wib

OWASP API1:

Broken object-level authorization (BOLA)

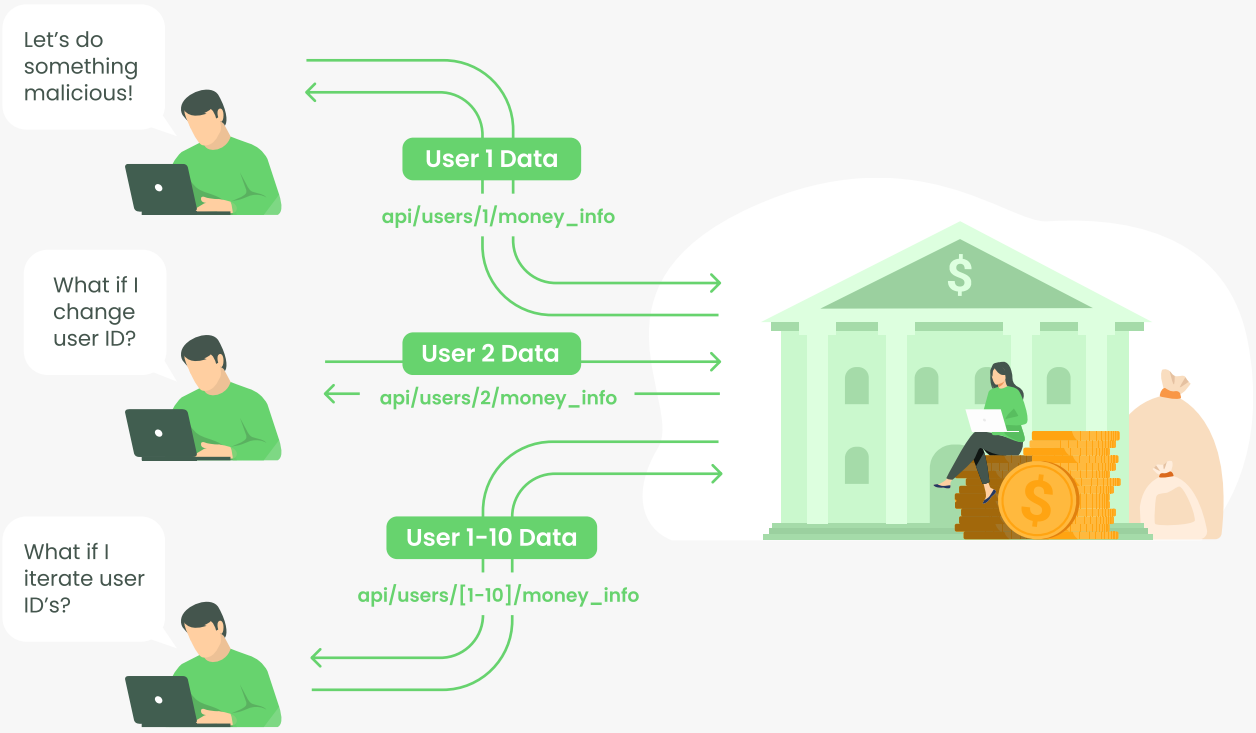
OWASP top 10

BOLA is the first threat in the OWASP API Security Top 10. It is the most common and impactful attack on APIs.

Object-level authorization is a security mechanism that ensures users can only access objects to which they have permission. A situation where one user has access to the data of another user is known as “broken object-level authorization.”

How Hackers Exploit It

To further understand this threat, we can imagine a typical bank API use case: account data access.



1. The attacker (user1) logs into their bank account to retrieve financial details (user1_data).
2. Then, they try another user id (user2) in that same request.
3. Instead of blocking his request, the bank returns the data information (user2_data).
4. The second request reveals a BOLA vulnerability. That means they can now automate this process and successfully request the data of many users by iterating through their user IDs.

Why You Should Care

When an application contains a BOLA vulnerability, it has a high chance of exposing sensitive data or other personal information to attackers. BOLA vulnerabilities, if identified, can be extremely easy to exploit, often utilizing a simple script.

It takes minimal effort to take advantage of this vulnerability. Attackers only need to replace the ID of their own resource in the API call with the ID of another user's resource. As a result, attackers can access the specified site by exploiting insufficient authorization checks.

This problem is frequent in API-based programs since the server component does not completely track the client's state, relying instead on object IDs given from the client to decide which item to access.

BOLA can lead to unauthorized data exfiltration, viewing, modification, or destruction. Furthermore, attackers can typically leverage these vulnerabilities to take over user or admin accounts if this assault occurs on a critical service, such as password reset or password change.

Traditional Tools Will Not Protect You

Many businesses still use security tools such as API gateways, Web Application Firewalls (WAFs), and other traditional outmoded protection methods. However, as threats become more complicated and sophisticated, these tools miss attacks that target the logic of APIs.

- **API Gateways**: API management tools that collect all user requests and turn them into one. The gateway becomes the entry point for every new request. However, these secure only known APIs, while many APIs could be outside the gateway.

- **WAFs:** Many solutions in this category rely solely on traditional application security methods. This category uses signatures to look for known attack patterns, but signatures are ineffective since each API is different and has its own set of vulnerabilities. These proxy-based solutions lack the architecture required to comprehend API context and, as a result, are unable to handle unique logic or identify attackers who are targeting specific vulnerabilities.

OWASP API Security Top 10 threats	WAFs	API Gateways	wib
Broken object Level Authorization	✗	✗	✓
Broken authentication	✗	!	✓
Excessive Data Exposure	✗	✗	✓
Lack of Resources & Rate Limiting	✗	!	✓
Broken Function Level Athorization	✗	!	✓
Mass Assignment	✗	✗	✓
Security Misconfiguration	!	✗	✓
Injection	✓	✓	✓
Improper Assets Management	✗	!	✓
Insufficent Logging & Monitoring	!	!	✓

How To Combat BOLA Threats

You must do three things to protect your APIs from BOLA threats:

1. In any function that uses a client input to access a database record, use an authorization mechanism to check if the logged-in user has permission to do the desired action on the record
2. Use GUIDs for record IDs that are arbitrary and unpredictable
3. Test your APIs

With the extensive use of APIs in modern applications, an AI-powered system that understands the logic of APIs can be your best line of defense for detecting when an authenticated user is trying to obtain unauthorized access to another user's data.
Furthermore, to best protect your product from a BOLA threat, you must consider a comprehensive solution that will address this kind of threat at the root—detecting it at the development stage, testing it at the testing stage, and ensuring it does not happen in production.

How Wib Can Help You

Wib is a full-lifecycle API security platform, defending against API security threats. The platform ensures comprehensive protection across the entire API software lifecycle from development to testing to production.

Wib utilizes state-of-the-art proprietary AI and ML to analyze millions of requests in real-time. It provides complete visibility of existing APIs, with actionable insights and comprehensive protection across the entire lifecycle. It learns your APIs inside and out and can provide complete visibility of your existing APIs, analyze their integrity, identify vulnerabilities, and detect attacks in real-time.

If you are building or using APIs in your applications (and you probably are), **sign up for a demo to see Wib in action and learn more.**