Actividad 1.2 Contesta las preguntas sobre el Protocolo HTTP y HTTPS y envía un archivo PDF como producto de las actividad Educatec

Gustavo Adolfo Gutierrez Martinez 20051193

1. ¿Qué significa HTTP?
   - a) HyperText Transfer Protocol
   - b) HyperText Transmission Protocol
   - c) HyperLink Transfer Protocol
   - d) HyperLink Transmission Protocol

2. ¿Cuál de las siguientes opciones NO es un método HTTP?
   - a) GET
   - b) POST
   - c) DELETE
   - d) SEND

3. ¿Qué código de estado HTTP indica que el recurso solicitado no se encontró en el servidor?
   - a) 200
   - b) 301
   - c) 404
   - d) 500

4. ¿Cuál es la principal diferencia entre HTTP y HTTPS?
   - a) HTTPS usa un puerto diferente al de HTTP.
   - b) HTTPS cifra los datos transferidos entre el cliente y el servidor.
   - c) HTTP es más rápido que HTTPS.
   - d) HTTP solo se usa para sitios web estáticos.

5. ¿Qué es un certificado SSL/TLS?
   - a) Un archivo que proporciona la identidad del servidor y cifra los datos transferidos.
   - b) Un tipo de servidor web.
   - c) Un método de compresión de datos.
   - d) Un tipo de navegador web.

Parte 2: Verdadero o Falso

6. HTTP es un protocolo sin estado.
   - a) Verdadero
   - b) Falso

7. HTTPS es más seguro que HTTP porque cifra las solicitudes y respuestas.

- a) Verdadero
- b) Falso

8. El método HTTP PUT se utiliza para recuperar datos de un servidor.
- a) Verdadero
- b) Falso

9. Un código de estado HTTP 500 indica un error del cliente.
- a) Verdadero
- b) Falso

10. Es posible usar HTTPS sin un certificado SSL/TLS.
- a) Verdadero
- b) Falso

11. Explica la diferencia entre los métodos HTTP GET y POST.
- Los métodos GET se usa para obtener información sin modificar el servidor y los datos se envían en la URL.
- Los métodos POST se usa para enviar o modificar información en el servidor y los datos se envían en el cuerpo de la solicitud.

12. Describe el proceso de una conexión HTTPS segura desde el momento en que el cliente envía una solicitud hasta que recibe una respuesta.
1. El cliente envía una solicitud para establecer conexión usando HTTPS.
2. Se inicia la negociación con el protocolo TLS y el cifrado.
3. El servidor envía un certificado al cliente y ambos intercambian claves para generar el cifrado.
4. Se generan claves simétricas para cifrar la sesión.
5. Se confirma una conexión segura.
6. Los datos se envían cifrados entre el cliente y el servidor.
7. Los datos recibidos son descifrados y procesados en el cliente y servidor.

13. Enumera y explica al menos tres códigos de estado HTTP diferentes y lo que representan.
1. **101 Switching Protocols**: El servidor acepta cambiar el protocolo según lo solicitado por el cliente (por ejemplo, de HTTP/1.1 a HTTP/2).

2. **400 Bad Request**: La solicitud del cliente es inválida o malformada y no puede ser procesada por el servidor.

3. **504 Gateway Timeout**: El servidor, mientras actuaba como una puerta de enlace o proxy, no recibió una respuesta a tiempo del servidor de upstream.

14. ¿Por qué es importante utilizar HTTPS en un sitio web que maneja información sensible?
Al ser información sensible es indispensable el uso de HTTPS, ya que de esta forma aseguramos que los datos estén cifrados y protegidos contra algún tipo de intercepción o alteración, también nos permite verificar la identidad del servidor aumentando así la confianza del usuario.

15. Describe cómo un navegador verifica la validez de un certificado SSL/TLS.
1. Primero el navegador recibe el certificado del servidor.
2. Se verifica la cadena de certificación confirmando que el certificado se encadena correctamente con una autoridad de certificación de confianza.
3. Se valida la forma digital usando la clave publica de la Autoridad de Certificación (CA).
4. Se valida la validez del certificado asegurándose que este dentro del periodo de valides revisando la fecha de validez.
5. Se valida el nombre del dominio, lo que quiere decir que, se asegura que el certificado sea valido para el dominio que se solicitó.
6. Se verifica que el certificado no haya sido revocado.
7. Se verifica que el certificado cumpla con las políticas y restricciones.
8. En caso de que alguno de los pasos anteriores falle entonces el navegador mostrara que la conexión no es segura.