

API Security - Why now?

Business urgency to secure APIs

Is your new microservice exposed to public internet?

Public exposure drastically increases the chances of a data breach, DDoS attacks, account takeover, unauthorized data manipulation, malware infiltration, and API abuse.

Do you perform authentication regression tests pre-release?

Failing to perform auth regression tests pre-release can lead to compromised user accounts, unauthorized transactions and data leaks.

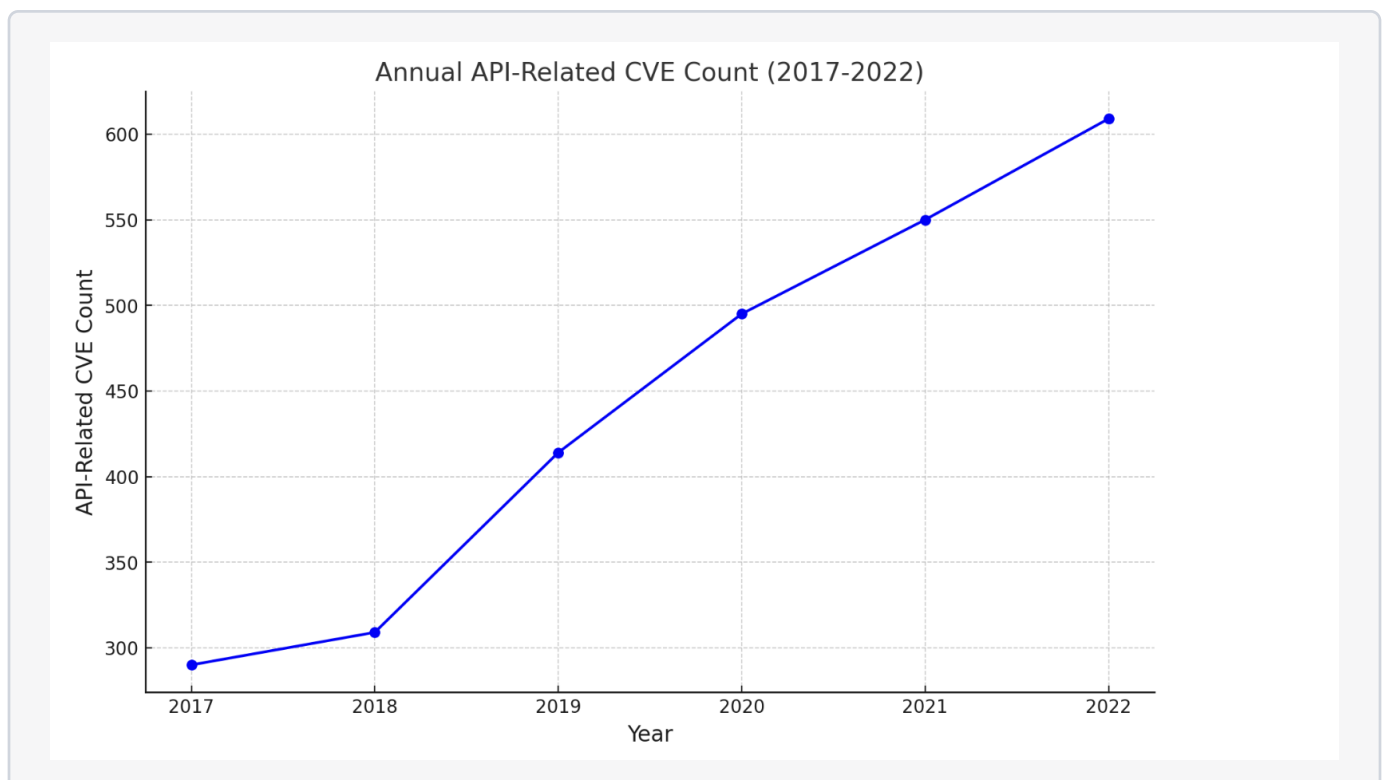
Is your microservice leaking sensitive data?

Are you inadvertently exposing sensitive data like SSNs or credit card information in your microservice responses? Is your microservice handling customer data securely?

Can a member access Admin exclusive APIs?

Have you thoroughly checked for privilege escalation issues in your system? Improper access control ranks among the most critical OWASP Top 10 vulnerabilities.

Rising API Vulnerabilities [CVEs]



Business Cost of API breaches

- The cost of rectifying an API breach averages \$4.5 million for enterprises.
- 30% of startups delay product launches due to API security concerns.
- API breaches can lead to system downtimes. This translates to a potential revenue loss of \$5,600 per minute, based on industry averages.
- A single API breach can lead to a 20% reduction in customer base within a month.

Recent Breaches

Date	Company	Industry	Details of the breach
Jan 2023	T-Mobile	Telecommunications	Impacted around 37 million customers, data accessed by hackers.
Jan 2023	PayPal	Finance	Unauthorized access to customer accounts using stolen credentials.
Jan 2023	Twitter	Social Media	Data of 200 million users sold on dark web.
Sep 2022	North Face	Retail	Compromised 200,000 accounts in a credential stuffing attack.
Oct 2023	LinkedIn	Social Media	2 million records Leaked
Oct 2023	23andMe	Pharmaceuticals	Leaked large amounts of user data due to brute force attack

API Security and Compliance

API Security is crucial for compliance like FedRAMP, GDPR and HIPAA. Neglecting it risks severe fines and data breaches. Prioritize robust security measures and regular audits to ensure compliance and protect sensitive data.

Top 3 API CVEs in last 5 years

1. [Broken Access Control](#): Allows unauthorized access to API functions and data due to insufficient user restrictions.
2. [SSRF](#): Enables attackers to make unauthorized requests to internal systems via the API.
3. [Broken Authentication](#): Permits identity theft or unauthorized access due to flawed authentication processes.

How Akto can help?

1. API Discovery

Akto automatically discovers and monitors APIs in real-time across various formats. Akto detects all API misconfigurations and categorizes APIs according to their risk scores.

API inventory			
30 days	Total APIs 1333 ↓ 21	Critical 1333 ↓ 21	Tested 80%
All	Groups	Hostname	Custom +
<input type="checkbox"/>	Group ↓	Total endpoints	Risk score
<input type="checkbox"/>	REST Endpoints	50	4.9
<input type="checkbox"/>	Js files	100	4.8
<input type="checkbox"/>	png files	400	4.7
<input type="checkbox"/>	PII Only	30	4.5
<input type="checkbox"/>	Newly Discovered	493	4.5
<input type="checkbox"/>	High Risk	22	4.5
<input type="checkbox"/>	Auth detected	33	4.3

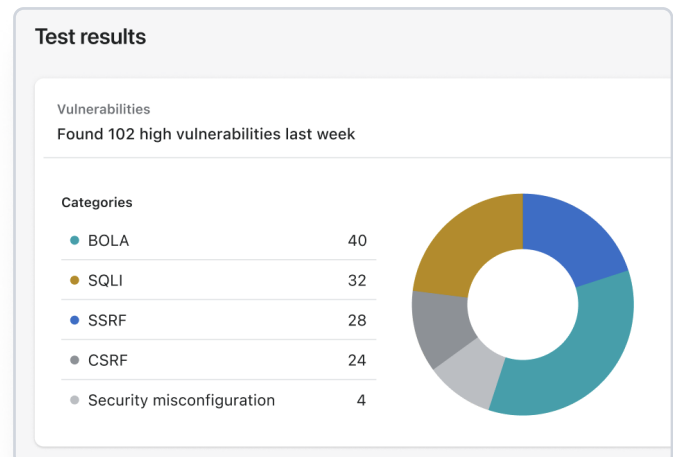
2. Sensitive Data Exposure

Akto's platform can identify sensitive parameters through API request and response. Our comprehensive database encompasses over 100 types of sensitive data, such as email addresses, phone numbers, Social Security numbers, and credit card information.

3. API Security Testing in CI/CD

Akto covers all aspects of the latest OWASP Top 10 ensuring complete coverage. We are particularly distinguished for our advanced test suites focusing on broken authentication and authorization.

Akto covers all aspects of the latest OWASP Top 10 ensuring complete coverage. We are particularly distinguished for our advanced test suites focusing on **broken authentication and authorization**.



Superpower - The Largest API Security Test Library

1. Akto's dedicated security team is committed to ensuring the highest standards of API security. Our team regularly updates our extensive Test Library ensuring the most current and comprehensive coverage.
2. Our platform boasts a robust collection of over 200 test cases.
3. Akto also provides the flexibility to select from these pre-existing templates or to create custom templates tailored to specific organizational needs

How to get started? [Schedule a demo](#)

Protect your APIs today from attacks with Akto's proactive answer to API Security. See for yourself with a free trial. Select from the options below.

[Start with Cloud version](#) | [Deploy self-hosted](#) | [Try Open Source](#) | [Schedule a demo](#)