UNIDAD6.ACTIVIDAD1

DESARROLLO

Francisco Javier Signes Costa 2º DAW online

Las aplicaciones que podemos crear haciendo uso de tecnología web nos pueden proporcionar experiencias de aplicaciones muy similares a las que ofrece una aplicación de escritorio, especialmente si utilizamos librerías JavaScript, pero toda la comunicación de los sitios web se realiza a través de un canal no seguro, tal y como es actualmente internet.

En esta actividad vamos a analizar cómo podemos crear sitios web que tengan una apariencia profesional y sobre todo vamos a investigar acerca de los sistemas de seguridad que debemos de implementar para garantizar que nuestra aplicación se comporte como una aplicación profesional.

En esta actividad, deberemos crear un documento de tipo Word, con una extensión que no sea mayor a 5 páginas, y que enviarás a tu profesor por email o mediante la plataforma educativa, detallando los siguientes puntos en los que analizaremos los siguientes puntos:

- Analiza qué es Bootstrap y busca otras librerías similares.
- Crea un documento en el que contemples todas las medidas de seguridad de debería de tener un sitio web. Desde los protocolos de comunicación y los certificados que se necesitan hasta la forma en cómo se debería de guardar la información en las bases de datos y el uso de métodos de cifrado de información.

Bootstrap

Bootstrap es una librería multiplataforma de código abierto desarrollada por Twitter para diseños de sitios y aplicaciones web. Contiene multitud de ayudas como plantillas de diseño con infinidad de elementos de diseño basado en HTML y CSS así como extensiones de JavaScript adicionales.

A diferencia de muchos frameworks, Bootstrap sólo se ocupa del desarrollo front-end.

Instalación

Existen varios modos de añadir Bootstrap a nuestro proyecto:

- *Instalación vía gestores de paquetes*. Bootstrap admite la instalación con varios de ellos:
  - Npm
  - Yarn
  - RubyGems
  - Composer (que ya lo hemos utilizado para instalar CodeIgniter)
  - NuGet
- *Instalación vía CDN via jsDelivr:* simplemente añadimos los links a bootstrap al head del HTML para que en cada petición se enlace a Bootstrap. Sería como trabajar en remoto con la librería.
- *Instalación vía CSS y JS compilado:* Descargamos los archivos directamente a nuestro proyecto y enlazamos sobre ese archivo.

Bootstrap añade a tu proyecto multitud de herramientas sobretodo utilidades que con CSS puro sería tedioso trabajar. No obstante, esta librería permite añadir CSS en forma de variables para hacer aún más flexible y adaptable tu proyecto.

Variables CSS

Bootstrap incluye variables que proporcionan un acceso fácil a valores comúnmente usados como colores y demás elementos. Todas las propiedades de Bootstrap vienen con el prefico *–bs*.

Estas variables las podemos usar en cualquier parte del código pero lo más normal es usarlas de manera global para, justamente, hacer que su potencial llegue a todo el código. Para ello Bootstrap nos da unas variables por defecto que las podemos usar en *:root* volviéndose accesibles en todas partes.

Estas variables son susceptibles de ser modificadas vía CSS para adaptarlas a nuestro diseño y necesidades.

Componentes

La manera de trabajar con Bootstrap es la de usar los componentes de que librería ofrece y adaptarlos directamente al proyecto. Hay muchos componentes pero los más importantes serían:

- Headers
- Sidebars
- Footers
- Dropdowns
- Botones
- Breadcrumbs
- Carrusel
- Formularios varios
- Sign-in
- Plantillas de inicio
- Navbars
- Etc.

Todos los componentes tienen una plantilla en la web de Bootstrap donde podemos copiar el código y adaptarlo al proyecto. Tenemos también la documentación por cada componente para poder ver su funcionamiento.

Iconos

Bootstrap incluye una amplia selección de iconos para aportar al proyecto. Al igual que cualquier componente, los podemos añadir de las mismas formas descritas anteriormente.

El uso de los iconos de Bootstrap se pueden incluir directamente en el HTML dependiendo de la instalación que hayamos hecho. Se recomienda usar width: 1em para un resizing via Font-size.

- Iconos embebidos
- Mediante el elemento <use> dentro del HTML (sprite)
- Referenciar el icono con <img>
- Iconos con clases para referenciarlos luego en CSS

Alternativas a Bootstrap

- Materialize
- ZURB Foundation
- Material Design
- Bulma
- Skeleton

- Uikit
- Metro4

Seguridad

La seguridad de un sitio web es complicada. Proteger un sitio requiere proteger todas las formas en que alguien con malas intenciones puede dañar tu sitio.

En pocas palabras, la seguridad de un sitio web es la protección que los propietarios de sitios web ponen en marcha para evitar que sus sitios web sufran ataques maliciosos.

¿Por qué deberíamos preocuparnos por la seguridad y cómo implementarla?

Cualquier ataque malicioso sobre una web tiene como objetivo el recopilar datos, bloquear accesos o evitar el normal funcionamiento del sitio. O todas juntas. Es importantísimo, por el bien reputacional de la empresa y de los datos que los clientes nos han dado, que éstos estén seguros y no puedan ser empleados de manera maliciosa por terceros con el fin de lucrarse.

Amenazas más comunes

Vulneración de datos

Una vulneración de datos se produce cuando alguien expone información confidencial. Las vulneraciones de datos pueden ocurrir por accidente, pero los ladrones cibernéticos también se dirigen a sitios web y aplicaciones web para robar datos que pueden vender en el mercado negro o utilizar para penetrar más en la red de la empresa. Los datos económicos y médicos son objetivos comunes, pero los hackers también pueden vender datos de estudiantes, correspondencia y fotos privadas e información de contacto de los clientes.

Denegación de servicio (Dos)

Un ataque de denegación de servicio (DoS) es un intento de bloquear un sitio web sobrecargando sus servidores. Un ataque similar es una denegación de servicio distribuida (DDoS). En un ataque distribuido, el tráfico proviene de diversos recursos. Esto hace que sea más difícil de detener. Puedes bloquear una fuente para que no inunde tu servidor web, pero es mucho más difícil mantener cientos de fuentes, sobre todo si la lista cambia constantemente.

Ransomware

El ransomware es un código malicioso que bloquea el acceso a tu sitio web hasta que pagas un rescate. El ransomware es cada vez más frecuente para las pequeñas empresas y los ayuntamientos. Un delincuente cifra los archivos informáticos y los datos de usuario, y luego se ofrece a venderte una clave de descifrado a cambio de dinero en efectivo (a menudo Bitcoin u otra criptomoneda). Se trata de un delito altamente rentable porque cuesta menos pagar el rescate que recuperar el acceso a los archivos comerciales de cualquier otra manera.

Scripting entre sitios (XSS)

El ataque de scripting entre sitios (XSS) se produce cuando un actor malicioso inyecta scripts ejecutables en el código de un sitio web. Cuando esto tiene éxito, el hacker puede acceder y controlar el sitio web para hacerse pasar por personas que tienen acceso legítimo a su código web.

Prácticas recomendadas de seguridad

- Mantener actualizados el software y los parches de seguridad
- Agregar SSL y HTTPS
- Requerir contraseñas complejas y cambiarlas frecuentemente
- Restringir los privilegios de administración
- Cambiar las opciones predeterminadas
- Hacer una copia de seguridad de los archivos
- Usar un firewall (WAF)
- Implementar la autenticación multifactor (MFA)
- Realizar inspecciones de seguridad
- Utilizar una red de distribución de contenido (CDN)
- Y sobre todo lo demás, educar y formar a los empleados sobre las prácticas recomendadas

Y si todo lo anterior no ha surtido efecto:

- Tener un plan de recuperación

Protocolos

Los protocolos de red se implementan utilizando múltiples capas con diferentes propósitos. Si bien se han desarrollado múltiples marcos para modelar este ecosistema, el más utilizado es el modelo de Interconexión de Sistemas Abiertos (OSI)

El modelo OSI:

- Capa física
- Capa de enlace de datos

- Capa de red
- Capa de transporte
- Capa de sesión
- Capa de presentación
- Capa de aplicación

IPsec y Red Privada Virtual (VPN)

SSL/TLS

DTLS

Kerberos

SNMPv3

HTTPS

Protección en bases de datos

La seguridad de las bases de datos se refiere al conjunto de herramientas, medidas y controles diseñados para establecer y mantener la confidencialidad, integridad y disponibilidad de las bases de datos.

Se deben proteger:

- Los datos en sí
- El sistema de gestión de bases de datos (DBMS)
- Cualquier aplicación asociada
- El servidor de base de datos físico y/o el virtual, y también el hardware subyacente.
- La infraestructura informática o de red utilizada

Amenazas habituales

- Amenazas internas:
  - Usuario malicioso
  - Usuario negligente
  - Infiltración
- Error humano
- Ataques por inyección SQL/NoSQL
- Desbordamiento
- Programas maliciosos
- Ataques a copias de seguridad
- Ataques de denegación de servicio (DoS/DDoS)

Bibliografía

- Bootstrap (framework) - Wikipedia, la enciclopedia libre
- Bootstrap · The most popular HTML, CSS, and JS library in the world.
- Using CSS custom properties (variables) - CSS: Cascading Style Sheets | MDN
- Top 7 mejores frameworks alternativas a Bootstrap - Guiadev
- Cómo proteger tu sitio web - Guía de seguridad en páginas web | Mailchimp
- Cuáles son los protocolos de seguridad de la información | Clinic Cloud
- 6 tipos de protocolos de seguridad de red - Check Point Software
- Seguridad de las bases de datos: guía básica | IBM