OWASP API Security Top 10 (2023).

The OWASP API Security Top 10 is a list of the ten biggest security risks for APIs. OWASP (the Open Worldwide Application Security Project) is the non-profit that maintains it, and most security teams treat it as the starting checklist. The 2023 version moved the access-control risks to the top, because that is where real-world breaches happen most, and it added two new ones: APIs that let callers use too many resources, and APIs that blindly trust the other APIs they call.

HOW IT WORKS

01 What are the ten risks in the 2023 list?

- API1:2023 Broken Object Level Authorization (BOLA): a request reaches data the caller is not allowed to see. The most common API flaw. SL7 explainer.
- API2:2023 Broken Authentication: the API gets the 'who is calling' check wrong. SL7 explainer.
- API3:2023 Broken Object Property Level Authorization: the caller can see the object but also sees or changes fields they should not.
- API4:2023 Unrestricted Resource Consumption: the API lets callers run costly operations with no limit.
- API5:2023 Broken Function Level Authorization: a normal user can reach admin-only endpoints.
- API6:2023 Unrestricted Access to Sensitive Business Flows: a flow like buying, transferring, or signing up accepts more requests than the business can absorb.
- API7:2023 Server Side Request Forgery: the API fetches a web address the attacker picked. The same flaw as web SSRF.
- API8:2023 Security Misconfiguration: default passwords, chatty error messages, missing security headers, debug endpoints left on in production.
- API9:2023 Improper Inventory Management-: forgotten API versions, undocumented endpoints, test environments left public.
- API10:2023 Unsafe Consumption of APIs: the API trusts the other APIs it calls, and gets hit when one of them is compromised.

SOURCES

[1] OWASP API Security Top 10 (2023)

[2] OWASP API Security Project

[3] OWASP Top 10 (2021)

[4] MITRE ATT&CK for Enterprise

02 What changed between the 2019 and 2023 lists?

The big shifts:

- Access control moved to the top. Broken Object Level Authorization is now API1, ahead of authentication. This matches what breaches show: login is usually present and roughly right, but access checks are where mistakes pile up.
- New: Unrestricted Access to Sensitive Business Flows (API6). Not the same as a missing rate limit. This is for flows, like buying, transferring, or signing up, that need more than rate limits to protect.
- New: Unsafe Consumption of APIs (API10). APIs lean on other APIs more and more. If the API you call is compromised, or sends back attacker-controlled data, your trust in it backfires.
- Object access and property access split apart. API3, Broken Object Property Level Authorization, is now its own entry. Same root cause as API1, different fix.

03 How does SecureLayer7 use this list?

As a coverage map, not a tick-box list. Every engagement starts with one question: which of these ten apply to this API? An internal admin API has a different scope than a public consumer API. A read-only API can often skip API6.

For each category in scope, we run a set of payloads and requests aimed at the real endpoints, then hand-build follow-up attacks wherever one half-works. The report shows per-category coverage, so an auditor can see which API risks were checked.

04 How does this relate to the regular OWASP Top 10?

They work together. Modern apps need both. The classic OWASP Top 10 (the 2021 edition) covers issues that hit web apps and APIs alike: injection, broken access control, weak cryptography. The OWASP API Security Top 10 covers the issues that are more common or more damaging on APIs. Most engagements use both lists to set scope.

Map your API to the OWASP API Top 10.

securelayer7.net/learn/api-security/owasp-api-top-10

Open online