

API(Application Programming Interfaces)

What Are APIs (Application Programming Interfaces)

An API is a set of rules that allow software applications to communicate with each other.

Simple Explanation:

Think of an API like a waiter in a restaurant. You (the user) tell the waiter (API) what you want (data or action), and they go to the kitchen (the server) and bring it back to you.

Examples:

Google Maps + Uber: Google talks to Uber's system via API to show ride options.

Venmo: Talks to your bank (like Wells Fargo) through secure APIs to transfer money.

Kayak: Uses APIs to pull flight prices from different airlines in real-time.

Definition: API Security Fundamentals

The foundational course API Security Fundamentals teaches the fundamentals of protecting Application Programming Interfaces (APIs). It describes typical threats, how attackers take advantage of APIs.

examples of actual breaches, and how to protect APIs using industry best practices.

What does API security mean?

API security is the process of defending Application Programming Interfaces (APIs) against attacks, abuse, and unauthorized access.

In Simple Language:

APIs are digital messengers that facilitate communication between various software applications. To ensure that only authorized users can access the messenger and that no one is intercepting or altering the message, API security is similar to installing cameras and locking the doors.

Example:

An API is used by a mobile banking app to check your balance. Your account data could be compromised by a hacker if that API isn't secure.

Where are APIs used?

Mobile apps (banking, shopping, social media)


Websites (login, payment)

IoT devices (smart home tech)

Business systems (CRM, ERP integrations)

Cloud services (AWS, Azure APIs).

The Perfect API Storm: Why APIs Are Under Threat

 API traffic accounts for 83% of all internet traffic.

APIs are used in websites, mobile apps, and smart devices.

The #1 Attack Vector is APIs

API-based attacks are the biggest cybersecurity threat, as Gartner predicted and now confirms.

Just 4% Pay Attention to API Security

Just 4% of teams test APIs for security, according to a RapidAPI survey; the majority merely check to see if they "work."

What Makes APIs So Appealing to Attackers?

1. They are everything's backdoors.

Apps can access databases, transaction systems, and private information through APIs.

Attackers can easily enter if APIs are improperly configured or lack adequate controls.

2. They're Easy to Discover

No hacking expertise is required to view API calls like `fetchFlights()` with complete payloads or examine browser traffic using developer tools.

3. The UI is Secure—APIs Aren't

What users can see and do is restricted by the user interface (UI).

However, attackers can circumvent all UI controls by using custom requests to directly target APIs.

4. They're Often Over-Privileged

A lot of APIs return excessive amounts of data or permit functionality that isn't visible in the user interface but can still be accessed through API calls.

5. The Attack Chain for the API Is Easy

Conventional cyberattacks necessitate intricate procedures (lateral movement, privilege escalation, recon).

Finding a flaw in an API and sending a malicious request results in an immediate data breach.

Regulators Are Paying Attention

Real Breaches:

T-Mobile: An API made 37 million records available.

Verizon (TracFone) was fined \$16 million for leaking API data.

Important Laws That Address APIs:

PCI-DSS 4.0: Demands that APIs be tested for security vulnerabilities, including logical

errors.

APIs must protect personal data under the GDPR and CCPA.

HIPAA: Protected Health Information (PHI) must be secured by APIs.

Public companies are required by SEC regulations to disclose API risks.

UN Requires Cars: Connected cars must have API security.

FedRAMP: Monthly scans for API vulnerabilities for cloud providers used by the US government.

3 Drivers of Regulation:

Security: APIs need to be developed and used in a secure manner.

Privacy: APIs need to safeguard user and client information.

Accessibility: Data portability requires APIs, but they must do so securely.