Conexión y consumo de APIs

Sesión Conceptual 2

{desafío} latam_


Inicio
Desarrollo
Cierre
Objetivo de la sesión
Activación de conceptos clave
Conceptualización
Ejercicios
Quiz
Cierre

Inicio

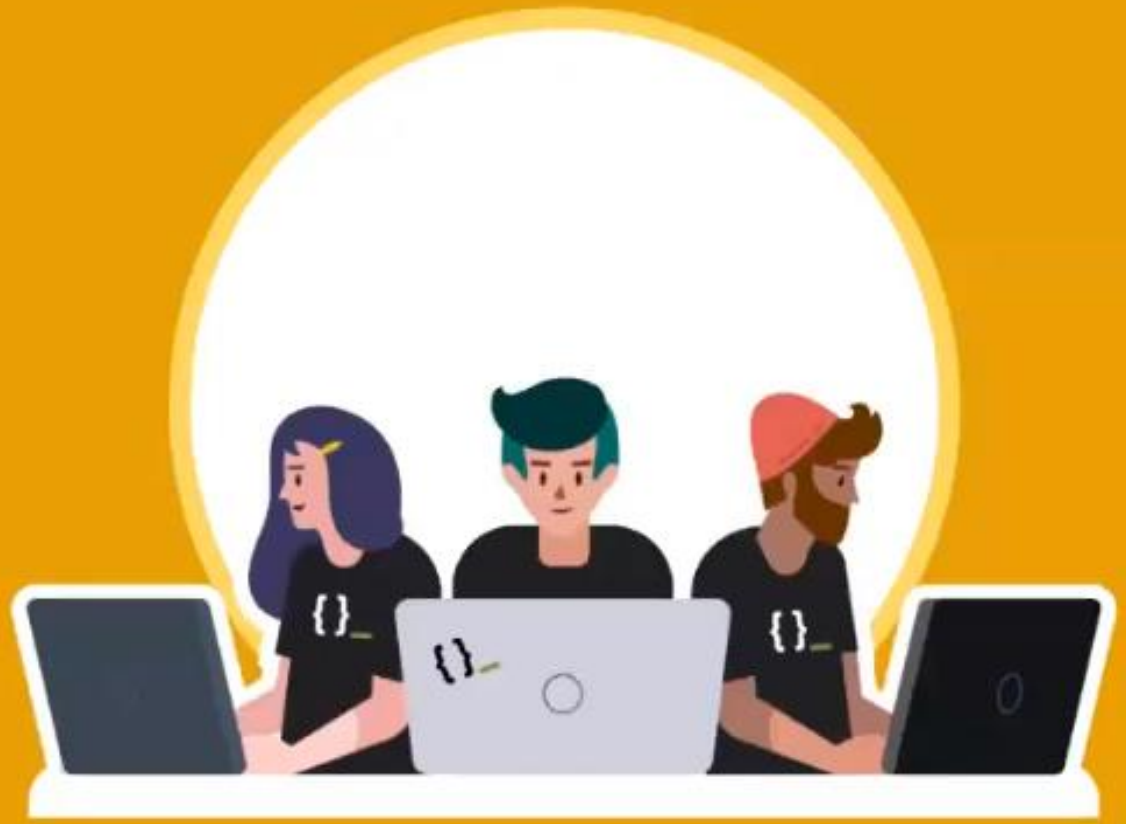
10 minutos

{desafío} latam_

¿Qué aprenderás?

- Reconocer la salida de una API y la transformación para implementarla dentro de su aplicación.
- Combinar los conocimientos de los módulos previos con información extraída mediante API para agregar versatilidad y robustez a sus aplicaciones.

{desafío} latam_



Desarrollo

70 minutos

{desafío}
latam_

/* Seguridad en las API */

{desafío}
latam_

API (application programming interface)

Interactuar con una API implica interactuar con datos ya sean estos públicos o de carácter sensible, acceso controlado. Por ello mencionaremos algunos ejemplos de seguridad con el cual, eventualmente, podríamos encontrarnos al momento de trabajar con APIs.

Entender distintas formas de seguridad nos puede ayudar a tratar con el cuidado necesario los datos extraídos de este tipo de APIs.

Encriptación SSL

SSL es un acrónimo de Secure Sockets Layer, una capa de seguridad que establece la encriptación entre el navegador y el servidor:

- Evita que la información que enviamos o recibimos sea leída por un tercero.
- Ya sea conectándonos a una página web por el navegador o a una API.

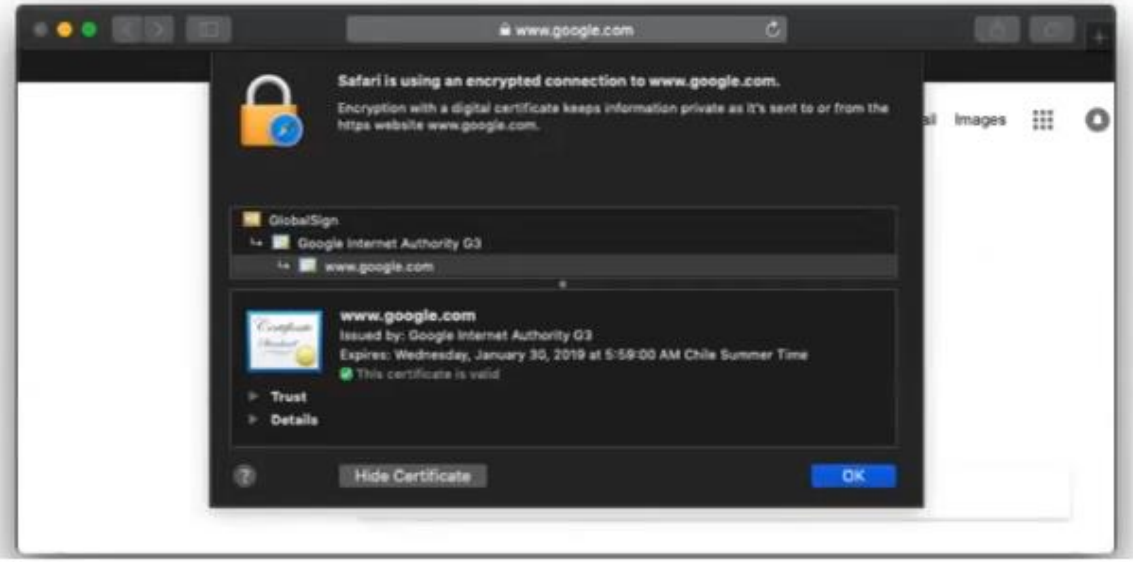
Para entender el funcionamiento de la encriptación, hay que tener presente que existen dos claves: una para cifrar y otra para descifrar. Explicaremos esto con un ejemplo.

Supongamos por un momento que la comunicación es entre dos personas, Alicia y Rob. Para cifrar el mensaje, Alicia tiene una clave y para descifrarlo, otra. Previo a comunicarse, Alicia se junta con Rob y le traspasa la clave para descifrar.

Conexión mediante SSL

Al conectarnos a un sitio que utiliza SSL con un navegador, se establece un acuerdo de forma automática, que es llamado en inglés handshake. En el que, el servidor envía un certificado que tiene el nombre del sitio y la clave pública al cliente.

El cliente ocupa la clave pública que viene en el certificado para cifrar un mensaje y se la devuelve al servidor. Si el servidor puede descifrar el nuevo mensaje significa que el servidor tiene la clave privada correcta.



Ventajas SSL

- Cifra el mensaje impidiendo que terceros puedan leerlo.
- Asegura que el emisor es quien dice ser, porque si alguien más cifró el mensaje con una llave destinada, el mensaje no tendrá sentido al descifrarlo.

Conectándose a SSL

- Postman identifica automáticamente si un request ocupa HTTPS y genera el código para conectarnos. La librería requests, por defecto, tiene la verificación de certificados SSL habilitada, por lo que si no puede verificar un certificado durante un request, ocurrirá un SSLError.

POSTMAN

Autenticación mediante TOKEN

Muchas APIs requieren de autenticación para poder acceder a sus servicios. Para autenticarse con una API, nuestro primer paso consiste en conseguir una clave para conectarse. Las mismas APIs disponen de servicio de registro, y al completarlo entregan un id. Esta clave recibe el nombre de TOKEN, el cual debe ser incluido dentro del llamado según las instrucciones entregadas en la documentación.

- Podemos agregar el token en la URL o en el HEADER para conectarnos a la API

Ejercicio guiado

"API Oxford Dictionary"

{desafío} latam_

Quiz

{desafío}
latam_

Cierre

10 minutos

{desafío} latam_

- ¿Qué es una API?
- ¿Qué es POSTMAN y para qué nos sirve?
- ¿Qué son los Métodos HTTP?
- ¿Cuántos Métodos HTTP existen y cuál es la utilidad de cada uno de ellos?
- ¿Para qué sirven los códigos de respuesta? ¿Cuáles son los más importantes de conocer?

{desafío} latam_

Academia de talentos digitales