White Paper

A Game Plan for OWASP Top 10 API Security Risks

How Akamai can help you address common API vulnerabilities and threats

Akamai Security



OWASP Top 10 API Security Risks

OWASP Top 10	Can Akamai help?
Broken Object Level Authorization	
Broken Authentication	
Broken Object Property Level Authorization	
Unrestricted Resource Consumption	
Broken Function Level Authorization	
Unrestricted Access to Sensitive Business Flows	
Server-Side Request Forgery	
Security Misconfiguration	
Improper Inventory Management	
Unsafe Consumption of APIs	

APIs live at the core of an enterprise's digital operations and cloud services, and increasingly at the core of the generative AI technologies that are redefining global business. They are the essential glue for microservices-based architectures, allowing applications to communicate and scale at unprecedented speeds. However, this same connectivity makes them a high-stakes target. While APIs drive innovation and boost revenue, they also represent security risk that is being magnified by the rapid adoption of artificial intelligence (AI).

Exposed or misconfigured APIs are prevalent, easy to compromise, and frequently sit outside the view of traditional security perimeters. The risks are greater than ever. In fact, 87% of organizations reported experiencing at least one API security incident in the past year, with the average financial impact now reaching US$700,000 per organization, according to the 2026 **Akamai API Security Impact Study**.

It's not a recent development. For years, organizations have struggled to achieve a full inventory of their APIs, but now the rapid and widespread adoption of AI is compounding the problem. As enterprises rush to integrate large language models (LLMs) and autonomous agents into the business, their sprawling, unmapped attack surface is only growing. Today, 42% of API security incidents involve APIs linked to enterprises' AI technologies. This surge in complexity has amplified a critical visibility gap.

> **Four years ago, only 40% of enterprises with full API inventories knew which of their APIs returned sensitive data. That number has since dropped to 23% at a time when a cleverly crafted prompt can trick an AI application's underlying API into sharing customer info, with no questions asked.** [1]

1 Akamai, 2026 Akamai API Security Impact Study, April 2026

For many enterprises, the attack surface has expanded much faster than their internal understanding of:

- **AI-driven API threats:** How attackers use automation to find vulnerabilities
- **Modern attack methods:** Including broken object level authorization (BOLA) and business logic abuse
- **Security controls:** The specific capabilities needed to protect AI-integrated environments

What can help? Many security teams turn to a foundational resource from the nonprofit Open Worldwide Application Security Project: The OWASP Top 10 API Security Risks.

The OWASP Top 10 API Security Risks provides the necessary framework to understand and address vulnerabilities stemming from misconfigurations, lax authentication, and unauthorized data access. It also offers a roadmap for identifying API abuse and protecting your organization from threats like BOLA.

Learn what the key OWASP-identified risks are and see how Akamai's API security solutions can help you mitigate them in an increasingly AI-driven threat landscape.

42%

Percentage of companies that experienced API attacks linked to AI technologies, such as apps, agents, and LLMs*



*2026 Akamai API Security Impact Study

Broken Object Level Authorization

Broken object level authorization (BOLA) vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs. This vulnerability can provide an opening for attackers to access resources directly, bypassing the anticipated application workflow and gaining unauthorized access to sensitive data. Organizations can reduce this risk by avoiding sole reliance on object IDs that clients pass in their requests. Instead, organizations can use non-guessable, random IDs for objects to ensure robust validation for every object. When appropriate, masking the true ID of objects can provide an additional layer of security.

How Akamai can help with BOLA vulnerabilities

Akamai's vigilant surveillance systems track threats and generate alerts for attempted BOLA exploitation, ensuring immediate attention and action.

Akamai mitigates risk by:

- Identifying BOLA exploitation attempts
- Classifying API endpoints susceptible to BOLA exploitation based on received inputs (e.g., enumerable parameters) as well as the relationships between API objects and properties
- Generating alerts on attempted or successful BOLA exploitation

33%

Percentage of organizations that cite "lack of visibility into AI/LLM-linked APIs and their risks" as one of their top three API risks*



*2026 Akamai API Security Impact Study

Broken Authentication

Broken authentication refers to broad vulnerabilities in the authentication process, exposing the system to attackers who can exploit these weaknesses to compromise API object protection. Typically, attackers capitalizing on broken authentication vulnerabilities manipulate loopholes in the system, such as weak passwords or session replay. To protect against broken authentication vulnerabilities, organizations can establish robust authentication and secrets management mechanisms, such as strong password policies, key rotation, strong token signatures, and encryption keys. Enforcing these stringent policies organization-wide can significantly reduce risk.

How Akamai can help with broken authentication

Akamai fortifies API security by identifying and rectifying weak authentication points, thwarting automated attacks, and proactively alerting on attempted exploitation attacks.

Akamai mitigates this risk by:

- Identifying API endpoints that do not require authentication or do not follow authentication best practices, such as weak token signatures or encryption keys and the acceptance of expired authentication tokens
- Protecting against automated dictionary or credential stuffing attacks through our bot management capabilities
- Handling authorization of JSON Web Tokens using strong token signatures through Akamai API Gateway capabilities
- Generating alerts on attempted broken user authentication exploitation

API testing: The need for speed is slowing down security

As organizations race to innovate, API testing remains a critical yet inconsistent pillar of the software development lifecycle (SDLC). **According to the 2026 Akamai API Security Impact Study** only 16% of organizations have security testing embedded across every stage of development. Instead, 30% report only partial integration into SDLC and CI/CD processes — a fragmented approach that increases remediation costs and allows vulnerabilities to slip into production.

A notable gap also persists between leadership and security practitioners. While 40% of C-suite executives claim advanced API testing maturity, only 28% of DevSecOps teams — the professionals on the front lines — agree. This discrepancy often stems from an overreliance on functional testing. While 44% of enterprises focus primarily on whether an API works, only 35% employ fully mature testing that targets real-world attack methods.

This vulnerability is being compounded by the rise of AI coding assistants. While these tools accelerate development, they often produce ungoverned code, exacerbating the trend of untested, vulnerable APIs. In fact, the surge in AI-generated code is now a top-three driver for organizations increasing their API security focus.

Broken Object Property Level Authorization

Broken object property level authorization (BOPLA) is a security flaw where an API endpoint unnecessarily exposes more data properties than required for its function, neglecting the principle of least privilege.

This flaw can inadvertently provide attackers with excessive data that can then be used to unearth more vulnerabilities or mine for sensitive data. This includes scenarios where properties exclusive to admin-level access can be manipulated by unauthorized users, further compromising system integrity. To ensure security and to prevent attackers from getting or manipulating surplus information, it is critical to provide appropriate access levels and data exposure, impeding potential attackers from exploiting these oversights.

How Akamai can help with BOPLA flaws

Leveraging Akamai's comprehensive tactics, companies are able to mitigate the risks of BOPLA by identifying and cataloging API endpoints and their associated properties.

Akamai mitigates this risk by:

- Identifying and labeling all endpoints and the API properties they expose, such as personally identifiable information (PII)
- Identifying undocumented or shadow API endpoints, objects, and properties, as well as abnormal properties
- Applying security policies on acceptable and defined parameters and properties to ensure data sanitization
- Applying security policies based on the full OpenAPI/Swagger specification and only allowing well-defined API endpoints and methods to access API objects and properties
- Generating alerts on attempted BOPLA exploitations

Unrestricted Resource Consumption

Unrestricted resource consumption (sometimes called “API resource exhaustion”) is a type of vulnerability where APIs do not limit the number of requests or the volume of data they serve within a given time. This oversight can open the door for attackers who seek to perform denial-of-service (DoS) attacks, which can make the system unavailable to legitimate users. Such exploitations can have serious business implications, resulting in loss of service availability, customer dissatisfaction, and potential revenue losses, depending on the length and range of the outage. It is critical to have measures in place that limit the rate of API requests and the size of data returns to prevent loss of service.

How Akamai can help with unrestricted resource consumption

Akamai secures your APIs from unrestricted resource consumption threats by:

- Identifying at-risk endpoints and providing real-time alerts on attempted volumetric attacks
- Spotting excessive errors, login attempts, or atypical behavior indicating risk

Akamai mitigates this risk by:

- Identifying API endpoints that are lacking rate limits or are under attack through large volumetric dictionaries or credential stuffing attacks
- Initiating workflows to slow down or block volumetric attacks
- Generating alerts on attempted volumetric attacks

Broken Function Level Authorization

Broken function level authorization (BFLA) can occur when access control models for API endpoints are incorrectly implemented. Incorrect or outdated access control methods can fail to adequately restrict unauthorized access — allowing attackers to access sensitive information or the system as a whole. To mitigate this risk, organizations can adopt the principle of least privilege, ensuring that all functions, particularly administrative ones, are only accessible to users with appropriate permissions.

How Akamai can help with BFLA

By tracking behavioral timelines, applying security policies to sensitive functions, managing key rotation and revocation, and prompt alerting of any suspicious attempts, Akamai can help to fortify organizations' BFLA prevention and response strategy.

Akamai mitigates this risk by:

- ✓ Identifying behavioral timelines on API endpoint access through capturing users, API keys, access tokens, session IDs, etc.
- ✓ Applying key rotation or exposed key revocation through Akamai API Gateway
- ✓ Generating alerts on suspicious attempts to access administrative functions

The AI frontier: OWASP extends outlook to LLM applications

The mass adoption of LLMs has triggered a significant shift in enterprises' approach to security. OWASP recognized that traditional security frameworks were ill-equipped for the nondeterministic nature of generative AI. Unlike standard code, which follows logic-based rules, LLMs process natural language — creating a loophole for attackers to bypass traditional security filters via prompt injection.

This led to the development of the **OWASP Top 10 for Large Language Model Applications** in mid-2023. It has since been folded into a larger initiative called the **OWASP GenAI Security Project** — and, in 2025, it was updated to address the rise of "agentic AI"; that is, models that don't just generate text, but take autonomous actions.

For API security, this framework is the new front line. Most enterprise LLMs interact with internal data through plug-ins and retrieval-augmented generation (RAG), both of which rely heavily on APIs. Risks like **LLM08: Excessive Agency** occur when an LLM is granted overprivileged API access, allowing a malicious prompt to trigger unauthorized actions, such as database deletions or data exfiltration. In this new landscape, the LLM effectively becomes a privileged user of your APIs. Securing the interface where the model meets your back-end systems is now just as critical as the traditional OWASP API protections.

Unrestricted Access to Sensitive Business Flows

Unrestricted access to sensitive business flows arises when an API exposes critical operations like business logic without sufficient access control. This can lead to unauthorized access and exploitation, causing significant harm to an organization. Exploitation typically involves understanding the business model backed by the API, identifying sensitive business flows, and exploiting loopholes to these flows. This can lead to impacts like preventing legitimate users from purchasing a product.

How Akamai can help with unrestricted access

Secure your business with Akamai's comprehensive API protection solutions, offering sensitive endpoint identification, real-time exploitation alerts, and expert consultancy to safeguard your critical data and operations.

Akamai mitigates this risk by:

- Identifying sensitive API endpoints, such as payment flows or endpoints handling PII
- Generating alerts on a variety of potential exploitations ranging from data exfiltration to data manipulation and suspicious attempts on these sensitive API endpoints
- Discovering, tagging, and assembling an inventory of all APIs that connect to GenAI models, LLMs, and AI services, including shadow and unmanaged endpoints



Server-Side Request Forgery

Server-side request forgery (SSRF) allows an attacker to induce the server-side application to make HTTPS requests to an arbitrary domain of the attacker's choosing. In a typical SSRF attack, the attacker tricks the server into making a request to internal resources, thereby bypassing firewalls and gaining access to internal services, which can lead to data exposure or remote code execution. To mitigate this risk, it's crucial to validate, filter, or sanitize user input and limit the outbound connections your server can make, ensuring that it only communicates with critical services.

How Akamai can help with server-side request forgery

Strengthen your security posture with Akamai, delivering anomaly detection in trusted API connections, effective key management, and immediate notifications on SSRF exploitation attempts.

Akamai mitigates this risk by:

- Applying protection through web application and API protection policies targeting SSRF attacks
- Applying key rotation or exposed key revocation through API Gateway

What businesses say they are using to secure their APIs*

80%
Web application firewalls (WAFs)

40%
Web application and API protection (WAAP) solutions

35%
Dedicated API security tools

*2026 Akamai API Security Impact Study

Security Misconfiguration

Security misconfiguration refers to the improper setup of security controls, which can leave a system vulnerable to attacks. This could include insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP(S) headers, and verbose error messages containing sensitive information. To mitigate risks, it's vital for organizations to ensure they have correctly configured their security controls across all aspects of their applications and APIs. This involves regular updates, thorough testing, and continuous monitoring to identify and rectify any misconfigurations promptly.

How Akamai can help with security misconfiguration

Enhance your insights as Akamai helps you identify shadow, rogue, or zombie API endpoints, align with security best practices, achieve robust HTTPS implementation, and receive instant alerts on security misconfigurations.

Akamai mitigates this risk by:

- Identifying shadow API endpoints that might expose low-level environments (e.g., testing and staging environments)
- Identifying and matching API endpoints, objects, and properties against security configuration best practices and standards
- Applying security policies through API security best practices, such as well-formed HTTPS requests and responses, configuring or removing correct HTTP headers, and ensuring full control over cross-origin resource sharing (CORS) and cache control headers
- Applying proper HTTPS implementation through SSL/TLS, including correct and secure cipher suites
- Generating alerts for misconfiguration or noncompliance withAPI security best practices and standards

Improper Inventory Management

Improper inventory management is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including shadow APIs — may be left unpatched and vulnerable to attack. This can lead to outdated components, unused pages or APIs, and unnecessary exposure of sensitive information. Unmaintained service management can make systems vulnerable to threats, and attackers can potentially gain access to sensitive data, or even the server, through unknown APIs that are connected to the same database. Access controls and regular audits are essential for avoiding constantly changing components of an organization's services.

How Akamai can help with improper API inventory management

Akamai persistently oversees API traffic to help discover hidden API endpoints and APIs with potential risks, providing organizations secure data storage, advanced threat analysis, and immediate alerts on potential exploitations.

Akamai mitigates this risk by:

- Continuously monitoring exposed API traffic flowing through your environments, including north-south API endpoints targeting publicly accessible APIs and east-west internal API endpoints
- Identifying shadow API endpoints that might expose low-level environments (e.g., testing and staging environments) or undocumented and/or deprecated API versions
- Creating an up-to-date API inventory based on risk scoring and data classification
- Generating alerts on a variety of potential exploitations ranging from data exfiltration to data manipulation and suspicious attempts on these sensitive API endpoints

Unsafe Consumption of APIs

Unsafe consumption of APIs refers to the risks associated with the use of third-party APIs without proper security measures in place. Organizations are increasingly reliant on third-party APIs to extend services and functionality, so these APIs are often trusted by default. This can lead to significant security vulnerabilities. Not implementing proper encryption, data validation, sanitization, and resource consumption limits can open organizations up to significant vulnerabilities. To mitigate these risks, organizations can implement encryption for all data transmitted over the network, validate and sanitize all data inputs, and set reasonable limits on resource consumption.

How Akamai can help with unsafe consumption of APIs

Continuously protect your systems by monitoring and validating your services to ensure security with Akamai's monitoring, alerting, and consulting services.

Akamai mitigates this risk by:

- Monitoring continuously on all exposed API traffic flowing through your environments, including east-west and outbound APIs that facilitate B2B and/or third-party integrations
- Generating alerts on a variety of potential exploitations ranging from data exfiltration to data manipulation and suspicious attempts on these sensitive API endpoints
- Applying protection through web application and API protection policies targeting a variety of API attacks collected in attack groups
- Detecting APIs connected to Model Context Protocol (MCP) servers to identify shadow integrations and ensure safe AI agent adoption

Final thoughts

Organizations and their security vendors must work closely together, aligning across people, processes, and technologies to institute a solid defense against the security threats outlined in the **OWASP Top 10 API Security Risks**.

At a time when internal AI initiatives and AI-powered attacks threaten enterprises across multiple vectors, Akamai's web application and API security solutions will help secure your organization against the most advanced forms of web application, DDoS, and API-based attacks. Additionally, Akamai **Managed Security Service** provides 24/7 monitoring, security management, and threat mitigation.

Learn about **Akamai API Security**

Learn about **Akamai App & API Protector**



Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more about Akamai's cloud computing, security, and content delivery solutions at **akamai.com** and **akamai.com/blog**, or follow Akamai Technologies on **X** and **LinkedIn**. Published 06/26.