What is BOLA?

BOLA stands for Broken Object Level Authorization. It is the API security flaw where the endpoint identifies which resource to operate on by an ID supplied in the request, but does not verify the calling user is authorized to access that resource. Changing the ID returns somebody else's data. BOLA tops the OWASP API Security Top 10:2023 because it is the highest-frequency, highest-impact flaw class in modern API breaches. Functionally identical to IDOR on traditional web applications; the API context tends to make the impact much larger.

HOW IT WORKS

01 How is BOLA different from IDOR?

Same root cause, different naming convention.

IDOR (Insecure Direct Object Reference) is the older term, from the classic OWASP Top 10 for web applications. BOLA is the API-specific name used in the OWASP API Security Top 10.

The difference matters in practice for two reasons. First, scope: an IDOR pentest covers the web pages; a BOLA pentest covers every API endpoint that loads an object by ID. Modern applications have many more API endpoints than web pages, which makes BOLA testing the bigger job. Second, impact: BOLA on a list endpoint that returns paginated results often exposes the whole dataset in one script. The blast radius of a BOLA is typically larger than the blast radius of an equivalent IDOR. See our IDOR explainer for the broader vulnerability class.

02 What do attackers do with BOLA?

Real exploit patterns from API engagements:

- Scrape the entire dataset. Walk the ID space (sequential integers, UUIDs leaked through other endpoints, IDs returned in list responses) and pull every object.
- Modify other users' data. PUT or PATCH endpoints with the same flaw let the attacker update somebody else's records.
- Targeted account takeover. BOLA on a password-reset or email-change endpoint lets an attacker take over a specific known account.

HOW TO DEFEND

- Centralize the check. A single authorization layer that runs on every API request and decides 'is this caller allowed to act on this resource in this way' is dramatically easier to audit than per-endpoint checks scattered across the codebase.
- Make the check explicit in the data layer. Queries that load an object should require the owner (or appropriate scope) as a parameter, not check the result after the fact. `SELECT * FROM invoices WHERE id = ? AND organization_id = ?` is much harder to forget than checking ownership afterwards.
- Test cross-tenant on every endpoint. Automated tests that try a wrong-tenant request on every endpoint catch regressions early. Most teams discover that several endpoints they assumed were safe are not.
- Treat unpredictable IDs as defense in depth. UUIDs reduce the cost of leaked IDs but do not replace authorization checks.

SOURCES

[1] OWASP API1:2023 Broken Object Level Authorization

[2] OWASP API Security Top 10 (2023)

[3] CWE-639 Authorization Bypass Through User-Controlled Key

- Cross-tenant data leakage. Multi-tenant APIs that forget to scope queries by tenant ID return data from other tenants. One of the most damaging BOLA outcomes for B2B SaaS.
- Mass exfiltration. Scripted enumeration over an indexed endpoint pulls millions of records in minutes.

03 How does SecureLayer7 test for BOLA?

Every API engagement runs BOLA testing across the entire authenticated surface.

- Map the object model. What are the resources (users, invoices, files, organizations, projects)? Which endpoints read, write, or list them?
- Test cross-account access. For each endpoint, fire the same request with another account's resource ID. Document everything that returns data, mutates, or even confirms existence in a way that aids enumeration.
- Test cross-tenant access. For multi-tenant APIs, the same test across tenant boundaries. This is often where the biggest findings are.
- Test indirect references. A user might not be allowed to access invoice 4287 directly, but a search endpoint that filters by ID might leak its existence. Test the indirect paths too.

Deliverable maps findings to OWASP API1:2023 with the specific code change required.

Find BOLA before someone enumerates your dataset.
securelayer7.net/learn/api-security/bola

Open online