FCFM
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Nombre: ALEXIS DURAN TIJERINA	**Matrícula**: 1479832
Unidad de Aprendizaje: Diseño Orientado a Objetos	**Nombre del profesor**: Miguel Salazar
Módulo: Week1	**Actividad**: Tipos de Aplicaciones y vulnerabilidades
Fecha: 18/08/2017	
María José Montes Díaz. (Abril 4, 2017). Las principales vulnerabilidades web. 19/08/2017, de Hacking-Etico Sitio web: https://hacking-etico.com/2017/04/04/las-principales-vulnerabilidades-web/	

Tipos de aplicaciones

Una forma de explicar a que se refiere el amplio campo de las aplicaciones porque hay muchos tipos de aplicación, que se comienza desde una aplicación a nivel hardware hasta una aplicación que el usuario visualiza desde su smartphone, para esto se lleva a la programación en muchos lenguajes, pero eso ya es otro tema.

Aplicación de tipo navegador web

Es un software, aplicación o programa que permite el acceso a la Web, interpretando la información de distintos tipos de archivos y sitios web para que estos puedan ser visualizados. Las características de este tipo de aplicación son que hay muchos tipos de navegadores como por ejemplo safari y cada una de ellas tienen muchas características, pero en general serian que tienen cada una de ellas un motor de búsqueda, los tipos de visualización y extensiones para cada una de estas aplicaciones como Firefox que tiene muchos tipos.

Aplicación de desarrollo de multimedia

Para la gestión de imágenes, vídeos o música. También de animación de gráficos imágenes o vídeos, editores vectoriales, secuenciadores musicales e Hipermedia. Tienen muchas características estos tipos de aplicación ya que se requieres muchas herramientas para la creación o el diseño de lo antes mencionado.

Software de simulación

Como simuladores científicos, sociales o de guerra, de emergencia, de vehículos o de vuelo. Estos tienen de características diferentes tipos de hardware para simular un entorno ya sea de alguna guerra como tipos de armas y por ejemplo un avión y controles para la simulación de la nave, sus botones y demás controles.

Aplicaciones móviles.

Estos tipos de aplicación que son para los smartphones y que hay una gran variedad de ellas y sus usos son muy extensos ya que hay muchas, desde el entretenimiento hasta de tipo oficina para administración y hasta diseño. Sus características o lo que les da valor son precisamente el valor de la información que contienen, la usabilidad ya que sea sencilla de usar y fácil entendimiento, diseño como la información relevante en la parte superior, soporte web, abiertas así que se puedan abrir y ejecutar en cualquier dispositivo.

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. Las características de estas aplicaciones son la administración tanto de recursos como de información de la compañía o de trabajo normal, facilitar los procesos de trabajo, aumentar la productividad y así aumentar una producción en la empresa.

FCFM
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Vulnerabilidades en aplicaciones WEB

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

Solución: Validar y limpiar todo lo que el usuario ingrese a nuestro sistema antes de realizar cualquier proceso además de usar Prepared statements y stored procedures.

Secuencias de comandos en sitios cruzados (Cross-site scripting, XSS).

Esta falla permite desplegar en el navegador datos no confiables proporcionados por usuarios, generalmente inyectando código javascript malicioso. Estos datos pueden secuestrar tu sitio web, permitiendo que tus usuarios sean redireccionados a sitios maliciosos o descarguen malware.

Solución: Validar y escapar cualquier dato a ser impreso en tu sitio, trata siempre de usar herramientas de templates los cuales te permitan optimizar este proceso (Freemarker o Smarty).

Autenticación rota. Se presenta cuando es posible suplantar la identidad del usuario al obtener acceso a datos como contraseñas o identificadores. Un ejemplo es poder modificar el id de la sesión en la cookie y obtener así acceso como un administrador o cambiar el perfil de acceso.

Solución: Verificar los procesos de autenticación, usar mecanismos y librerías ya existentes. No guardar información sobre permisos o identidad en cookies.

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.

Solución: Controlar el flujo de los procesos usando tokens únicos por sesión y por solicitud

Referencias directas e inseguras a objetos.

Exponer referencias a objetos de implementación interna como archivos, directorios y base de datos por lo que 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.

Solución: Usar siempre controles de acceso y no ofrecer datos sobre la implementación interna.