OWASP API Security Project

Main | Acknowledgments | Join | News | RoadMap | Translations

Check out the new OWASP API Security Top 10 2023 !

What is API Security?

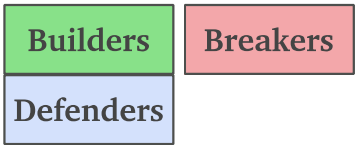
A foundational element of innovation in today's app-driven world is the API. From banks, retail and transportation to IoT, autonomous vehicles and smart cities, APIs are a critical part of modern mobile, SaaS and web applications and can be found in customer-facing, partner-facing and internal applications. By nature, APIs expose application logic and sensitive data such as Personally Identifiable Information (PII) and because of this have increasingly become a target for attackers. Without secure APIs, rapid innovation would be impossible.

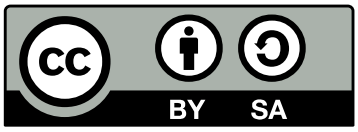
API Security focuses on strategies and solutions to understand and mitigate the unique vulnerabilities and security risks of Application Programming Interfaces (APIs).

API Security Top 10 2023

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

API Security Information





Here is a sneak peek of the 2023 version:

- **API1:2023 - Broken Object Level Authorization**

  APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface of Object Level Access Control issues. Object level authorization checks should be considered in every function that accesses a data source using an ID from the user. Continue reading.

- **API2:2023 - Broken Authentication**

  Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising a system's ability to identify the client/user, compromises API security overall. Continue reading.

- **API3:2023 - Broken Object Property Level Authorization**

  This category combines API3:2019 Excessive Data Exposure and API6:2019 - Mass Assignment, focusing on the root cause: the lack of or improper authorization validation at the object property level. This leads to information exposure or manipulation by unauthorized parties. Continue reading.

- **API4:2023 - Unrestricted Resource Consumption**

  Satisfying API requests requires resources such as network bandwidth, CPU, memory, and storage. Other resources such as emails/SMS/phone calls or biometrics validation

Downloads or Social Links

API Security Top 10 2023
API Security Top 10 2019 (PDF)
GraphQL Cheat Sheet
GitHub Discussions
Mailing List

Code Repository

GitHub

Leaders

Erez Yalon
Inon Shkedy
Paulo Silva

Upcoming OWASP Global Events

OWASP Global AppSec Singapore 2023

- October 4-5, 2023

OWASP Global AppSec Washington DC 2023

- October 30 - November 3, 2023

OWASP Global AppSec San Francisco 2024

- September 23-27, 2024

OWASP Global AppSec Washington DC 2025

- November 3-7, 2025

are made available by service providers via API integrations, and paid for per request. Successful attacks can lead to Denial of Service or an increase of operational costs. Continue reading.

- **API5:2023 - Broken Function Level Authorization**

  Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers can gain access to other users' resources and/or administrative functions. Continue reading.

- **API6:2023 - Unrestricted Access to Sensitive Business Flows**

  APIs vulnerable to this risk expose a business flow - such as buying a ticket, or posting a comment - without compensating for how the functionality could harm the business if used excessively in an automated manner. This doesn't necessarily come from implementation bugs. Continue reading.

- **API7:2023 - Server Side Request Forgery**

  Server-Side Request Forgery (SSRF) flaws can occur when an API is fetching a remote resource without validating the user-supplied URI. This enables an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall or a VPN. Continue reading.

- **API8:2023 - Security Misconfiguration**

OWASP Global AppSec San Francisco 2026

- November 2-6, 2026

APIs and the systems supporting them typically contain complex configurations, meant to make the APIs more customizable. Software and DevOps engineers can miss these configurations, or don't follow security best practices when it comes to configuration, opening the door for different types of attacks. Continue reading.

- **API9:2023 - Improper Inventory Management**

  APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. A proper inventory of hosts and deployed API versions also are important to mitigate issues such as deprecated API versions and exposed debug endpoints. Continue reading.

- **API10:2023 - Unsafe Consumption of APIs**

  Developers tend to trust data received from third-party APIs more than user input, and so tend to adopt weaker security standards. In order to compromise APIs, attackers go after integrated third-party services instead of trying to compromise the target API directly. Continue reading.

Licensing

The OWASP API Security Project documents are free to use!

alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

Edit on GitHub

Spotlight: Corellium

CORELLIUM

Corellium helps developer and security teams build, test, and secure mobile devices and apps through the power of virtualization. Our Arm-native virtualization platform is used by businesses, agencies and security communities around the world to strengthen security testing and streamline DevSecOps. With highly performant, scalable, and accurate virtual devices, Corellium dramatically accelerates mobile R&D and enables never-before-possible security research and penetration testing. Visit Corellium.com for a free trial.

Corporate Supporters

mercari

epam

intruder

salesforce

Qualys.

GUARDSQUARE
Mobile application protection

Checkmarx

Contrast
SECURITY

COALFIRE

Become a corporate supporter