AKAMAI CHECKLIST

OWASP Top 10 API Security

APIs have become the standard for building and connecting modern applications, especially with the increasing move to microservices-based architectures. This is why it is important to protect your organization from the most common API security risks identified by the Open Worldwide Application Security Project (OWASP). Let's review the current 2023 list so you can be better informed on your journey to secure your APIs.

OWASP API Top 10 coverage by Akamai

- **API1:2023 — Broken Object Level Authorization:** BOLA vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs.
- **API2:2023 — Broken Authentication:** BA refers to broad vulnerabilities in the authentication process, exposing the system to attackers that can exploit these weaknesses to compromise API object protection.
- **API3:2023 — 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.
- **API4:2023 — Unrestricted Resource Consumption:** This is a type of vulnerability, sometimes called API resource exhaustion, where APIs do not limit the number of requests or the volume of data they serve within a given time.
- **API5:2023 — Broken Function Level Authorization:** BFLA can occur when access control models for API endpoints are incorrectly implemented.
- **API6:2023 — Unrestricted Access to Sensitive Business Flows:** This risk arises when an API exposes critical operations like business logic without sufficient access control.
- **API7:2023 — 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.
- **API8:2023 — Security Misconfiguration:** This refers to the improper setup of security controls, which can leave a system vulnerable to attacks.
- **API9:2023 — Improper Inventory Management:** This is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including deprecated, legacy, and/or outdated APIs — may be left unpatched and vulnerable to attack.
- **API10:2023 — Unsafe Consumption of APIs:** This refers to the risks associated with the use of third-party APIs without putting proper security measures in place.

Want to learn more about the difference between the 2019 and 2023 OWASP Top 10 API Security Risks list? Check out this blog post.

Work with us

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

About Akamai

Akamai provides industry-leading security solutions, highly experienced experts, and Akamai Connected Cloud, which gleans insight from millions of web application attacks, billions of bot requests, and trillions of API requests every single day. Akamai's web application and API security solutions will help secure your organization against the most advanced forms of web application, distributed denial-of-service (DDoS), and API-based attacks.

 | Support | Published 08/23