Que es un API

API son las siglas en inglés para «application programming interface» o interfaz de programación de aplicaciones.

Verbos

Get	Request data - Can be Cached - Remains in the browser history - Can be bookmarked - Length restrictions - Calling it multiple times has side effects
Post	Send data - Never cached - No length restrictions
Put	Update data(resource) - Id based - Calling it multiple times has same result - Updates whole item/resource
Patch	Partial Update - Only updates what is given of resource
Delete	Deletes item/resource
Head	Request Header - Similar to Get - Only gets header not data - Useful before downloading a large file

API Testing - Prev

Que endpoint están disponibles?

Que resultado se considera positivo?

Que resultado se considera negativo?

Que resultado se considera un error?

Tipos de API Testing

Validacion	Validaciones genericas
Funcional	Confirma que el api hace lo que requiere
Carga	Capacidad de llamadas
Fiabilidad	Confiabilidad y buena coneccion
Securidad	Valida la autorizacion
Penetracion	
Fuzz	

Autentificación y Autorización

Autentifi-cación	el **proceso o acción de verificar** la identidad de un usuario o proceso.
Autorización	La autorización es una función que **especifica los privilegios de acceso** del usuario a los recursos de tu servicio.

Metodos de Autentificación

Básica	Nombre de usuario y una contraseña;
Token	Token basado en usuario y contraseña
Clave API	Usa claves generadas por el sistema; Private y Public Key
OAuth 2.0	Access Tokens **Autorización abierta**

Autenticación Basica

Se realiza mediante el encabezado HTTP Authorization.
Cualquiera que intercepte la trasmisión de datos puede decodificar fácilmente esta información.
Esto se denomina ataque Man-In-The-Middle **(MiTM).**
Para proteger tu API mediante la autentificación básica debe ser únicamente mediante una conexión **TLS/HTTPS**

Autenticación por Token

El servidor guarda en base de datos este registro y lo devuelve al usuario para que a partir de ese momento no envíe más credenciales de inicio de sesión en cada petición HTTP.
En lugar de las credenciales, simplemente se debe enviar el token codificado en cada petición HTTP.

Autenticación Clave API

Este sistema es más seguro que los métodos anteriores, pero **la generación de credenciales debe ser manual y esto dificulta la escalabilidad de tu API.**
La automatización de generación e intercambio de key's es una de las razones principales por las que se desarrolló el método de autentificación **OAuth.**

Autenticación OAuth

Utiliza **tokens de acceso**. Un token de acceso es un dato que representa la autorización para acceder a los recursos en nombre del usuario final.
OAuth 2.0 no define un formato específico para los tokens de acceso. Sin embargo, en algunos contextos, a menudo se usa el formato **JSON Web Token (JWT)**.
Esto permite a los emisores de tokens incluir datos en el propio token.
Además, por razones de seguridad, los tokens de acceso pueden tener una **fecha de vencimiento**.