

Desarrollo de Web Api's con .NET

Token y manejo de excepciones



UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

**Centro de
e-Learning**

Un poco de repaso...

- ¿Qué es Blazor y que no permite realizar esta tecnología?
- ¿Qué características o particularidades tiene una aplicación hecha en Blazor?
- ¿Qué ventajas nos ofrece? ¿Y qué desventajas?

¿Qué vamos a ver hoy?

- Autenticación basada en token
- Manejo de excepción y registro de errores
- Repaso



¿Qué es un
token?

¿Qué es un token?

Es un método de seguridad el cual una API nos provee para que podamos realizar operaciones.

El cliente le solicita un token a la API a la cual se va a conectar.

El cliente debe enviar este token en el encabezado de Autorización al realizar solicitudes a recursos protegidos.

Nos permite el acceso a un determinado recurso o URL (endpoint).

¿Qué es un token?

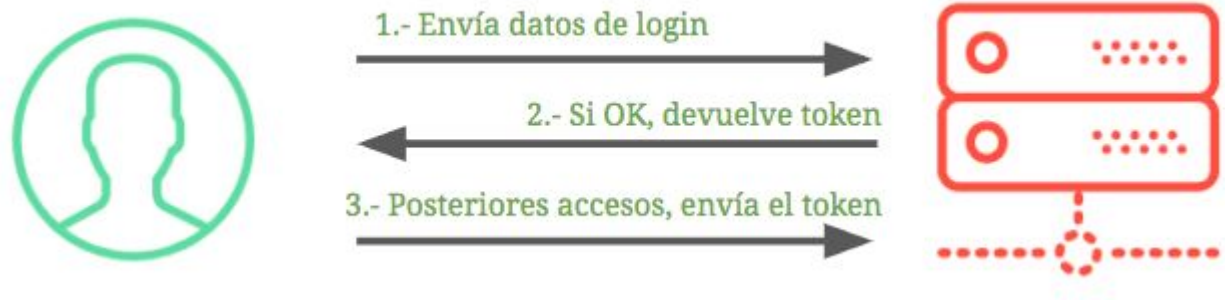
Como consecuencia de no tener estado y no tener sesiones en el servidor para cada usuario, el backend es incapaz de recordar al usuario entre llamada y llamada a la API.

Para evitar que en cada llamada el usuario deba entregar su clave y password se usa un token, que no es más que una cadena de texto bien larga, encriptada con una clave.

Según se hace el login, el servidor devuelve al cliente un token y el cliente en futuros accesos entrega ese token para certificar que está autenticado.

¿Cómo funciona la autenticación?

1. El cliente envía los datos de login a la API
2. La API entrega un token con cierta validez
3. El cliente almacena el token
4. El cliente envía el token en posteriores accesos
5. Cuando el token vence, el cliente debe solicitar uno nuevo a la API



Al iniciar el cliente...

Al arrancar la aplicación, el cliente debe asegurarse:

1. Si es correcto entonces está autenticado. Puede hacer llamados a la API.
2. Si no es válido, deberíamos borrarlo del almacenamiento local y mantener el estado de aplicación, mostrando que no está autenticado.
3. Si el cliente no tiene el token almacenado, entonces se entiende que no está autenticado y no necesitamos verificar nada. En este caso el estado de la aplicación debería demostrar que no se está logueado.

Validez del token

El token generalmente tiene un tiempo de validez, que se establece en el servidor, al momento de generar.

Durante el tiempo de validez del token, este podrá ser utilizado para autorizar el acceso a ciertos recursos por parte del cliente.

Cuando el token caduque, el servidor lo rechazará y el cliente no podrá acceder a aquella información u operación solicitada.

¡¡A trabajar!!

