LSTI

Diseño orientado a objetos

Carlos Abel Lugo Gonzalez
FCFM Ciudad Universitaria

Asignación de la Semana 1

Ensayo sobre aplicaciones de software.

Software de aplicación

Las funciones de una aplicación dependen de su propósito, según el cual pueden clasificarse en dos categorías:

Programas básicos (o utilitarios)

Son aplicaciones cuyo propósito es mejorar, en alguna forma, el desempeño del ordenador.

Programas de productividad

Son aplicaciones cuyo propósito es facilitar, agilizar y mejorar para el usuario, la ejecución de ciertas tareas.

Aplicación móvil

¿Qué es una aplicación móvil?

Una aplicación móvil es un programa que usted puede descargar y al que puede acceder directamente desde su teléfono o desde algún otro aparato móvil – como por ejemplo una tablet o un reproductor MP3.

Aplicaciones de escritorio

Una aplicación de escritorio es aquella que se encuentra instalado en el ordenador o sistema de almacenamiento (USB) y podemos ejecutarlo sin internet en nuestro sistema operativo, al contrario que las aplicaciones en la nube que se encuentran en otro ordenador (servidor) al que accedemos a través de la red o internet a su software.

Aplicaciones de Consola

Se puede definir una aplicación de consola como aquella que se ejecuta en una ventana de MS-DOS, es decir, en línea de comandos.

Lo más común dentro del desarrollo bajo la plataforma .Net es la creación de aplicaciones Web o aplicaciones Windows sin embargo la mejor forma de sentar unas bases firmes acerca de la programación orientada a objetos es comenzar construyendo aplicaciones sencillas de consola.

Aplicación web

Las aplicaciones web reciben este nombre porque se ejecutan en el internet. Es decir que los datos o los archivos en los que trabajas son procesados y almacenados dentro de la web.

El concepto de aplicaciones web está relacionado con el almacenamiento en la nube. Toda la información se guarda de forma permanente en grandes servidores de internet y nos envían a nuestros dispositivos o equipos los datos que requerimos en ese momento, quedando una copia temporal dentro de nuestro equipo.

Estos grandes servidores de internet que prestan el servicio de alojamiento están ubicados alrededor de todo el mundo, así hacen que el servicio prestado no sea tan costoso o gratuito en la mayoría de los casos y extremadamente seguro.

Ejemplo de aplicaciones web:

- Correo electrónico

Servicios como Gmail y Yahoo! se ejecutan en tu buscador y realizan las mismas tareas de programas de correo electrónico como Microsoft Outlook.

Después de hacer el ingreso a un servicio de correo electrónico online, puedes utilizarlo inmediatamente, sin necesidad de instalar algún programa en tu equipo.

- Google Docs

Esta conjunto de programas ofimáticos. Se ejecutan desde tu navegador y funcionan de igual manera que los programas que hacen parte del paquete de Microsoft Office, ya que puedes utilizarlo para crear documentos, hojas de cálculo, presentaciones y más.

- Facebook

Permite crear un perfil en línea e interactuar con tus amigos. Como los perfiles y conversaciones están en constante evolución, Facebook utiliza tecnología de aplicaciones web a través del sitio para mantener la información actualizada.

¿Cómo funcionan las aplicaciones web?

Cuando utilizas una aplicación web estás trabajando desde tu computador o dispositivo móvil, pero la mayor parte del procesamiento se hace dentro de en una red de servidores.

Estos servidores pueden unir todo su poder de procesamiento con el fin de tramitar solicitudes de todo el mundo, y a su vez, utilizan servidores especializados para almacenar los datos con los que estás trabajando, así como los datos de los demás usuarios.

Como todo esto sucede sin problema ni demora alguna, pareciera que la aplicación se está ejecutando dentro de tu equipo.

Ventajas de las aplicaciones Web:

1. Muchas aplicaciones web son gratuitas.
2. Puedes acceder a tu información en cualquier lugar y momento.
3. No dependes de tu computador o de algún equipo específico ya que el contenido está almacenado en la web.
4. Muchas de las aplicaciones web permiten que varias personas trabajen simultáneamente en ellas.
5. Los documentos y archivos no se te van a perder ni borrar a menos que tú así lo quieras.

Riesgos

Cuando se va a atacar un sistema, lo último que se quiere es que salten todas las alarmas. Es por eso que usar fuentes online es una buena herramienta. Se puede utilizar hacking de buscadores para localizar URLs con paso de parámetros, para comprobar si éstos están correctamente validados, para buscar correos electrónicos u otra información que pueda extraerse de un determinado sitio: ficheros de backup o de configuración que hayan quedado indexados, etc.

METADATOS

Otra fuente de información importante son las fugas de información que se producen por culpa de los metadatos, que van incluidos en los documentos que se publican en Internet.

Con estos datos, es posible conocer nombres de usuario, equipos, sistemas operativos, versiones de software, etc. que se utiliza en la organización.

Si no se tiene cuidado, con estos datos es posible incluso realizar un mapa interno de la organización, desde los equipos cliente, con los usuarios de cada uno, hasta los servidores de los que se dispone, pasando por impresoras, etc.

Es por esto que es muy importante, antes de subir un documento o publicarlo, realizar una limpieza de metadatos del mismo.

Herramientas como FOCA, son de gran utilidad para comprobar qué información sensible estamos publicando, sin que seamos conscientes.

Vulnerabilidades web

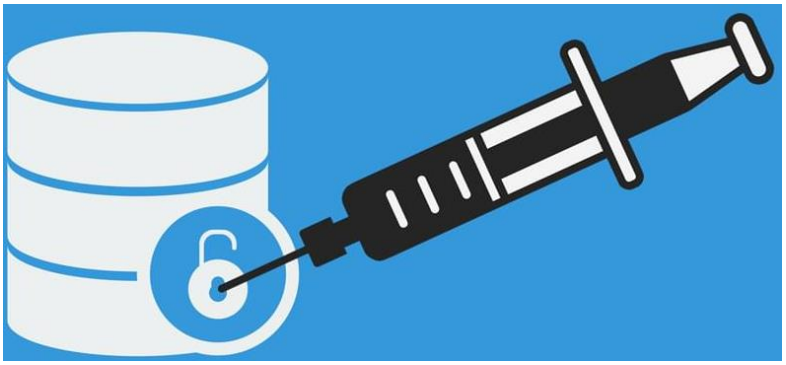
Una vez que hemos visto lo importante que es la información acerca de nosotros que tenemos publicada, y que debemos intentar controlar, veamos qué vulnerabilidades más importantes puede presentar un sitio web.

En primer lugar nos situamos en el escenario, tenemos una plataforma montada sobre un sistema operativo, con su motor de base de datos, lenguajes, normalmente interpretados, certificados, etc. Ésta es la parte del servidor web en sí. Las vulnerabilidades que tendrá desde ese punto de vistas serán:

-Configuración débil, por defecto o mal configurado. Esto suele producirse por intentar desplegar el servicio lo más rápido posible o por una confianza excesiva en el software utilizado, incluso por desconocimiento. Cuando se expone a Internet un sistema con su configuración por defecto, si se encuentra una vulnerabilidad en el mismo, el exploit por defecto funcionará. Es

necesario revisar el servicio a desplegar y buscar una configuración suficientemente fuerte.

– Comunicación insegura entre cliente y servidor. Es muy importante que la comunicación entre cliente y servidor esté cifrada, sobre todo, cuando se trata de envíos de formularios, por ejemplo, para autentificarse en sitio web. En muchas ocasiones, se configura el sitio web para usar cifrado, con una configuración débil, permitiendo protocolos inseguros, como SSLv2 y SSLv3, o suites de cifrado vulnerables, como MD5. Esto dará una falsa sensación de seguridad, el cliente verá que hay un certificado, que el sitio web, aparentemente está cifrado, y, sin embargo, por culpa de los protocolos permitidos, podría ser relativamente fácil descifrar esta comunicación. Es por ello que es necesario revisar el estado de la calidad en la configuración de nuestros certificados.



– Software desactualizado. Una vez desplegado el sistema, independientemente de que se hiciese el trabajo correctamente, pasado el tiempo, el software se des actualiza. Se localizan vulnerabilidades, se corrigen en versiones posteriores, etc. Es necesario llevar un control de las versiones utilizadas, así como mantener el software actualizado, en el menor tiempo posible, desde que se libera una nueva versión. En caso contrario, al cabo de un tiempo, nuestro sistema será vulnerable y existirán exploits públicos que permitirán atacarlo.

Vulnerabilidades de la aplicación, estas vulnerabilidades son propias de la aplicación que se quiere desplegar, del código de la misma. Independientemente de que la plataforma sobre la que despleguemos la aplicación esté correctamente fortificada, si la aplicación posee vulnerabilidades, corremos el riesgo de que puedan encontrarse y ser atacadas.

Las vulnerabilidades más comunes en una aplicación web son:

1. Cross-Site Scripting (XSS).

Esta es una vulnerabilidad o, mejor dicho, un conjunto de vulnerabilidades, que permiten, utilizando los parámetros de entrada de la aplicación, modificar y añadir código a la misma.

Son vulnerabilidades que se encuentran en el servidor, pero que están destinadas a atacar al cliente.

Generalmente, se necesita que el cliente sigua un enlace de la aplicación, en el que se ha modificado algún parámetro, para permitir añadir código, que se ejecutará en el navegador del cliente.

Normalmente, el código inyectado será html o JavaScript y la intención será un robo de cookies del cliente, predicción del id de sesión, etc.

Esta vulnerabilidad se aprovecha de la confianza en el cliente en el sitio web: Verá que es el dominio de la aplicación y que, al seguir el enlace, llega realmente al sitio web que quería, no hay suplantación del mismo.

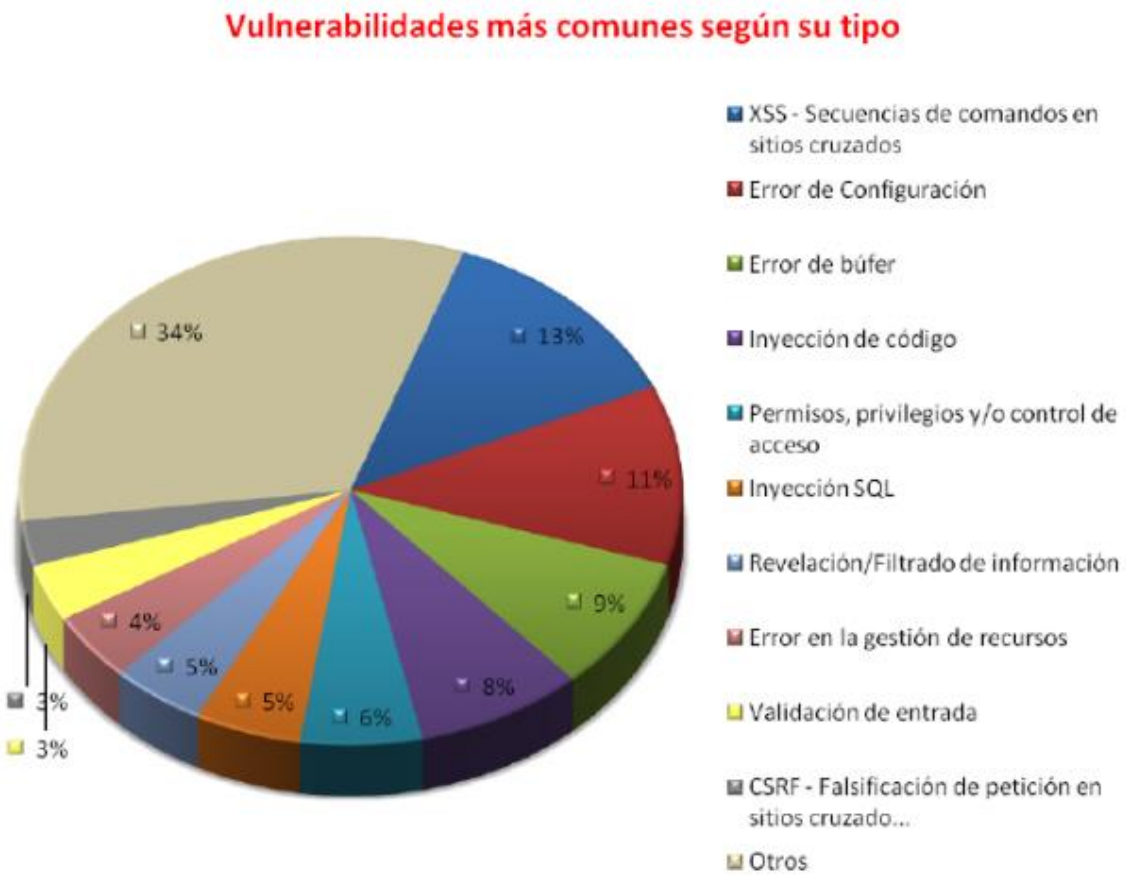
2. Cross Site Request/Reference Forgery (CSRF)

Esta vulnerabilidad es una evolución de los XSS. En este caso, se va a explotar la confianza en el servidor sobre el cliente. Es decir, nos haremos pasar por un cliente legítimo, utilizando datos parciales del mismo.

Esta vulnerabilidad está presente en formularios. Cuando estos se envían al servidor, es necesario asegurarse que la petición es legítima y debemos asegurarnos que el cliente ha realizado la petición, realizando los pasos previos necesarios.

3. SQL INJECTION

Si los ataques XSS son peligrosos, ya que pueden provocar un robo de sesión, los SQLi son aún más porque permiten acceder y manipular la BBDD. La idea es modificar las consultas que hace la aplicación a la base de datos, aprovechando las entradas de usuario a la aplicación.



Finalmente es aconsejable realizar auditorías de seguridad con periodicidad adecuada. Asimismo, es bueno recordar que la seguridad debe ser gestionada y es por esto que desde ESET Latinoamérica contamos con

la unidad ESET Security Services destinada a brindar auditorías de seguridad.

Bibliografía

https://www.consumidor.ftc.gov/articulos/s0018-aplicaciones-moviles-que-son-y-como-funcionan

https://es.wikipedia.org/wiki/Aplicaci%C3%B3n de escritorio

https://desarrolloweb.com/articulos/1354.php

https://www.mastermagazine.info/termino/3992.php

https://support.kaspersky.com/mx/614

https://www.gcfaprendelibre.org/tecnologia/curso/informatica basica/aplicaciones web y todo acerca de la nube/3.do

https://hacking-etico.com/2017/04/04/las-principales-vulnerabilidades-web/

https://www.welivesecurity.com/la-es/2012/07/31/vulnerabilidades-estadisticas-e-impacto/