wib

OWASP API4:

Lack of Resources and Rate-Limiting

OWASP top 10

API requests use network, CPU, memory, and storage resources. APIs usually have no restrictions on the amount or number of resources a specific client/user can request. Instead, the API architecture supports a certain amount of usage for each user group.

An API client can make thousands or even millions of API calls per second or request hundreds or thousands of data records simultaneously, and the server will still try to proceed with them.

How Hackers Exploit It

Imagine a website with an employee table with a maximum of 5 users per page.

Employeeid	Departmentid	FirstName	LastName	Address1	Address2	City	State	Country	PostalCode
1	1	Tom	Hanks	1st Street	Columbia Ave	Los Angeles	CA	US	123456
2	2	Bruce	Willis	2nd Street	Farmers Ave	Seattle	wA	US	123456
3	2	Johnny	Depp	5th Street	Shuttle Ave	Los San Antonio	TX	US	123456
4	1	Christian	Bale	8th Street	SpaceX Ave	Chicago	IL	US	123456
5	1	Heath	Ledger	7th Street	Discovery Ave	Los Angeles	CA	US	123456

The following query retrieves the list of employees from the server: /api/employees?page=1&size=5

If a hacker changes the size argument to 100, database performance issues may occur. As a result, the application could slow down or crash, becoming unable to handle queries (DoS attack). Any legitimate actions that rely on personnel data will suffer.

Why You Should Care

n the case of a lack of resources, attackers can jam the API by sending more requests than it can handle or by sending requests at a rate that exceeds the API's processing speed. When a single client or a group of clients makes too many requests at once, the requests overwhelm the server's ability to handle them. These queries can grind an API to a halt, slowing service and, in some instances, resulting in a Denial of Service (DoS). The lack of rate-limiting also can enable malicious attackers to brute-force passwords by attempting to find them with massive numbers of API requests.

Due to a lack of rate-limiting, brute-force attacks against authentication endpoints and endpoints with Broken Object Level Authorization might also occur. For example, suppose there is no restriction on how many times a user can log in. In that case, hostile attackers can brute-force users' passwords by attempting to log in using massive numbers of API requests with different passwords until they succeed.

Traditional Tools Will Not Protect You

Traditional security tools like WAFs and API Gateways recommend basic or static rate restriction, but they have no idea what constitutes "typical" API usage. As threats become more complicated and sophisticated, these tools miss attacks that target the logic of APIs.

It is challenging to protect modern complex microservice applications without understanding API context. Unfortunately, WAFs and API gateways lack the context needed to inform security teams what a typical value for an API parameter should be. Therefore, they miss assaults where an attacker manipulates a single API parameter value to overwhelm an application.

How to Combat Lack of Resources and Rate-Limiting Threats

You must do four things to protect your APIs from lack of resources and rate-limiting threats:

1. Set a restriction on how many times a client can call the API in a certain period of time
2. Notify the client when the limit has been reached by providing the limit number as well as the time when the limit will be reset
3. Add adequate server-side validation to query string and request body parameters, particularly those controlling the number of records that a response will return
4. Define and enforce maximum data size limits for all incoming parameters and payloads, such as string length limits and array size limits

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.