Seguridad de servicios en **Plugcore**

Plug Soluciones TIC S.L.
info@plugcore.com


https://github.com/plugcore/plugcore


https://www.linkedin.com/company/plugcore


https://twitter.com/plugcoreit

Seguridad de servicios

1. **Introducción**
2. **Cómo securizar un servicio**
3. **Tipos de seguridad**
4. **Configuración**

Introducción

- Todo lo que vamos a comentar hoy está en el paquete @plugcore/web, con lo cual si no lo tenemos instalado lo vamos a necesitar.
- Siempre tenemos que pensar en la seguridad a la hora de realizar nuestras aplicaciones
- Sistema de seguridad más común para servicios REST: JWT
- Siempre podemos utilizar nuestro sistema de seguridad a medida

Cómo securizar un servicio

```
@Controller({ urlBase: '/posts' })
export class PostsController {
    @Get({
        // Simplemente tenemos que indicar en "security" que
        // tipo de seguridad queremos para este método
        security: 'jwt'
    })
    public async getAllPosts(request: Request, response: Response) {
        console.log(request.jwtPayload); // Ejemplo de JWT, si llegamos
                                         // a este punto es que ha pasado
                                         // el check de seguridad.
        return [];
    }
}
```

Tipos de seguridad

- Actualmente hay 3 tipos de seguridad implementados:
    - **JWT**: Ver más info en https://jwt.io/, pero básicamente es un token que debe ser informado en los headers de las peticiones, ese token contiene la información del usuario que está ejecutando la acción. El token se genera previamente en un servicio de login.
    - **Basic Auth**: Estándar de http, el usuario y contraseña se pasan como texto plano en un header, no recomendable dada la baja seguridad.
    - **Custom**: Siempre podemos implementar un sistema de seguridad a medida si no nos gusta ninguna de las opciones anteriores.

Configuración

- La configuración del sistema de seguridad se divide en 2 partes:
    - **Usando el sistema de configuration.json**: Aquí tendremos que indicar si queremos activar el sistema de seguridad y algunos aspectos de el.
    - **Clase de servicio**: En la cual implementaremos los métodos de login, para que podamos hacer una petición a la bbdd y comprobar que el usuario que está intentado hacer login en nuestro servicio es correcto.

configuration.json

```
{
    "web": {
        "auth": {
            "enabled": true, // Tenemos que activar la seguridad si queremos usarla en cualqueir ruta ya que por defecto está desactivada
            "securityInAllRoutes": ["jwt", "basic"], // Array que contiene un listado de seguridades a aplicar a todas las rutas,
            "securityInOas": ["basic"],
            "jwtPrivateKey": "8981F9391AF549443CC7D5141B24DJ4C",
            "jwtAlgorithm": "HS256", // Posibles valores "HS256" | "HS384" | "HS512" | "RS256", ver https://jwt.io/
            "jwtLoginPath": "/auth/jwt", // Url de login de JWT
            "jwtExpiration": 432000 // Tiempo de vida que se le da a cualquier token en segundos
        }
    }
}
```

Servicio de implementación

```
@Service()
export class RoutesAuthImplService {
    // Recibe un objeto request cuando se llame a la url de login de JWT (ver más
    // adelante) y tendrá que devolver el payload que se vaya a poner en el JWT de
    // salida, si hay cualquier problema hay que devolver null o lanzar una excepción
    // Ver https://github.com/plugcore/plugcore/wiki/API-Rest#seguridad
    @JwtLogin()
    public async jwtLogin(request: Request) {
        this.log.info('jwtLogin');
        if (request.body && request.body.user === 'testUser') {
            return {
                prop1: 'string1',
                prop2: 2
            };
        }
    }
}
```

GRACIAS POR SU TIEMPO

Para más información
info@plugcore.com
germanml@plugcore.com
sergiolc@plugcore.com

plugcore.com