AKAMAI-CHECKLISTE

OWASP Top 10 API-Sicherheit

APIs haben sich zum Standard bei Aufbau und Verbindung moderner Anwendungen entwickelt, insbesondere angesichts des zunehmenden Umstiegs auf Microservices-Architekturen. Aus diesem Grund ist es wichtig, Ihr Unternehmen vor den häufigsten API-Sicherheitsrisiken zu schützen, die durch das Open Worldwide Application Security Project (OWASP) ermittelt wurden. Werfen Sie einen Blick auf die aktuelle Liste für 2023, um besser über Methoden zum Schutz Ihrer APIs informiert zu sein.

Abdeckung der OWASP API Top 10 durch Akamai

- ☑ **API1:2023 – Fehlerhafte Autorisierung auf Objektebene:** Sicherheitslücken durch fehlerhafte Autorisierung auf Objektebene (Broken Object Level Authorization – BOLA) entstehen, wenn die Autorisierung eines Clients nicht ordnungsgemäß für den Zugriff auf spezifische Objekt-IDs validiert wird.
- ☑ **API2:2023 – Fehlerhafte Authentifizierung:** Fehlerhafte Authentifizierung bezieht sich auf weitreichende Sicherheitslücken im Authentifizierungsprozess, durch die das System Angreifern ausgesetzt ist. Diese können Schwachstellen ausnutzen, um den API-Objektschutz zu gefährden.
- ☑ **API3:2023 – Fehlerhafte Autorisierung auf Objekteigenschaftsebene:** Fehlerhafte Autorisierung auf Objekteigenschaftsebene (Broken Object Property Level Authorization – BOPLA) ist ein Sicherheitsfehler, bei dem ein API-Endpunkt unnötig mehr Dateneigenschaften offenlegt, als für seine Funktion erforderlich ist, und so das Prinzip der geringstmöglichen Berechtigungen vernachlässigt wird.
- ☑ **API4:2023 – Uneingeschränkte Ressourcennutzung:** Sicherheitslücken dieser Art werden manchmal als API-Ressourcenüberlastung bezeichnet. Dabei werden die Anzahl der Anforderungen oder das Datenvolumen, das die API innerhalb eines bestimmten Zeitraums bearbeiten kann, durch die APIs nicht begrenzt.
- ☑ **API5:2023 – Fehlerhafte Autorisierung auf Funktionsebene:** Fehlerhafte Autorisierung auf Funktionsebene (Broken Function Level Authorization – BFLA) kann auftreten, wenn Zugriffskontrollmodelle für API-Endpunkte falsch implementiert sind.
- ☑ **API6:2023 – Unbeschränkter Zugriff auf sensible Geschäftsabläufe:** Dieses Risiko entsteht, wenn eine API kritische Vorgänge wie Geschäftslogik ohne ausreichende Zugriffskontrolle offenlegt.
- ☑ **API7:2023 – Serverseitig manipulierte Anforderungen:** Serverseitig manipulierte Anforderungen (Server Side Request Forgery – SSRF) ermöglichen es einem Angreifer, die serverseitige Anwendung dazu zu veranlassen, HTTPS-Anfragen an eine beliebige Domain seiner Wahl zu senden.
- ☑ **API8:2023 – Fehlerhafte Sicherheitskonfiguration:** Dies bezieht sich auf die unsachgemäße Einrichtung von Sicherheitskontrollen, die ein System anfällig für Angriffe machen kann.
- ☑ **API9:2023 – Fehlerhafte Bestandsverwaltung:** Dies stellt für jedes Unternehmen, das APIs verwaltet, eine Herausforderung dar. API-Sicherheitslösungen können bekannte APIs schützen. Unbekannte und auch veraltete APIs sind aber möglicherweise nicht gepatcht und daher anfällig für Angriffe.
- ☑ **API10:2023 — Unsichere Nutzung von APIs:** Dies bezieht sich auf die Risiken, die mit der Verwendung von Drittanbieter-APIs verbunden sind, wenn keine angemessenen Sicherheitsmaßnahmen ergriffen werden.

Möchten Sie mehr über den Unterschied zwischen den OWASP-Listen über die wichtigsten 10 API-Sicherheitsrisiken für die Jahre 2019 und 2023 erfahren? Lesen Sie diesen Blogbeitrag.

Zusammenarbeit mit uns

Unternehmen und ihre Sicherheitsanbieter müssen eng zusammenarbeiten und Menschen, Prozesse und Technologien zusammenbringen, um effektiven Schutz vor den in den OWASP API Security Top 10 beschriebenen Sicherheitsrisiken zu gewährleisten.

Über Akamai

Akamai bietet branchenführende Sicherheitslösungen, erfahrene Experten und die Akamai sConnected Cloud mit Einblicken in Millionen von Webanwendungsangriffen, Milliarden von Bot-Anfragen und Billionen von API-Anfragen pro Tag. Die Sicherheitslösungen für Webanwendungen und APIs von Akamai schützen Ihr Unternehmen vor den fortschrittlichsten Formen von Webanwendungs-, DDoS- (Distributed Denial of Service) und API-basierten Angriffen.

 | Support | Veröffentlicht: 08/23