Universidad Autónoma de Nuevo león

Facultad Ciencias Fisco Matemático

DOO

LSTI

Miguel Salazar

Edgar Vázquez Márquez

1657462 Grupo: 006 Aula: 101

Viernes 18 de agosto de 2017

San Nicolas, Nuevo León

TIPOS DE APLICACIONES DE SOFTWARE

Mientras estaba navegando en algunas páginas y blogs de internet llegue a la conclusión de los más importantes serían los siguientes:

Software de información para trabajadores

Estas servirían más que nada a la gestión de datos e igual a la documentación.

Software acceso a contenidos

Serian los navegadores web, aplicaciones multimedia, programas de presentación, etc.

Software de entretenimiento

Se inclinaría más que nada en los videojuegos.

Software educativo

A las aplicaciones para gestión de clases y entrenamiento, gestión de encuestas, etc.

Software de desarrollo multimedia

Para la gestión de imágenes, vídeos o música. También de animación de gráficos imágenes o vídeos, editores vectoriales, secuenciadores musicales.

- Algunos ejemplos de Software de Aplicación:
- Los Procesadores de texto como Word, Bloc de Notas.
- Editores de imágenes como Adobe Fireworks, o Adobe Photoshop.
- Sistemas Administradores de Bases de Datos (Oracle, SQL Server).
- Editores de Páginas Web, Adobe Dreamweaver.
- Editores de Lenguaje de programación Visual Studio PHP Edit.
- Programas de Contabilidad.
- Programas de Gestión de proyectos como MS Project.
- Programas de Diseño asistido por computadora como Auto CAD.

VULNERABILIDADES DE UNA PAGINA WEB

La web pueden presentar diversas vulnerabilidades que van de acuerdo a los servicios que puedan prestar. De acuerdo con la OWASP (Open Web Application Security Project) las vulnerabilidades en aplicaciones web más explotadas a finales del año 2013, fueron las siguientes:

- Injection
- Broken Authentication and Session Management
- Cross Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration

OWASP tuvo una pequeña variación a la lista que subió en el 2009 a la del 2013.

Injection

Consiste en insertar o inyectar una consulta SQL a través del intercambio de datos entre el cliente y la aplicación.

Un ataque de SQL Injection, es capaz de leer datos sensibles de la base de datos, modificar los datos de dicha base de datos (Insert, Delete, Update), ejecutar operaciones como administrador, recuperar el contenido de un archivo dado que se encuentra en el Sistema de directorios del Sistema Manejador de Bases de Datos (DBMS) y en algunos casos ejecutar comandos en el sistema operativo.

Broken Authentication and Session Management

La autenticación y la gestión de sesiones incluyen todos los aspectos relacionados con el manejo de la autenticación de usuarios y la gestión de sesiones activas. La autenticación es un aspecto crítico de este proceso, pero incluso los sólidos mecanismos de autenticación pueden ser debilitados por funciones de administración de credenciales defectuosas, incluyendo cambio de contraseña, olvido mi contraseña, recuerdo mi contraseña, actualización de cuenta y otras funciones relacionadas. Todas las funciones de administración de cuentas deben requerir re autenticación incluso si el usuario tiene un ID de sesión válido.

Cross Site Scripting (XSS)

El XSS es un fallo de seguridad en sistemas de información basados en web, que más que comprometer la seguridad del servidor web compromete la seguridad del cliente.

El XSS es un ataque, que consiste en inyectar código, HTML y/o JavaScript en una aplicación web, con el objetivo de que el cliente ejecute el código inyectado al momento de ejecutar la aplicación.

Insecure Direct Object References

Esta vulnerabilidad no supe muy bien o más bien buscar un ejemplo o un significado algo mas coherente. En una página se lo referían a cuando una referencia a un objeto de implementación interna, tal como un archivo o llave de base de datos, se expone a los usuarios sin ningún otro control de acceso. Según el curso de protección de datos personales, el atacante puede manipular esas referencias para obtener acceso a los datos no autorizados.

Security Misconfiguration

La configuración errónea de seguridad puede ocurrir en cualquier nivel de una pila de aplicaciones, incluida la plataforma, el servidor web, el servidor de aplicaciones, la base de datos, el marco y el código personalizado. Los desarrolladores y administradores de sistemas deben trabajar juntos para asegurarse de que la pila entera esté configurada correctamente.