UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

Facultad de Ciencias Físico Matemáticas

Diseño Orientado a Objetos

SEMESTRE: Agosto-Diciembre 2017

MTRO: Miguel Ángel Salazar Santillán

ACTIVIDAD: Ensayo

Salón: 413

ALUMNO: José Santiago Vázquez García

SAN NICOLÁS DE LOS GARZA, NUEVO LEÓN A 18 DE AGOSTO DEL 2017

FCFM
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Existen demasiados tipos de software como el software de sistema y de aplicación.

El de sistema consiste en programas de bajo nivel interactuando con el ordenador a un nivel muy básico, como los sistemas operativos y compiladores. A cambio del software de aplicación o programas de usuario final

Existen demasiados tipos de software como los de a continuación:

Software acceso a contenidos como navegadores web, aplicaciones multimedia, programas de presentación.

Software de entretenimiento como videojuegos

Software educativo

Software de información para trabajadores como Aplicaciones para la gestión del tiempo, gestión de datos, documentación, software de análisis, software de ayuda, recursos del sistema y software financiero.

Software para empresas como software de gestión de base de datos

Software de simulación como simuladores científicos, sociales o de guerra, de emergencia, de vehículos o de vuelo.

Software de desarrollo multimedia para la gestión de imagenes, vídeos o música. También de animación de gráficos imágenes o vídeos

Software de ingeniería de producto como asistido por ordenador (CAD),

Solo por mencionar algunos.

El software de programación se puede dividir como: Editores de texto, Compiladores, Intérpretes, Enlazadores, Depuradores, Entornos de Desarrollo Integrados (IDE)

FCFM
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Top Vulnerabilidades de una aplicación web

Autenticación rota: ocurre cuando es posible suplantar ña identidad del usuario al obtener accesos como contraseñas o identificadores, por ejemplo modificar el id de la sesión en la cookie y obtener acceso.

Secuencia de comandos en sitios cruzados: permite desplegar en el navegador datos no confiables ingresados por usuarios generalmente inyectando código JavaScript malicioso, así poder secuestrar el sitio web, permitiendo a los usuarios ser redireccionados a sitios web maliciosos

Inyección: Ocurre cuando a nuestro sistema entra información no confiable a través de formularios o comandos que son interpretados por nuestra base de datos. Puede resultar robo o pérdida de información.

Solicitudes falsificadas en sitios cruzados: el atacante engaña a la víctima a enviar solicitudes HTTP que no desea lo que permite al atacante ejecutar operaciones que el usuario no desea.

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.

Insuficiente protección en la capa de transporte. Todo el tráfico en internet puede ser escuchado, y al enviar información sensitiva como contraseñas, números de tarjeta o documentos sin su apropiada autenticación y encriptación, alguien puede tener acceso a esa información.

FCFM

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Bibliografía

https://www.owasp.org/index.php/Main_Page