OWASP TOP 10 API 2023

Broken Object Level Authorisation

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

Broken Object Level Authorisation

APIs often unveil endpoints responsible for object IDs, significantly increasing the risk of Object Level Access Control vulnerabilities.

In every function that retrieves data using a user-supplied ID, object level authorisation should be rigorously applied.

Broken Authentication

SENCODE
CYBER SECURITY

Broken Authentication

SENCODE
CYBER SECURITY

Frequent misconfigurations in authentication mechanisms enable attackers to seize authentication tokens or abuse flaws to impersonate other users.

Such compromises degrade the overall security posture of the API.

Broken Object Property Level Authorisation

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

Broken Object Property Level Authorisation

This type merges two issues: API3:2019 Excessive Data Exposure and API6:2019 - Mass Assignment.

Both originate from insufficient or incorrect authorisation validations at the object property level, which could lead to data leaks or unauthorised data manipulation.

Unrestricted Resource Consumption

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

Unrestricted Resource Consumption

Fulfilling API requests draws on various resources like network bandwidth and CPU.

Additionally, certain external services are utilised via API integrations, incurring costs per request. Poor security can result in Denial of Service attacks or increased operational costs.

Broken Function Level Authorisation

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

Broken Function Level Authorisation

Complex access control structures, incorporating various layers and unclear distinctions between administrative and standard functions, often result in authorisation vulnerabilities.

These vulnerabilities can allow attackers to access resources or admin functionalities.

Unrestricted Access to Sensitive Business Flows

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

Unrestricted Access to Sensitive Business Flows

APIs exposed to this risk reveal key business functionalities, like ticket purchasing, without adequate controls. This vulnerability can cause business harm and isn't necessarily the result of coding errors.

Server-Side Request Forgery (SSRF)

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

Server-Side Request Forgery (SSRF)

SSRF vulnerabilities may arise when an API fetches external resources without sufficient URI validation. This can allow attackers to compel the API into sending requests to unintended destinations, even if firewalls or VPNs are in place.

Security Misconfiguration

SENCODE
CYBER SECURITY

Security Misconfiguration

SENCODE
CYBER SECURITY

APIs and their supporting systems often contain intricate configurations, intended for customisation. Overlooked or incorrectly applied security configurations can open avenues for multiple forms of attacks.

Improper Inventory Management

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

Improper Inventory Management

APIs frequently expose a greater number of endpoints than traditional web applications. Consequently, keeping an up-to-date inventory of hosts and API versions is vital for mitigating risks such as exposed debug endpoints and deprecated APIs.

Unsafe Consumption of APIs

SENCODE
CYBER SECURITY

Unsafe Consumption of APIs

SENCODE
CYBER SECURITY

Developers often place undue trust in data sourced from third-party APIs, adopting lesser security standards. To breach an API, attackers might focus on these third-party integrations rather than the primary API.

WORRIED ABOUT YOUR API?

CONTACT US

Email: office@sencode.co.uk

Phone: 01642 716680

Website: sencode.co.uk


SENCODE
CYBER SECURITY
SECURITY BEYOND COMPLIANCE