11086 - Programación en Ambiente Web - UNLU
Primer Parcial 2020

Alumno: Pavlo Fedorov (Legajo 113080)

Entrega: archivo PDF por mail a la dirección paw@unlu.edu.ar antes del viernes 1 de mayo a las 23.59.59, es decir cuenta con 36hs para realizarlo. Además del envío por mail del PDF se solicita suban también dicho archivo PDF a un repositorio propio y envíen dicha dirección en mail aparte o por whatsapp/telegram para garantizar recepción a tiempo utilizando dos vías independientes y con timestamp.
Metodología: el examen es individual y si bien puede utilizar libros e Internet, el examen debe ser autocontenido y con respuestas «propias», no con URLs hacia material externo. Puede incluir esquemas o lo que considere necesario para ilustrar sus respuestas.
Nota Importante: En ninguno de los 10 puntos se solicita código. Responda cada punto considerando el escenario más real/auténtico que pueda imaginar y explicite cada una de sus asunciones.

Imagine una aplicación web "portal de noticias" y responda las siguientes consignas:

1. ¿Por qué las sesiones pueden guardar mucha más información que las cookies? ¿Qué almacenaría para esta app en cookies y/o sesiones?

A diferencia de las cookies, que se almacenan a nivel local en el navegador web del cliente, las sesiones pueden almacenar mucha más información ya que se alojan remotamente en el servidor web, el cual, por lo general posee un espacio de almacenamiento superior a la máquina de un cliente particular que utiliza un navegador web. El tamaño de las cookies está limitado por el navegador web del lado del cliente. Además, a diferencia de las cookies, que pueden ser manipuladas por el usuario, y estan limitadas en cantidad de información que pueden almacenar, las sesiones almacenan datos más sensibles, los cuales no pueden ser manipulados por el usuario.
Suponiendo que el portal de noticias posee un acceso público a determiandos artículos peridísticos y un acceso privado, mediante un usuario registrado en el portal, a artículos pagos, se podría utilizar cookies para ambos tipos de usuarios para almacenar el origen de la conexión, es decir, desde donde se conecta dicho usuario así como la preferencia de las categoria de noticias más vista. Por otro lado, teniendo en cuenta, al acceso via autenticación, se utilizaría una sesión para almacenar datos más relevantes del usuario registrado como por ejemplo las credenciales de tarjetas de crédito/débito o algunas carecterísticas de su plan mensual de beneficiario.

2. ¿Qué ventajas ofrece el uso de Virtualhost en el contexto de servidores Web (en gral y en particular para esta app)?

El uso de Virtualhost en el contexto de los servidores Web ofrece las siguientes ventajas:
- Permite configurar e implemetar múltiples sitios en un mismo equipo físico o servidor abaratando notablemente los costos de tener un equipo dedicado exclusivamente para cada sitio.
-Desde el punto de vista de quien quiera tener un sitio web alojado, se disminuye considerablemente el costo de acceso, es decir, se abarata el costo para aquellos clientes que contraten un servicio de alojamiento para su sitio web.
-Cada sitio puede tener su propia configuración además de su contenido.

Desde el punto de vista de la aplicación de noticias, dentro de la organización se podría implementar las directivas del virtual hosting de manera que sea posible tener configurado, un sitio para el ambiente de desarrollo y otro para UAT, donde se llevan a cabo las pruebas de aceptación de

usuario para los cambios que pasan desde el ambiente de desarrollo. Esto resultaria ser un beneficio a la hora de medir los costos en el caso de que se quiera adquirir uno o varios servidores físicos.

3. Defina con sus palabras la diferencia principal entre contenido estático y dinámico.

Teniendo en cuenta un criterio dirigido hacia la web, el contenido estático es un contenido que se presenta de forma estática donde el objetivo principal es ofrecer datos al usuario, los cuales se mantienen invariantes en el transcurso del tiempo en un determinado sitio web.
Por otro lado, un contenido dinámico hace referencia a aquellos elementos del sitio web que cambian con el tiempo, es decir, que pueden sufrir modificaciones y alteraciones de acuerdo a las acciones (interacciones) llevadas a cabo por un usuario sobre el contenido.
Como ejemplo, teniendo en cuenta el portal de las noticias, el nombre del portal como su historia descriptiva puede generarse como contenido estático a partir de un lengauje de marcado como HTML. Por su parte, el listado principal de las últimas noticias como contenido dinámico se puede generar a partir de un lenguaje de programación del lado del servidor como por ejemplo PHP, y si se quiere añadir alguna opción interactiva del lado del cliente como la votación positiva o negativa de una nota periodística, es posible utilizar JavaScript.

4. ¿Cómo aplicaría el modelo MVC para el diseño de esta app?. No necesita escribir código alguno, sino argumentar conceptualmente como separaría la lógica de la app en estos tres elementos.

En la capa de modelo se tendrian las siguientes entidades o modelos:

- Privilegios
- Usuarios
- Noticias
- Categorias

Cada uno de estos modelos mapeados a clases tendria métodos que permitan crear, actualizar, eliminar o visualizar cada instancia de dicho modelo, además de otras características como el acceso a sus atributos.
Cada modelo usuario tendría una relación con el modelo privilegio así como también cada noticia tendría relación con categoría.

En la capa de las vista se tendría en primer lugar una vista para el listado de cada modelo así como también las vistas para el alta, baja (lógica) y actualización/modificación para cada uno.

Con respecto a la capa del controlador, se tendría un controlador por cada modelo que permita tener funcionalidades referidas para visualizar el listado de los diferentes elementos de cada modelo asi como operaciones de altas, bajas y modificaciones retornando las vistas correspondientes para cada petición.

5. a) ¿Por qué es posible afirmar que PDO mejora la seguridad en la capa de base de datos de una app PHP?
b) ¿Qué otras cuestiones debemos tener en cuenta en la capa de base de datos en el sentido de la seguridad?

(a) PDO (PHP Data Objects) mejora la seguridad en la capa de base de datos de una aplicación PHP debido a que permite realizar operaciones sobre la base de datos con sentencias preparadas o precompiladas evitando que un usuario malicioso aplique técnicas de inyección de código SQL por ejemplo en cualquier operación de consulta o actualización. Además, dichas sentencias preparadas

permiten establecer automáticamente los datos utilizados en los marcadores de posición (parámetros) evitando de esta manera el ataque descrito anteriormente.

(b) Cuestiones que se deben tener cuenta en la capa de la base de datos en el sentido de la seguridad:

- El acceso al servidor físico que almacena la base de datos, no debría ser directamente visible para usuarios finales o ciertos individuos del equipo de desarrollo por la sensibilidad que puedan acarrear ciertos datos almacenados.

- Llevar auditoria de accesos y actualizaciones sobre los datos de una base de datos así como determinar que información a nivel de tablas pueden visualizar los diferentes usuarios que acceden mediante una aplicación alojada en el servidor web de un sitio.

- Posibilidad de encriptar la base de datos a nivel de bloque de disco.

6. La app muestra signos de "envejecimiento" en cuanto al diseño, tanto usuarios finales como redactores del portal lo informan a diario. ¿Qué ideas se le ocurren al respecto?

En la actualidad, la tecnología avanza de manera vertiginosa y es muy fácil quedarse atrás si no se toman ciertas directivas para lograr mantener actualizado un sitio web en términos de diseño y tecnología. Básicamente, si se está llegando a una situación donde un sitio web muestra señales de “envejecimiento”, se debería proceder a una paulatina migración del contenido de presentación a esquemas modernos que puedan adapartse al usuario o cliente final y la gran variedad de dispositivos como tablets, télefonos móviles, entre otros. Es necesario, que la aplicación pueda modernizarse en los aspectos de diseño teniendo en cuenta características como la responsividad, la adaptabilidad a diferentes dispositivos, mayor accesibilidad para personas con diferentes capacidades, mejor operabilidad y una interfaz amigable para el usuario. Todas estas características permitirían atraer un gran número de clientes o usuarios potenciales.

8. Imagine ahora que el "portal de noticias" debe considerar tener un "paywall" (ciertos contenidos se vuelven pagos) y por ende almacenará tarjetas de débito / crédito de los clientes.
a) ¿Cuáles son las implicancias de seguridad de esta nueva funcionalidad?
b) ¿Cómo implementaría algún límite sobre la cantidad de noticias que puede ver un usuario que no paga, e.g. puede ver sólo 10 artículos por mes calendario?

(a) Tanto las credenciales de acceso de usuarios registrados en el portal como el almacenamiento de determinados datos de las tarjetas de débito/ crédito constituyen una mayor sensibilidad en cuanto a datos se refiere. En este caso se deberá reforzar las medidas de seguridad en cuanto a mantener al resguardo aquellos datos de los titulares. Esto significa reforzar las medidas de seguridad de la red interna donde se aloja esa información, restringir el acceso físico a dicha información por parte de los individuos que forman parte del portal de noticias, mantener un registro y supervisión de todos los accesos a los recursos de la red como así también el envío de cualquier información referida a las tarjetas almacenadas por una red pública, debe estar cifrado.

(b) Una vez que el usuario se registra, por defecto se le podría permitir acceder solamente a 10 artículos por mes calendario habilitando una noticia por cada categoría hasta llegar a 10 mediante un proceso que controle en caso de que no haya un pago acreditado y por ende dicho usuario tenga un atributo asociado que le permita a la aplicación decidir si debe mostrarle todas las noticias o solamente una parte, como en este caso, por cada mes.

9. Se requiere implementar un buscador de noticias dentro de esta app. Explique qué responsabilidades tiene cada capa de la aplicación en la resolución de la búsqueda. ¿Qué método HTTP le parece el más adecuado para implementar esto? ¿Qué problemas observa?

La capa del navegador tendrá la responsabilidad de tomar el criterio de búsqueda y enviar una petición HTTP con los respectivos parámetros al servidor. Cuando reciba la respuesta del servidor, deberá mostrar las noticias según el criterio de búsqueda.
Dentro de la capa del servidor, la aplicación tendrá la responsabilidad de tomar la petición HTTP y traducirla a una llamada de la capa de persistencia, la cual le devolverá mediante un operación de consulta a la base de datos el correspondiente resultado de la información necesaria. Una vez que la aplicación, dentro de la capa del servidor, obtenga el resultado esperado, lo enviará como respuesta mediante HTTP al navegador web del usuario.
El método HTTP más adecuado para implementar esta funcionalidad es el GET debido a que justamente es una primitiva que está diseñada, desde el uso correcto, para recuperar cualquier dato o recurso del servidor web.
Como las peticiones GET tienen restricciones de longitud, se tendria que controlar que el crierio de búsqueda sea considerablemente acotado.