API security, in concrete terms.

API security is the practice of keeping the application programming interfaces behind modern products from being abused by attackers. APIs differ from classic web applications in three ways: every endpoint is independently authorized, the responses are structured data that scripts can scrape easily, and a single misconfigured endpoint often exposes orders of magnitude more data than a single misconfigured web page.

HOW IT WORKS

01 Topics

- OWASP API Security Top 10 (2023): Every Risk Explained: the ten biggest API risks, with the access-control risks at the top.
- What is BOLA (Broken Object Level Authorization)?: the most common API flaw, reaching data that is not yours. The API version of IDOR.
- What is Broken Authentication in APIs?: token, session, and password failures that turn an API into an open door.
- What is GraphQL Penetration Testing?: GraphQL adds its own attacks (introspection, batching, deep queries) that REST does not have.
- API Rate Limit Bypass: Techniques and Defenses: when the wall against scraping and password-guessing turns out to have a side door.

SOURCES

[1] OWASP API Security Top 10 (2023)

[2] OWASP API Security Project

[3] MITRE ATT&CK for Enterprise

Scope an API penetration test.
securelayer7.net/learn/api-security

Open online