
> —— 来源：owasp.org

Akamai 如何提供帮助

企业可以使用 WAAP 保护 Web 应用程序和 API 免受软件和数据完整性失效的影响。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。

- **App & API Protector**
  - 提供强大的反序列化攻击保护。
  - 实施最新的 TLS 版本和强密码来防范可能导致数据完整性问题的中间机器攻击。
  - 通过实施采用 Edge DNS 的 DNSSEC，从而确保为 DNS 记录提供数据源身份验证和数据完整性保护。这可以防止篡改 DNS 记录，从而避免用户被引导至不受信任的来源。
- 借助 **Akamai Guardicore Segmentation** 中的洞察模块，您可以查询网络中可能易受攻击的任何资产。不仅如此，借助内置精细实施，您还可以在创建修复之前对任何受影响的资产进行隔离。
- **Enterprise Threat Protector** 可以检测网络钓鱼攻击。此类攻击旨在将应用程序的管理员和超级用户引诱到容易受到攻击的环境或不受信任的来源。
- 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。
- **Page Integrity Manager** 可以检测第三方脚本，监控其变化，然后对已受到破坏的脚本采取措施。

A09：安全日志记录和监控失效

“日志记录、检测、监控和主动响应能力不足的情况时有发生：

- 未记录可审计事件，例如登录、登录失败和高价值交易。
- 警告和错误生成不充分或不明确的日志消息，或未生成日志消息。
- 未监控应用程序和 API 的日志中的可疑活动。
- 日志仅存储在本地。
- 无效的警报阈值和响应升级流程，或未建立该流程。
- 基于动态应用程序安全测试 (DAST) 工具的渗透测试和扫描无法触发警报。

应用程序无法实时或近乎实时地检测和升级主动攻击，或发出相关警告。”

—— 来源：owasp.org

Akamai 如何提供帮助

安全日志记录和监控失效会导致企业在修复漏洞的能力方面存在缺口，并导致这些漏洞被恶意人员利用。Akamai 提供如下多种功能来帮助企业更好地了解攻击：

- Akamai 在 Akamai Control Center 图形用户界面中提供仪表板和报告工具。
- Akamai 的应用程序安全产品与企业现有的 SIEM 基础架构相集成，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。
- **Managed Security Service** 提供 24/7 全天候分析和响应功能。
- **App & API Protector** 包含一项受罚区功能，可允许增加 IP 日志记录以显示恶意或可疑活动，以便进行进一步深入分析。
- **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。与其身份感知代理功能结合使用时，企业可以精细地了解用户操作，甚至包括监控每个 GET/POST 操作。
- 借助 **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。
- **Akamai Guardicore Segmentation** 可提供关于网络内部通信流的深入可见性，因此可以在发生未经授权的通信或意外通信时触发警报，并且可以在各个进程或服务级别实施安全策略以限制此通信。借助添加的违规检测模块，企业可以快速检测和修复潜在威胁。

漏洞 10：服务器端请求伪造

> “只要 Web 应用程序在未验证用户提供的 URL 的情况下获取远程资源，就会发生 SSRF 缺陷。这让攻击者能够强制应用程序将精心设计的请求发送到意外目的地，甚至可以绕开防火墙、VPN 或其他类型的网络访问控制列表 (ACL) 的保护措施。”
>
> —— 来源：owasp.org

Akamai 如何提供帮助

Akamai WAAP 包含可以查找 URL 注入的规则。此功能可以防止攻击者诱导服务器进入其他位置并提交请求 - 这样会让您的安全分析师认为这像是有效请求。

- **App & API Protector** 规则有助于防止这些漏洞利用请求到达易受攻击的服务器。
- **Akamai Guardicore Segmentation** 可以在服务器级别监控和阻止意外的出站流量。

结论

要针对 OWASP 10 大漏洞建立最佳防御方案，企业需要与其安全供应商携手合作，尽快发现漏洞并实施适当的解决方案来缓解这些漏洞。详细了解 Akamai 的边缘安全产品组合。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。