CICLO: DAW
MÓDULO DE DESARROLLO WEB
ENTORNO SERVIDOR

Ejercicios Teóricos

Alumno:
Edward-Ionut, Bunoaica
Y1963355C

Contenido

(Una vez realizado el informe, no olvidar actualizar esta tabla del índice **(F9 + Actualizar toda la tabla)**, con el fin de que se actualicen todos los epígrafes y números de página)

1. Ejercicios basados en mensajes:

- Explica cómo funciona una arquitectura basada en mensajes y menciona dos ejemplos de tecnologías que la implementan.

  Una arquitectura basada en mensajes funciona transmitiendo mensajes entre los diferentes servicios. Para poder conoces este servicio hay que conocer la estructura del mensaje que se debe enviar para ser procesado. Estos mensajes se comunican entre servidores desacoplados. Esto quiere decir que los servidores no hace falta que estén conectados entre ellos.

  Dos empresas que usan este tipo de arquitectura son Microsoft y Amazon

- ¿Cuáles son las ventajas y desventajas de utilizar una arquitectura basada en mensajes en comparación con una arquitectura monolítica?

  Principalmente una arquitectura de mensajes está basada en mandar mensajes sin afectar a los procesos que se estén llevando a cabo sin demorar nada, mientras que la arquitectura monolítica está enfocada en desplegar sus propios procesos a parte para que se desarrollen por separado.

- Describe la diferencia entre la comunicación síncrona y asíncrona en arquitecturas basadas en mensajes.

  Las comunicaciones asíncronas en arquitectura de mensaje son aquellas en las que el mensaje espera a un receptor, esto quiere decir que en caso de que no haya un receptor en el instante en el que está siendo enviado el mensaje se almacena temporalmente, en caso de no haber un receptor se borra y se continúa con el siguiente. La comunicación síncrona hace más o menos lo mismo solo que una vez enviado el mensaje y no hay receptor, el mensaje se almacena hasta que haya un receptor disponible, hasta que el mensaje no sea recibido no se envía otro.

2. Ejercicios basados en recursos:

- Explica en qué consiste una arquitectura basada en recursos y cómo se diferencia de una basada en mensajes.

Una arquitectura basada en recursos como su nombre indica se basa en diferentes recursos que se les otorga a los usuarios para que puedan consumir o usar esos recursos otorgados. En esta arquitectura solo se recibirán las respuestas solicitadas. Esta arquitectura se diferencia de la basad en mensajes debido a que no necesita la abstracción para su mecanismo.

- ¿Qué papel juegan los verbos HTTP en las arquitecturas basadas en recursos? Da ejemplos de cada uno.

En la arquitectura basada en recursos los verbos HTTP son esenciales para su funcionamiento ya que con ellos se hacen las peticiones creadas por el usuario para conseguir los recursos. Estos verbos son los siguientes:

-GET: Se utiliza para solicitar información de recursos

-POST: Se usa para la creación de nuevos recursos.

-PUT: Actualiza un recurso en su totalidad.

-PATCH: Actualiza un recurso parcialmente.

-DELETE: Borra un recurso existente.

- ¿Por qué REST es considerado un paradigma de arquitectura basada en recursos? Explica sus principios fundamentales.

REST es considerado un paradigma de la arquitectura de recurso debido a que usa los verbos HTTP de la misma manera en la que lo hace la arquitectura. REST se diseñó en base a un uso correcto de HTTP, a la arquitectura cliente-servidor, que debe ser sin estado (no deben compartir información entre peticiones) y que todos los recursos deben tener un URI (identificador único).

3. Ejercicios sobre aspectos de seguridad

- Explica qué es el hashing en contraseñas y por qué es importante en la seguridad de datos.

El hashing de contraseñas es una forma de cifrar contraseñas mediante una función hash criptográfica. El hash lo que hace es convertir la contraseña en una cadena alfanumérica usando diferentes algoritmos. Esto es importante para la seguridad de los datos debido a ciber-delincuentes que lo que intentan muchas veces es poder robas estos datos o también para evitar que alguien que no sea la persona que sepa la contraseña pueda usarla

- ¿Cuál es la diferencia entre autenticación y autorización? Da un ejemplo práctico

La autenticación sirve para confirmar que el usuario que quiere iniciar sesión es quien dice ser, mientras que la autorización es la que se confirma que el usuario tiene los permisos suficientes para acceder a cierta información. Esto se puede resumir con un ejemplo muy sencillo, nosotros al poner contraseña a nuestro usuario de Windows estamos autenticando que somos nosotros. En el caso de poner permisos de administrador en nuestro escritorio solamente los usuarios con privilegios de administrador pueden acceder.

- Menciona tres buenas prácticas para la gestión segura de credenciales en una arquitectura orientada a servicios

Principalmente podemos usar una práctica poniendo usuario y contraseña para poder acceder, una segunda práctica podría ser usar un certificado digital como credencial y una última podría ser una tarjeta inteligente o un lector de tarjetas como por ejemplo en la sanidad pública.

4. Ejercicios sobre seguridad de mensajes. Cortafuegos

- Cómo protege un cortafuegos una arquitectura basada en servicios? Explica su funcionamiento.

Antes de decir como el firewall protege un servicio web, vamos a explicar cómo funciona. El firewall es el encargado de proteger nuestro servicio web de conexiones no autorizadas o cualquier tipo de dato malicioso o que no esté permitido. En el caso de un servicio web el firewall es el encargado de ver todo el tráfico de datos, conexiones y comunicaciones que suceden en nuestra web, su misión es prevenir los accesos no autorizados en nuestra red.

- Qué diferencias existen entre un cortafuegos de red y un cortafuegos de aplicación?

El firewall de red es aquel que protege una red local del acceso no autorizado para evitar ataques. Mientras que un firewall de aplicación es aquel ubicado entre los usuarios externos y las aplicaciones para analizar cualquier comunicación que pase. Luego este firewall aísla las solicitudes maliciosas y las bloquea.

- Explica que es el cifrado de extremo a extremo en la seguridad de mensajes y por qué es relevante.

El cifrado de extremo a extremo es un tipo de cifrado que absolutamente nadie puede interceptar, este método protege nuestras comunicaciones y solo pueden ser vistas por el emisor y receptor. Ni google ni cualquier otra empresa puede ver nuestros mensajes. Esto es muy importante ya que esto hace que nuestras conversaciones sean más seguras, privadas y sin intercepción de nadie.

5. Ejercicios sobre control de acceso. El modelo RBAC

- Explica en qué consiste el modelo RBAC y menciona sus principales beneficios.

El modelo RBAC es un mecanismo de control de acceso que define los roles y privilegios para determinar si un usuario se le debe dar acceso a ciertos recursos o no. Principalmente este modelo reduce la complejidad, especialmente en las grandes organizaciones donde puede haber muchas personas en un equipo. Mejora la seguridad al aplicar el principio del mínimo privilegio, esto significa que RBAC restringe el acceso únicamente a lo que es necesario.

- ¿Cuál es la diferencia entre un modelo de acceso basado en roles y un modelo basado en atributos?

Como sus nombres indican el modelo RBAC se basa en roles mientras que ABAC se basa en atributos. Es decir, RBAC concede acceso mediante la función que tenga el usuario y sus permisos, mientras que ABAC concede acceso mediante los atributos del usuario.

- ¿Cómo se implementaría un sistema de control de acceso basado en RBAC en un servicio web?

Un RBAC se implementa a nivel de interfaz. Esto quiere decir que el modelo RBAC controla las vistas, las interfaces y las pantallas que tienen los roles de usuarios individuales. Esto garantiza que los usuarios solo accedan a los datos que tienen permitidos en su rol. Un ejemplo de una empresa que use RBAC es DHL la empresa alemana repartidora a nivel internacional.

6. Ejercicios sobre la seguridad en comunicaciones. Protocolos seguros.

- ¿Cuál es la diferencia entre HTTP y HTTPS? Explica el papel del protocolo TLS en la seguridad

HTTP que significa hyper text transfer protocolo y HTTPS o hyper text transfer protocole secure son dos protocolos que impulsan la comunicación de la red. Estos protocolos lo que hacen es intercambiar datos con un servidor web y nos lo devuelve en forma de página web. Como su nombre indica uno es más seguro que otro debido a que usa TLS, también llamado SSL para encriptar las peticiones y respuestas HTTP normales y firmar esas peticiones digitalmente.

- ¿Qué es un certificado SSL y cómo garantiza la seguridad en las comunicaciones?

El certificado SSL es u certificado que autentica la identidad de un sitio web y habilita una conexión cifrada. El certificado SSL acredita que las páginas web son legales y que sus transacciones son seguras de un extremo a otro.

- ¿Por qué es importante la autenticación mutua en protocolos seguros como TLS?

Esto es importante para que no se suplante la identidad de la otra parte del canal de comunicación. Esto quiere decir que los dos extremos del canal de comunicación se verifican mutuamente para que se acredite que son ellos y no haya ninguna suplantación.