UANL

FCFM

Diseño Orientado a Objetos

Tarea 1

Maestro: Miguel Angel Salazar Santillán

Alumno: Adrián Campos Treviño

1547530

Tipos de aplicaciones web

Web Estática

Este tipo de aplicación muestra poca información dentro de ella, están comúnmente desarrolladas con HTML y aunque también pueden mostrar objetos en movimiento dentro de si mismas como por ejemplo imágenes de tipo GIF, videos precargados, entre otros.

Este tipo de aplicaciones solo se puede modificar descargando el archivo HTML, modificarlo y luego volverlo a subir al servidor donde se mostraba, este tipo de cambios solo los puede lograr la empresa que diseño la aplicación.

Web dinámica

Este tipo de aplicaciones son más complejas que sus aplicaciones hermanas, manejan mucha más información que cargan de bases de datos fuera de la aplicación, los contenidos que se visualizan en este tipo de aplicación se actualizan cada vez que el usuario entra a ella, cuentan con un panel de administración desde el que se administra, pública y crea el contenido de la aplicación de manera mas simple.

Vulnerabilidades en aplicaciones web

Una aplicación web puede ser blanco de ataques o daños desde el robo de información de los usuarios hasta que tu aplicación sea convertida en un portal donde se descarguen programas maliciosos.

Las vulnerabilidades más comunes son:

Configuración errónea de seguridad

Posiblemente la más común de todas, la mala configuración de seguridad en una aplicación puede llevar a un desastre si no se refuerza lo más pronto posible. Los atributos por defecto son lo que más afecta en este tipo de problema, pues la contraseña “admin1234” aparte de ser deducible también vienen en los diccionarios de los atacantes por fuerza bruta.

Solicitudes falsificadas en sitios cruzados.

El atacante engaña a la victima al enviar solicitudes HTTP que no desea lo que permite al atacante ejecutar operaciones que el usuario no desea, esto se puede relacionar con los pop ups que aparecen en sitios de dudosa seguridad.

Referencias directas e inseguras a objetos.

Exponer referencias a objetos de implementación interna como archivos, directorios y base de dato por lo qué pueden ser manipulados. Por ejemplo si usamos un script de descarga que recibe como parámetro el nombre del archivo, puede ser usado para enviar al atacante nuestro documento de configuración con la clave de nuestra base de datos, una solución a esto es usar controles de acceso y no ofrecer datos sobre la implementación interna.

Almacenamiento inseguro

Si un atacante tuviera acceso a nuestra información y esta no se encontrará asegurada, podría acceder a contraseñas y datos de tarjeta de crédito de usuarios y clientes entre otra información sensitiva, al encriptar información sensible en nuestra base de datos evitamos que el atacante pueda llegar a la información que se almacena en las bases de datos, de esta forma si es que entra tendría también que desencriptar la información llevándole mas tiempo.

Inyección

Este tipo de ataque ocurre cuando información no confiable entra por medio de los formularios o comandos que se interpretan por la base de datos, esto puede resultar en robos o perdidas de información, una forma de evitar esto es validar y limpiar lo que el usuario pueda ingresar al sistema antes de correr un proceso.