Secure Application Design

Requisitos de finalización

Taller de Arquitectura Empresarial: Diseño de Aplicaciones Seguras

En este taller, diseñaremos y desplegaremos una aplicación segura y escalable utilizando infraestructura de AWS, con un enfoque en las mejores prácticas de seguridad. Nuestra arquitectura contará con dos componentes principales:

Servidor 1: Servidor Apache

El servidor Apache será responsable de servir un cliente HTML+JavaScript asíncrono a través de una conexión segura usando TLS. El código del lado del cliente será entregado mediante canales cifrados, asegurando integridad y confidencialidad de los datos durante la descarga.

Servidor 2: Spring Framework

El servidor Spring manejará los servicios backend, ofreciendo endpoints RESTful. Estos servicios también estarán protegidos usando TLS, asegurando comunicación segura entre el cliente y el backend.

Características Clave de Seguridad:

- **Cifrado TLS:** Transmisión segura de datos usando certificados TLS generados mediante Let's Encrypt, garantizando confidencialidad e integridad.
- **Cliente Asíncrono:** Nuestro cliente HTML+JavaScript utilizará técnicas asíncronas para optimizar el rendimiento manteniendo comunicación segura.
- **Seguridad de Login:** Se implementará autenticación de inicio de sesión, con contraseñas almacenadas de forma segura como hashes.
- **Despliegue en AWS:** Todos los servicios serán desplegados y administrados en AWS, aprovechando su infraestructura segura y confiable.

Este taller guiará a los participantes a través del proceso de integración de estas medidas de seguridad, configuración de despliegues multi-servidor y uso de técnicas modernas de cifrado para proteger datos de los usuarios.

Ayuda: https://docs.aws.amazon.com/linux/al2023/ug/ec2-lamp-amazon-linux-2023.html

Ayuda 2: https://spring.io/guides/gs/securing-web

Rubric

Trabajo en Clase (50%)

Participación y Colaboración (20%)

- Participa activamente en discusiones y actividades grupales.
- Colabora efectivamente con compañeros durante los ejercicios prácticos.
- Contribuye con ideas y soluciones durante las sesiones de diseño arquitectónico.

Rendimiento en el Laboratorio Práctico (30%)

- Despliega exitosamente la aplicación en AWS siguiendo las instrucciones proporcionadas.
- Demuestra una configuración correcta de Apache y Spring en servidores separados.
- Configura TLS para la descarga del cliente desde Apache y para solicitudes REST hacia Spring.
- Implementa seguridad de login con almacenamiento de contraseñas como hashes.
- Genera e instala certificados Let's Encrypt en ambos servidores.
- Entrega todo el código relevante en un repositorio de GitHub, incluyendo documentación clara.

Tarea (50%)

Diseño de Arquitectura de la Aplicación (25%)

- Presenta un documento detallado con el diseño de la arquitectura de la aplicación.
- Describe correctamente la relación entre Apache, Spring y el cliente HTML+JS asíncrono.
- Demuestra comprensión de estrategias seguras de despliegue en AWS.

Implementación de Seguridad (15%)

- Entrega una aplicación completamente funcional que cumpla con todos los requisitos de seguridad.
- Configura y demuestra el uso de TLS para conexiones seguras entre el cliente, Apache y Spring.
- Implementa funcionalidad de inicio de sesión con contraseñas almacenadas como hashes.
- Utiliza Let's Encrypt para la gestión de certificados.

Entregables Finales (10%)

- Repositorio GitHub que contenga todo el código fuente, un README con instrucciones de despliegue, resumen de arquitectura y capturas de pruebas.
- Un video demostrando el despliegue de la aplicación y explicando las características de seguridad.