UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Universidad Autónoma de Nuevo León

Facultad de Ciencias Físico Matemáticas

Licenciatura en Seguridad en Tecnologías de Información

Diseño Orientado a Objetos

Maestro: Miguel Salazar

Ensayo

Nombre: Daniel de la Rosa Rodríguez

Matrícula: 1666385

19 de agosto de 2017, Cd. Universitaria, San Nicolás de los Garza, Nuevo León

Los softwares de aplicación son programas diseñados para usuarios, estos se utilizan para facilitar tareas específicas dentro del sistema computacional, como pueden ser aplicaciones ofimáticas (procesador de texto, hoja de cálculo, presentaciones, sistema de gestión de DB), de sistema de control y automatización industrial, educativo, medico etc.

Según las funciones de estas aplicaciones se pueden clasificar en dos categorías:

- ***Programa básico o de utilería***

  Cuyas aplicaciones tienen como propósito mejorar el desempeño del sistema computacional

- ***Programas de productividad***

  Son las aplicaciones que facilitan, agilizan y mejoran la ejecución de ciertas tareas del usuario:
  - **Procesadores de texto**: sirven para editar y/o procesar texto
  - **Hojas de cálculo**: aplicaciones para introducir, calcular, manipular y analizar conjuntos numéricos
  - **Hojas de presentación**: estas sirven para que el usuario cree y edite presentaciones con imágenes, texto, sonido y hasta video
  - **Web**: aplicaciones para acceder a un servidor web a través de internet mediante un navegador
  - **Administradores de DB**: sirven para acceder, almacenar, procesar y administrar grandes colecciones de datos
  - **Móviles**: estas aplicaciones exclusivas para dispositivos inteligentes móviles

Cada una de estas aplicaciones tiene una tarea asignada por hacer según las necesidades del usuario. Pues también existen tipos de software como los son los softwares de programación que sirven para el desarrollo de aplicaciones y software de sistema que son los controladores del sistema para la ejecución de sectores del dispositivo y administración de recursos y brindarle al usuario una interfaz gráfica para controlar el sistema.

Dentro de las aplicaciones web se pueden ver infinidades de vulnerabilidades:

1. **XSS (Cross Site Scripting)**:
   Es un fallo de seguridad en aplicaciones web que compromete la seguridad del cliente. Es un ataque que consiste en inyectar código HTML y/o JavaScript en una aplicación con el objetivo de que el cliente ejecute el código al momento de ejecutar la aplicación. Se da cuando una aplicación web permite inyectar código en la página. Esto se puede lograr por medio de formularios o URL.

2. **CSRF (Cross Site Request Forgery)**:
   Es similar al XSS, salvo que este se basa en explotar la confianza del usuario que tiene en un sitio web. Esta trata que el usuario es forzado a ejecutar acciones no deseadas en la aplicación en la que se encuentra autenticado. Habitualmente se usa la ingeniería social como apoyo, malintencionando a la persona para forzarla a que ejecute acciones que el mismo usuario no quiere hacer, como puede ser la ejecución de código de manera remota.

3. **Buffer Overflow**:
   Como resultado de esta vulnerabilidad es que la información en pila es sobrescrita incluyendo las funciones de punto de retorno, los datos establecen el valor del retorno, así que la función regresa. Transfiere el control al código malicioso contenido en los datos del atacante.

4. **SQL Injection**:
   Consiste en insertar una consulta SQL a través del intercambio de datos entre el cliente y la aplicación. Este ataque es capaz de leer cualquier dato de la DB, modificarlos, ejecutar operaciones como administrador, recuperar contenido de un archivo, etc. y esto se debe a que se encuentra en sistema administrador del DBSM y en algunos casos ejecuta comandos en el SO.

5. **Database**:
   Estas son vulnerables si no se tiene una buena configuración de seguridad y están propensas al SQLi si no tiene una buena validación dentro de la aplicación con la que interactúa.

Referencias:

Políticas y buenas prácticas de seguridad en servidores web del CDMIT, vulnerabilidades en aplicaciones web, capitulo 2. UNAM.