Desarrollo web en Entorno Servidor

UT02-b Spring Boot

Proyecto – API REST Segura

Prof. Diego Linares Ortiz

UT02.b Proyecto
API REST Segura

Puesta en marcha

En este ejercicio práctico vas a realizar la implementación de una API REST segura donde aplicaremos todas las técnicas que hemos visto hasta ahora. **Es imprescindible que vayas paso a paso, para así asegurar que la aplicación se construye sobre unos cimientos sólidos y estables.**

Para empezar el proyecto deberás seguir una serie de pasos:

1- Plantea una idea de API REST, la cual deberás desarrollar. Esta idea de aplicación deberá tener unas tablas a las cuales se deberá acceder haciendo uso de la API.
2- Una vez tengas la idea, deberás plantear las tablas que vas a gestionar. Por ejemplo:
    a. Idea: Aplicación de gestión de reservas de viaje.
        i. Tabla 1: Usuarios
        ii. Tabla 2: Reservas
        iii. Tabla 3: Detalles_Reserva
    b. Idea: Aplicación de gestión de viajes en grupo
        i. Tabla 1: Usuarios
        ii. Tabla 2: Viajes
        iii. Tabla 3: Destinos
    c. Idea: Aplicación de reparto de tareas del hogar
        i. Tabla 1: Usuarios
        ii. Tabla 2: Tareas_Domesticas
        iii. Tabla 3: Asignaciones_Diarias
    d. Idea: Aplicación de reparación/tareas de mecánica a domicilio
        i. Tabla 1: Usuarios
        ii. Tabla 2: Talleres
        iii. Tabla 3: Citas_Taller
    e. Idea: Aplicación de planificador de presupuesto
        i. Tabla 1: Usuarios
        ii. Tabla 2: Tipos_Gastos
        iii. Tabla 3: Gastos_Diarios
3- Una vez tengas la idea y las tablas planteadas, deberás plantear todos los campos que las tablas deberán tener así como el tipo de dato y las restricciones que vas a aplicar.
4- Cuando hayas cumplido el punto 4, ya puedes pasar a realizar un diagrama de entidad-relación de las tablas.
5- Cuando hayas cumplido el punto 5, puedes pasar a crear el repositorio y demás especificaciones.

Objetivo

El objetivo del proyecto es que realices una API REST segura desde principio hasta el fin. Deberás terminar teniendo una API que cumplirá con los principios SOLID, segura, probada y bien documentada.

Enunciado

Construye e implementa una API REST segura siguiendo las siguientes restricciones:

1. Realiza los pasos explicados en la introducción del proyecto. Una vez realices esos pasos, puedes pasar al punto 2 del enunciado. NO SE CORREGIRÁ NINGÚN PROYECTO QUE NO HAYA ENTREGADO UN PLANTEAMIENTO PREVIO DEL MISMO
2. Crea un repositorio en GitHub, que sea público y que tenga al profesor como colaborador directo del repositorio. Crea un README.md donde plantees los siguientes puntos:
    a. Nombre del proyecto
    b. Idea del proyecto
    c. Justificación del proyecto
    d. Descripción detallada de las tablas que intervendrán en el proyecto
3. En el README anteriormente construido deberás incluir lo siguiente (aparte de lo ya descrito)
    a. Indicar los endpoints que se van a desarrollar para cada tabla
    b. Describir cada uno de los endpoints. Realiza una explicación sencilla de cada endpoint.
    c. Describe la lógica de negocio que va a contener tu aplicación.
    d. Describe las excepciones que vas a generar y los códigos de estado que vas a poner en todos los casos.
    e. Describe las restricciones de seguridad que vas a aplicar dentro de tu API REST
    SI FALTARA CUALQUIER PUNTO DE LOS ANTERIORMENTE DESCRITOS, EL PROYECTO SE DARÁ COMO INVÁLIDO
4. Realiza la implementación de la API siguiendo las directrices que has marcado en la parte de la documentación que ya has desarrollado. La aplicación deberá cumplir con los siguientes mínimos:
    a. Debe haber una entidad Usuario que:
        i. Tenga al menos los campos *username*, *password* y *roles*.
        ii. La password debe almacenarse “*hasheada*” en la BDD

    b. Debe haber al menos 2 entidades más además de la entidad Usuario, que:
        i. Tenga un CRUD mínimo implementado
        ii. Tenga diferentes restricciones de acceso a los endpoints asociados a dichas entidades.
    c. Debes implementar la seguridad de la aplicación haciendo uso de Spring Security y que cumpla:
        i. Que se usa un cifrado asimétrico por clave pública y privada para el control de acceso.
        ii. Que se usa JWT para el control de acceso.
        iii. Que hay variedad de restricciones de control de acceso a los endpoints (*lo mismo que el punto b.ii*)
5. Una vez realizada la implementación de la API, realiza pruebas del buen funcionamiento de la misma.
    a. Usa insomnia, swagger o postman para probar los diferentes endpoints de la API
    b. Plantea las pruebas que vas a realizar para comprobar el buen funcionamiento de la API implementada
    c. Documenta las pruebas realizadas para mostrar que la API ha cumplido con su funcionamiento.
6. Cuando finalices toda la implementación y las pruebas podrás concluir el proyecto incluyendo los siguientes puntos a la documentación:
    a. ¿Qué tecnologías has usado?
        i. Indica las dependencias que has incluido en tu proyecto.
        ii. Indica el software que has usado (IntelliJ, Insomnia, XAMPP, navegadores, etc)
        iii. Describe brevemente dichas tecnologías y su propósito dentro del proyecto
    b. ¿Qué es una API REST? ¿Cuáles son los principios de una API REST? ¿Dónde identificas dichos principios dentro de tu implementación?
    c. ¿Qué ventajas tiene realizar una separación de responsabilidades entre cliente y servidor?

Conclusión y entrega

Para concluir el proyecto, deberás realizar un documento en formato ***.pdf*** que contenga toda la documentación que se pide para el proyecto. Entrega también un enlace al repositorio de GitHub. Mucho cuidado con los commits, si hay muy pocos commits se investigará la validez del proyecto.

RAs y CEs evaluados

6. Desarrolla aplicaciones de acceso a almacenes de datos, aplicando medidas para mantener la seguridad y la integridad de la información.

a) Se han analizado las tecnologías que permiten el acceso mediante programación a la información disponible en almacenes de datos.

b) Se han creado aplicaciones que establezcan conexiones con bases de datos.

c) Se ha recuperado información almacenada en bases de datos.

d) Se ha publicado en aplicaciones Web la información recuperada.

e) Se han utilizado conjuntos de datos para almacenar la información.

f) Se han creado aplicaciones Web que permitan la actualización y la eliminación de información disponible en una base de datos.

g) Se han utilizado transacciones para mantener la consistencia de la información.

h) Se han probado y documentado las aplicaciones.

7. Desarrolla servicios Web analizando su funcionamiento e implantando la estructura de sus componentes.

a) Se han reconocido las características propias y el ámbito de aplicación de los servicios Web.

b) Se han reconocido las ventajas de utilizar servicios Web para proporcionar acceso a funcionalidades incorporadas a la lógica de negocio de una aplicación.

c) Se han identificado las tecnologías y los protocolos implicados en la publicación y utilización de servicios Web.

d) Se ha programado un servicio Web.

e) Se ha creado el documento de descripción del servicio Web.

f) Se ha verificado el funcionamiento del servicio Web.

g) Se ha consumido el servicio Web.

8. Genera páginas Web dinámicas analizando y utilizando tecnologías del servidor Web que añadan código al lenguaje de marcas.

a) Se han identificado las diferencias entre la ejecución de código en el servidor y en el cliente Web.

b) Se han reconocido las ventajas de unir ambas tecnologías en el proceso de desarrollo de programas.

c) Se han identificado las librerías y las tecnologías relacionadas con la generación por parte del servidor de páginas Web con guiones embebidos.

d) Se han utilizado estas tecnologías para generar páginas Web que incluyan interacción con el usuario en forma de advertencias y peticiones de confirmación.

e) Se han utilizado estas tecnologías, para generar páginas Web que incluyan verificación de formularios.

f) Se han utilizado estas tecnologías para generar páginas Web que incluyan modificación dinámica de su contenido y su estructura.

g) Se han aplicado estas tecnologías en la programación de aplicaciones Web.

9. Desarrolla aplicaciones Web híbridas seleccionando y utilizando librerías de código y repositorios heterogéneos de información.

a) Se han reconocido las ventajas que proporciona la reutilización de código y el aprovechamiento de información ya existente.

b) Se han identificado librerías de código y tecnologías aplicables en la creación de aplicaciones Web híbridas.

c) Se ha creado una aplicación Web que recupere y procese repositorios de información ya existentes.

d) Se han creado repositorios específicos a partir de información existente en Internet y en almacenes de información.

e) Se han utilizado librerías de código para incorporar funcionalidades específicas a una aplicación Web.

f) Se han programado servicios y aplicaciones Web utilizando como base información y código generados por terceros.

g) Se han probado, depurado y documentado las aplicaciones generadas.

Indicadores	**Niveles de logro**		
	Bien	**Regular**	**Insuficiente**
	100%	50%	0%

RA 6. Desarrolla aplicaciones de acceso a almacenes de datos, aplicando medidas para mantener la seguridad y la integridad de la información.

e) Se han utilizado conjuntos de datos para almacenar la información.

h) Se han probado y documentado las aplicaciones.

Indicadores	Niveles de logro		
	Bien	Regular	Insuficiente
	100%	50%	0%