API modular segura

Seguridad empresarial - Protección de APIs REST

Webster Cosme de la Rosa
Máster Universitario en Ciberseguridad y Privacidad con especialidad en Tecnologías

Pau del Canto Rodrigo
Consultor

Víctor Garcia Font
Profesor responsable de la asignatura

Universitat Oberta de Catalunya

9 de enero del 2023
Fecha de entrega

Índice

Introducción

Resumen del proyecto

- Protege un API mediante un API Gateway
- El API es monolítica y modular, de fácil adaptación a un modelo microservicios
- El API Gateway establece múltiples capas de seguridad

Justificación del proyecto

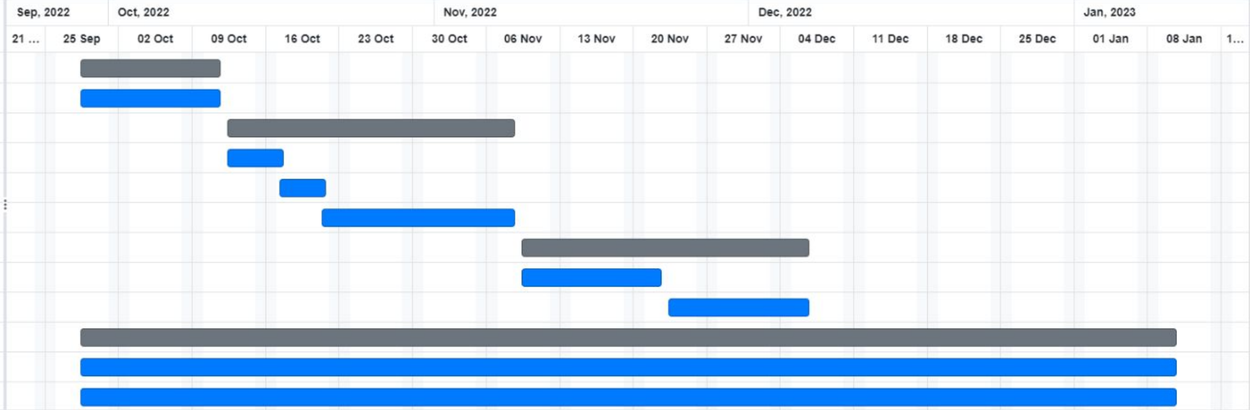
- El uso de microservicios desde el inicio del proyecto no es lo ideal en la mayoría de casos
- La cantidad de amenazas en internet es muy alta por lo que hay que reducir las vulnerabilidades para alcanzar un riesgo razonable
- Proyectos similares en la actualidad que necesitan un ejemplo que tenga buenas prácticas de seguridad

Objetivos

- Ser ejemplo de arquitectura monolítica modular bajo altos estándares de calidad
- Hacer frente a la mayor cantidad de vulnerabilidades descritas en el TOP Ten de OWASP
- Proteger los servicios del API mediante el uso de un API Gateway

Planificación

Name	Start Date	End Date	Duration
▾ PEC 1	Sep 28, 2022	Oct 11, 2022	10 days
Plan de trabajo	Sep 28, 2022	Oct 11, 2022	10 days
▾ PEC 2	Oct 12, 2022	Nov 08, 2022	20 days
Definición del negocio DEMO	Oct 12, 2022	Oct 17, 2022	4 days
Diseño del API	Oct 17, 2022	Oct 21, 2022	5 days
Implementación en SpringBoot	Oct 21, 2022	Nov 08, 2022	13 days
▾ PEC 3	Nov 09, 2022	Dec 06, 2022	20 days
Configuración del contenedor de Kong	Nov 09, 2022	Nov 22, 2022	10 days
Configuración del contenedor de sWAF	Nov 23, 2022	Dec 06, 2022	10 days
▾ PEC 4	Sep 28, 2022	Jan 10, 2023	75 days
Memoria	Sep 28, 2022	Jan 10, 2023	75 days
Script sencillo de despliegue	Sep 28, 2022	Jan 10, 2023	75 days



Negocio

Operaciones CRUD en la tienda

- Mascotas
- Pedidos
- Usuarios

Figura 2: Dominio de la aplicación

Arquitectura

Arquitectura hexagonal

- Adaptador primario: recibe las peticiones
- Dominio: gestiona el problema a resolver
- Puerto secundario: dispone de la dependencias necesarias

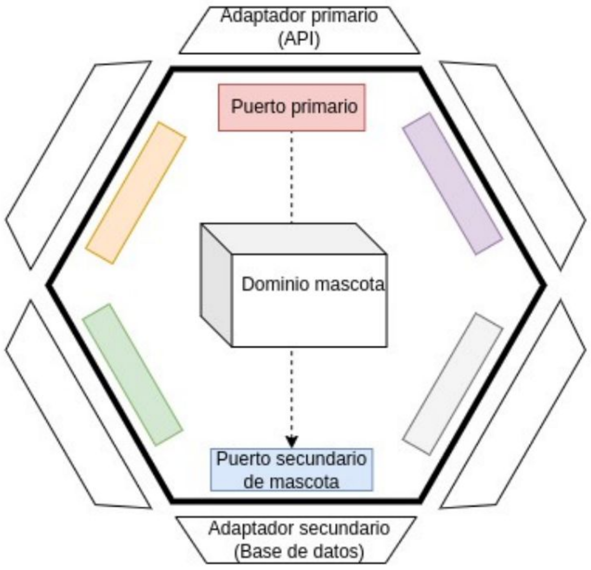


Figura 5: Arquitectura hexagonal

Metodología

Diseño guiado por pruebas

1. Definición del test en función de un requisito
2. Comprobación de que el test falla
3. Modificación del código fuente para que las pruebas pasen
4. Repetir desde el paso 1 si es necesario

Figura 8: Desarrollo guiado por pruebas

Kong API Gateway

Protección del API Modular

- ➢ Key Authentication
- ➢ Lista de control de acceso
- ➢ Frecuencia límite
- ➢ Detección de bots
- ➢ Límite de tamaño de la petición
- ➢ Correlación de identificación

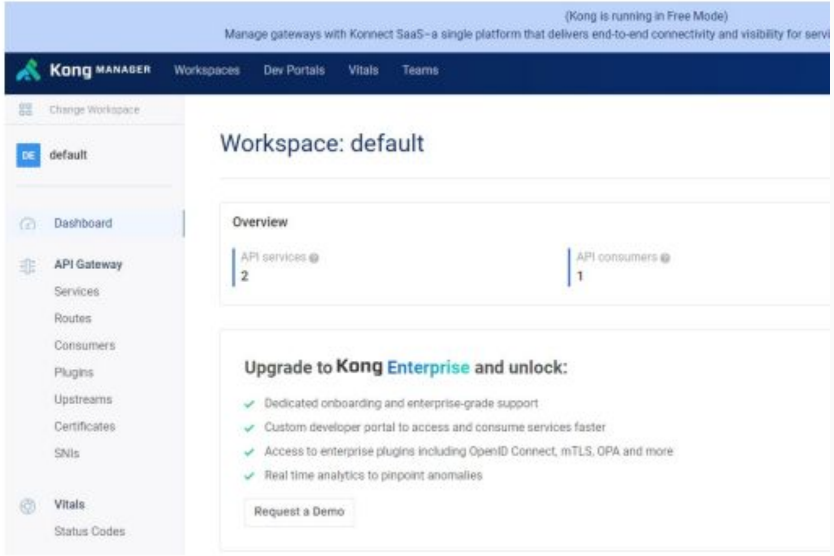


Figura 22: Interfaz web del menú principal de Kong

Resultado obtenido

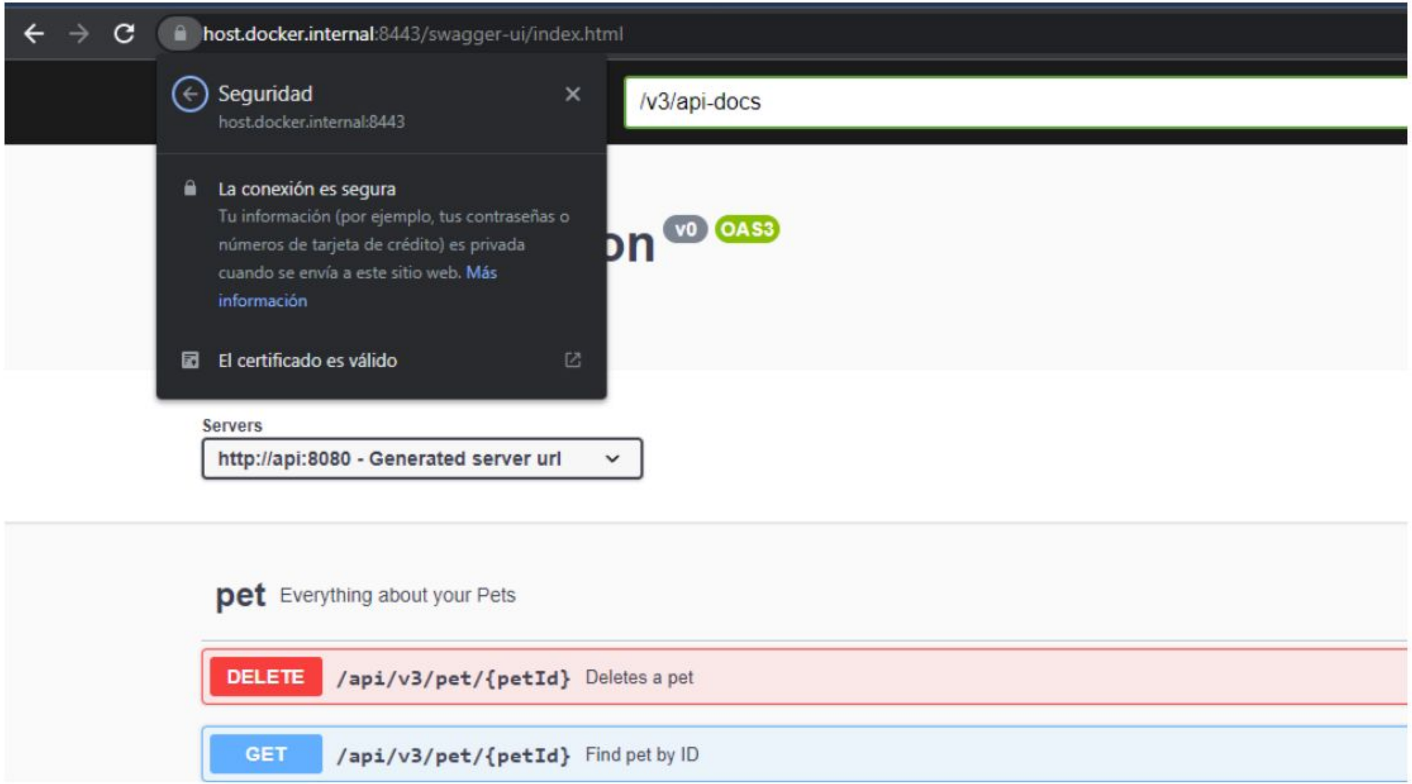


Figura 37: Petición por HTTPS y navegador exitoso

Conclusiones

- Se ofrece acceso a los servicios con confiabilidad, integridad y disponibilidad
- Se ha reducido la complejidad del negocio para poner foco en el diseño de una arquitectura y metodología seguras
- Se ha seguido la planificación fielmente. El profesor colaborador ha participado en el proyecto mediante la aclaración de los requisitos y la resolución de las consultas
- Se espera que se reduzca la huella medioambiental
- Como líneas de trabajo a futuro se
    - Admitir múltiples métodos de autenticación
    - Corrección de las vulnerabilidades en las imágenes de docker
    - Análisis estático de código en la pipeline

Final

Gracias por la atención