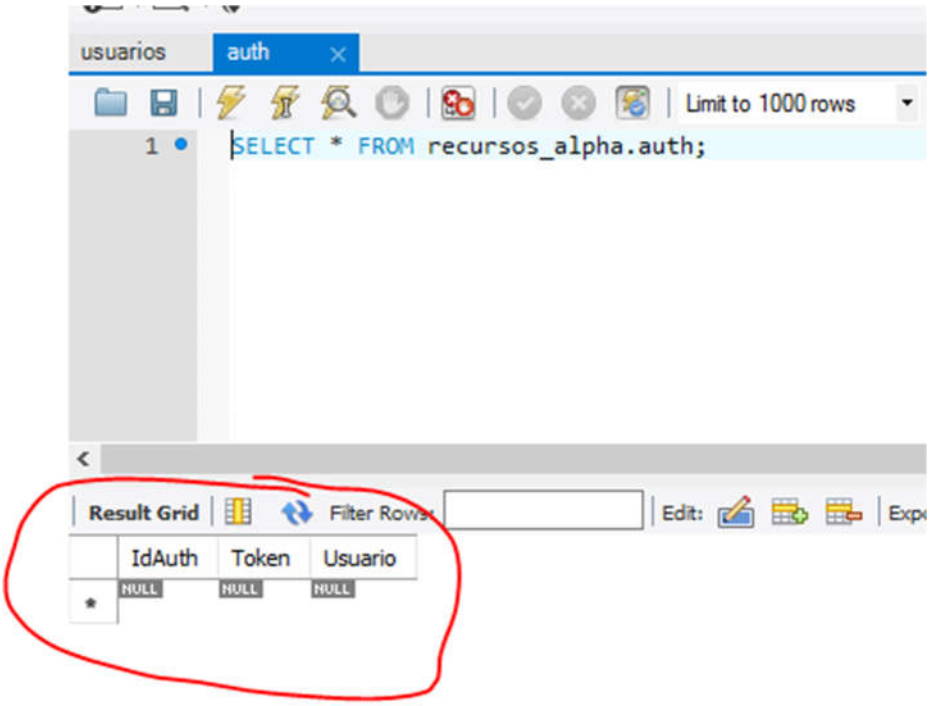
Tarea II – Servicios Web

El propósito en esta tarea es configurar un nuevo servicio web usando REST o SOAP, para la comunicación entre el cliente y el servidor.

Parecía que el sistema estaba usando una arquitectura cliente-servidor no estándar.., Es decir, que para iniciar la sesión en el lado del cliente, era necesario crear una base de datos local en el cliente, siendo otras tablas accedidas directamente en el servidor… Esto no parece ser correcto pues normalmente el servidor tiene que comprobar la validez del usuario para entregar los datos al mismo, pero en este caso el usuario no era validado por el servidor…
Con esto en mente, se ha implementado un sistema de autorización usando un servicio web que involucra la creación de "tokens", con los que se validan los usuarios registrados.

Se ha creado una nueva tabla en la base de datos llamada **Auth**, esta tabla tiene 3 columnas: **IdAuth, Token y Usuario**.



Para dar soporte a esta tabla se ha creado la clase POJO **Auth**. Esta clase contiene todas las funciones y siguientes métodos:

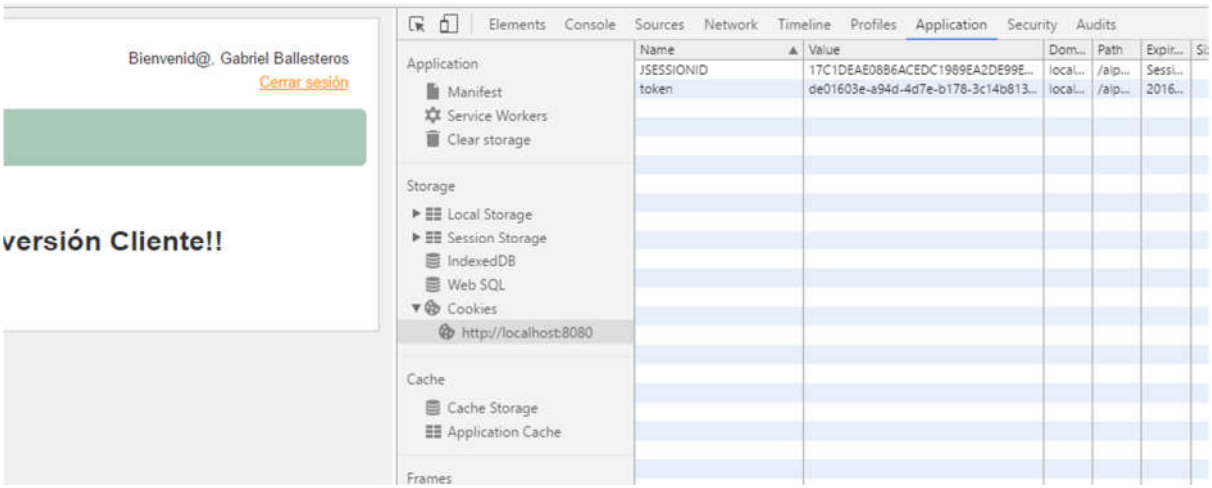
- **generateToken**: crea un nuevo token para el acceso.
- **getAuthByToken**: devuelve un objeto Auth, basado en un token.
- **save:** método que guarda el objeto Auth en la base de datos.

Han sido creados dos nuevos servicios web llamados **validaToken** y **accesoUsuario**.

El primer servicio web **validaToken** es accedido mediante la dirección URL /validaToken. El servidor recibe un token del cliente y devuelve un objeto **Auth** si el elemento es válido y devuelve “null” si no es válido.

El segundo servicio web **accesoUsuario,** es accedido mediante la dirección URL /accesoUsuario. El servidor recibe un nombre de usuario y la contraseña de la cuenta y se comprueba la validez de los datos en la base de datos. Si el nombre de usuario y la contraseña son correctos se crea un nuevo registro en la tabla **Auth** que contiene un nuevo token generado por nuestra clase **Auth** y enlaza este token con el usuario conectado.

Después de este proceso, se devuelve al cliente un objeto **Auth** y nuestro cliente guarda el token en las cookies del navegador, como se puede ver en la siguiente imagen.



Cada vez que el cliente necesita algo del servidor debe pasar el token al servidor utilizando el servicio /validaToken.

Ideas para el futuro

Es preciso corregir otros servicios web en el lado del cliente, ya que todavía no están funcionando. El único servicio que se ejecuta (funciona) es el del login.

Crear fecha y hora para el token. Invalidar token después de un tiempo determinado (fecha de caducidad).