



GETTING STARTED WITH API SECURITY TESTING: FROM BASICS TO PRACTICAL ATTACKS

ABOUT CYBERWARFARE LABS



CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform



INFINITE LEARNING EXPERIENCE

About Speaker

Abhijeet Kumar (Security Researcher)

His research areas include Red Team Operations, Network Security, Cloud infrastructure, and Linux Systems. Apart from this, he enjoys researching Adversarial TTPs and experimenting in his homelab during his free time.



API 101

BASICS OF API

- ★ An **Application Programming Interface** a.k.a. **API** is a set of protocols that allows different software systems to communicate and share data with each other.



TYPICAL API ARCHITECTURE

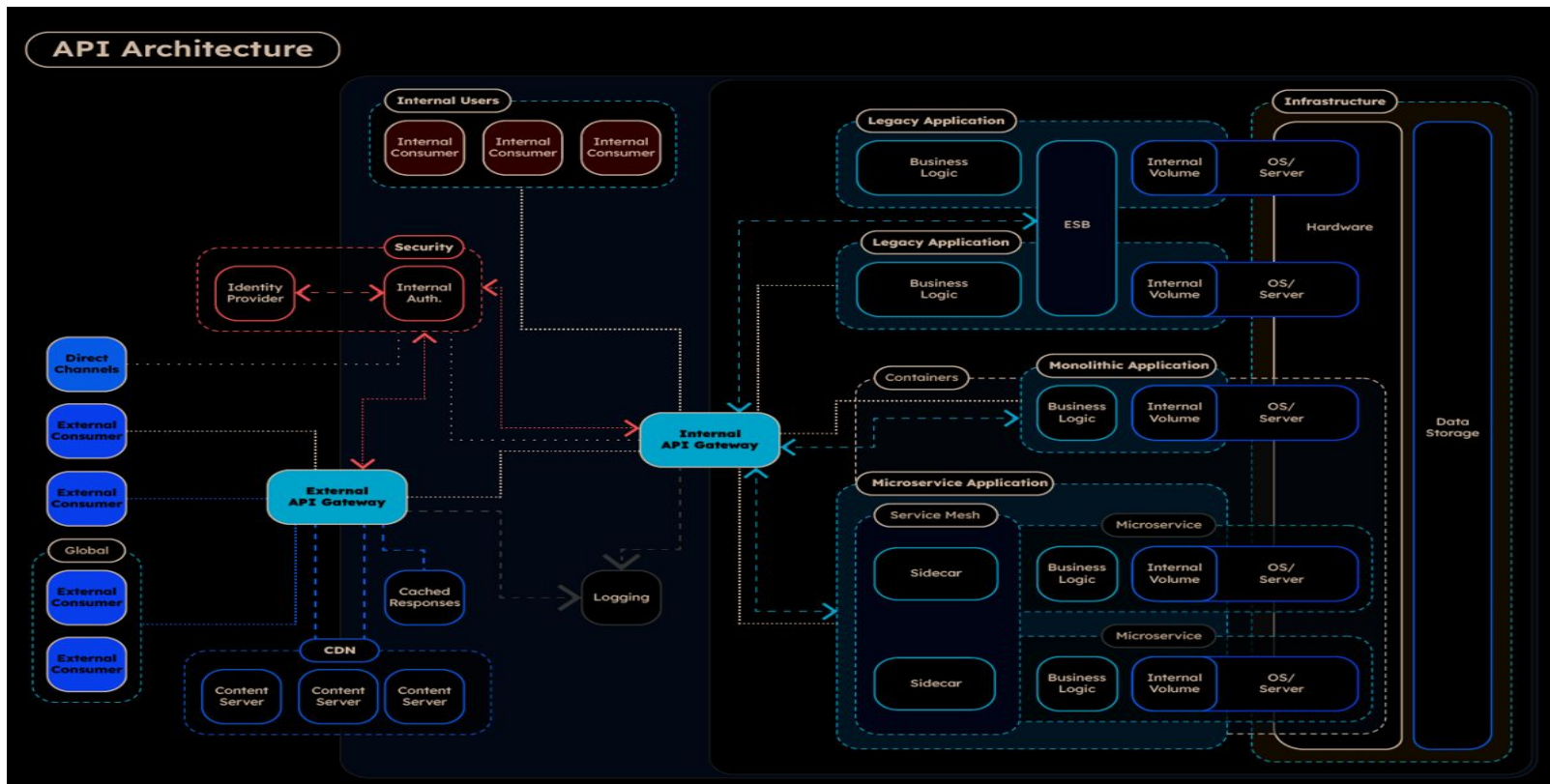
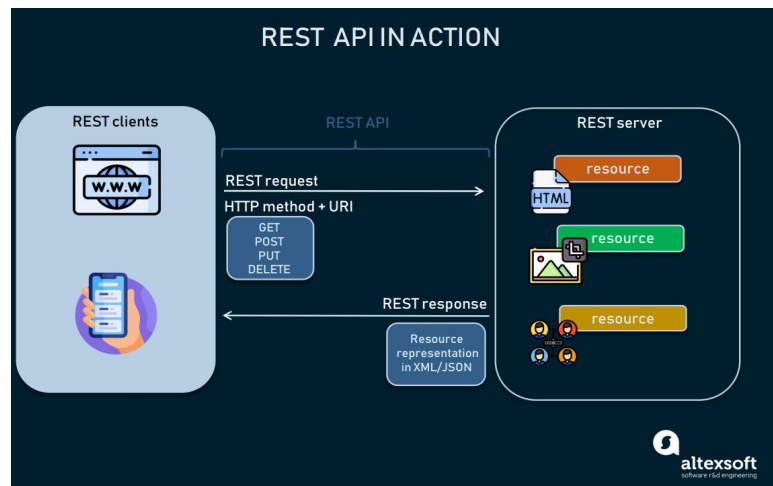


Fig. Enterprise API Architecture

★ REST (REpresentational State Transfer) API :-

- Flexible, resource-based HTTP API.
- Supports standard HTTP VERBS including GET, POST, PUT, and DELETE.

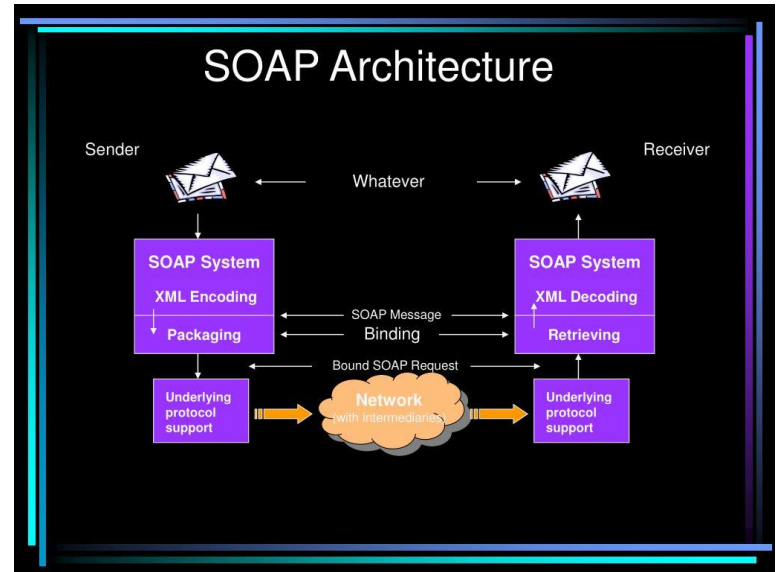


Source: [AltexSoft](#)

API PROTOCOLS

★ SOAP (Simple Object Access Protocol) API :-

- XML-based, strict schema validation focused API.
- Supports multiple protocols, including HTTP, SMTP, and TCP.



Source: [SlideServe](#)

API SECURITY RISKS

- ★ Poor or missing AuthN/AuthZ lets attackers access protected endpoints or impersonate users.
- ★ Unvalidated inputs can cause injection attacks, and improper data handling can expose sensitive data through APIs.



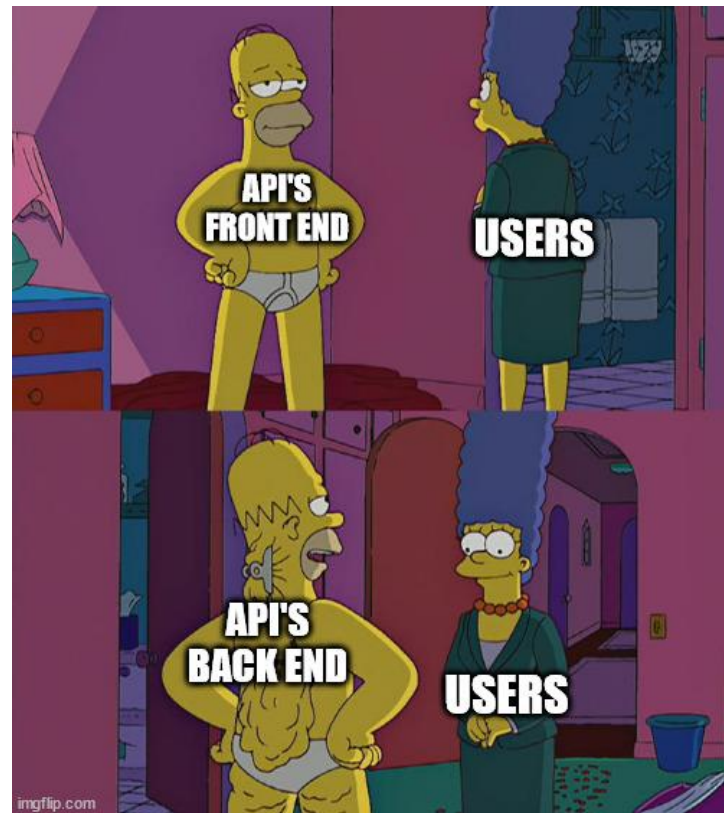
INTRODUCTION TO OWASP TOP 10

- ★ A list of [Top 10](#) most exploited vulnerabilities released by [Open Web Application Security Project \(OWASP\)](#).
- ★ Top 10 lists include Web Apps, API, LLM and CI/CD.
- ★ Release cycle is every 4 years.
- ★ Data is collected from the industry vendors & cybersecurity community.

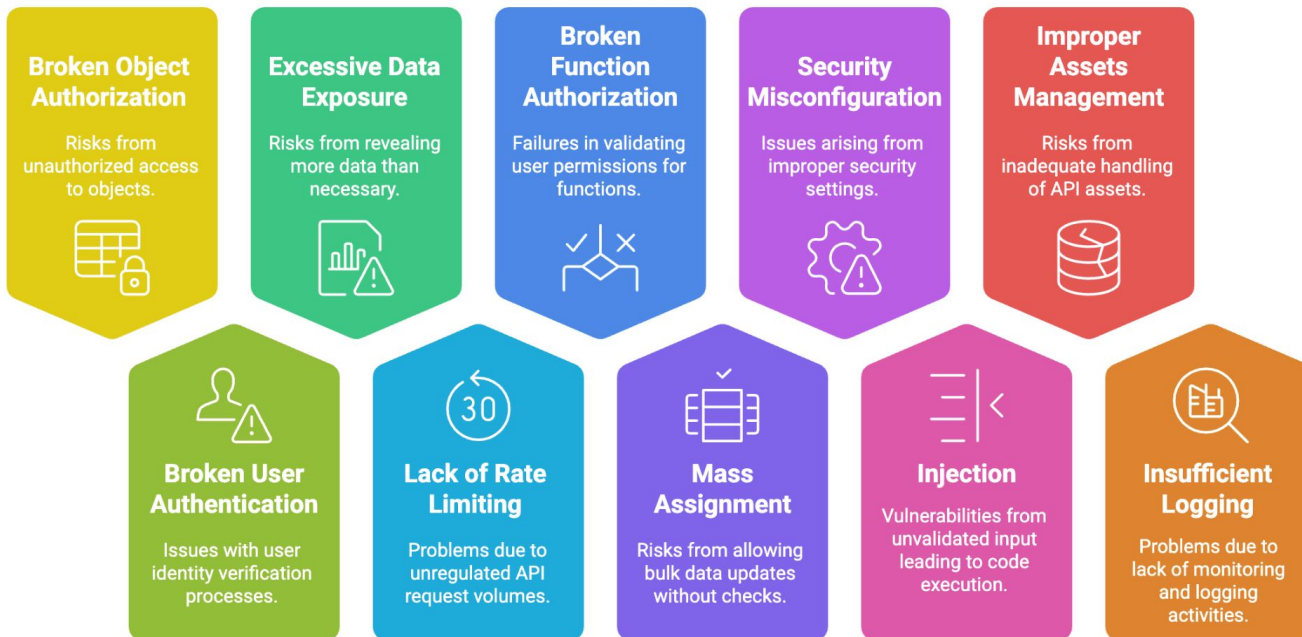


OWASP API SECURITY TOP 10

- ★ OWASP published its last [API Security Top 10](#) list back in 2023.
- ★ List contains some of the most common exploitation vectors used for compromising API during that list compilation period.



OWASP API SECURITY TOP 10



Source: [EdgeOne](#)

OWASP API SECURITY TOP 10



OWASP API Security Top 10 -2019


- 1 Broken Object Level Authorization
- 2 Broken User Authentication
- 3 Excessive Data Exposure
- 4 Lack of Resources & Rate Limiting
- 5 Broken Function Level Authorization
- 6 Mass Assignment
- 7 Security Misconfiguration
- 8 Injection
- 9 Improper Assets Management
- 10 Insufficient Logging & Monitoring

OWASP API Security Top 10 – 2023

- 1 Broken Object Level Authorization
- 2 Broken Authentication
- 3 Broken Object Property Level Authorization
- 4 Unrestricted Resource Consumption
- 5 Broken Function Level Authorization
- 6 Unrestricted Access to Sensitive Business Flows
- 7 Server Side Request Forgery
- 8 Security Misconfiguration
- 9 Improper Inventory Management
- 10 Unsafe Consumption of APIs

Source: [Wattlecorp](https://wattlecorp.com/owasp-api-security-top-10-2023)

RECONNAISSANCE

reconnaissance /rĭ-kŏn'ə-səns, -zəns/ 

noun

1. An inspection or exploration of an area, especially one made to gather military information.
2. An examination or survey of a region in reference to its general geological character.

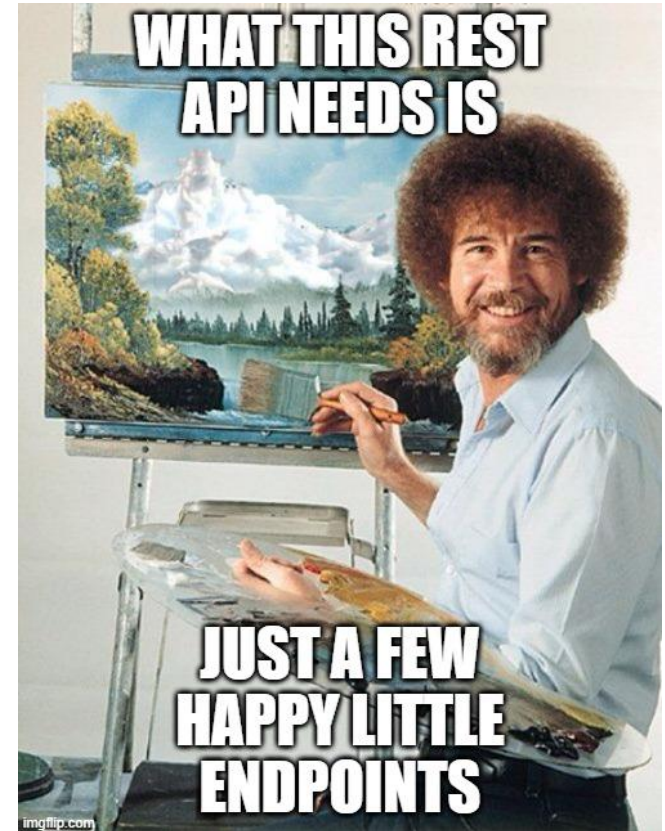
CRAWLING

- ★ Crawling is the automated collection of web pages to map a site's structure.
- ★ Juicy places :-
 - Directories
 - Sitemap file
 - Robots.txt



FUZZING

- ★ Fuzzing is automated testing with unexpected inputs to find flaws.
- ★ Juicy places :-
 - URL/Query Parameters
 - Endpoint Patterns
 - Cookies/Session IDs



API DOCUMENTATION

- ★ Explains how APIs can be used by other programs.
- ★ Provides simple instructions and examples for interaction.
- ★ Clarifies rules, access, and expected responses.



INTRODUCTION TO BURP SUITE

- ★ Burp Suite is a set of web application testing tools developed by PortSwigger.
- ★ Core tools include :-
 - Proxy, Repeater, Intruder, Scanner, Collaborator, Extender.



INTRODUCTION TO POSTMAN

- ★ Postman is a tool used for building, testing, and managing APIs.
- ★ It supports REST, SOAP, GraphQL, among other protocols.
- ★ Provides tools for inspecting HTTP responses.



Source: [Specbee](#)

INTRODUCTION TO FFUF

- ★ FFUF stands for Fuzz Faster U Fool.
- ★ Designed for fast discovery of hidden resources.
- ★ High-speed directory and file fuzzing using wordlists.
- ★ Support for fuzzing parameters, headers, POST data.



INTRODUCTION TO NUCLEI

- ★ [Nuclei](#) is a fast, community-driven vulnerability scanner that uses YAML-based DSL.
- ★ It was originally developed by [ProjectDiscovery](#).
- ★ It detects issues across applications, APIs, networks, DNS, and cloud.





Demo time

I'm not nervous...



Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

support@cyberwarfare.live

To know more about our offerings, please visit: **<https://cyberwarfare.live>**