SEGURIDAD EN APLICACIONES WEB

AUTOR: ANGEL ALBERTO VARÓN QUIMBAYO

San Marcos

ÍNDICE

INTRODUCCIÓN

El constante avance tecnológico, la globalización de mercados, la alta demanda de aplicaciones web y el afán de las organizaciones por ser competentes exige que los profesionales de TI desarrollen a diario aplicaciones web donde exigen que éstas garanticen la seguridad de la información, es por esto, que es de vital relevancia que conozcamos de temas tan importantes como: vulnerabilidades de las aplicaciones web, autenticación/autorización, anatomía de un ataque a una aplicación web, OWASP, clasificación de amenazas, herramientas de intrusión, técnicas de ataque directo al usuario, debilidades de las aplicaciones web, análisis de técnicas de defensa directa y prevención de ataques, estos conocimientos le permitirán generar estrategias para desarrollar aplicaciones web más confiables.

OSWASP es un proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables. Todas las herramientas, documentos, foros y capítulos de OWASP son gratuitos y abiertos a cualquiera interesado en mejorar la seguridad de aplicaciones. Abogamos por resolver la seguridad de aplicaciones como un problema de usuarios, procesos y tecnología porque las soluciones más efectivas incluyen mejoras en todas estas áreas. a partir de lo cual se plantea la siguiente pregunta, ¿Qué tan importante es tener conocimientos sobre Seguridad en Aplicaciones WEB y cómo los aplicó en el campo laboral?

Seguridad en Aplicaciones WEB

Una aplicación web que sea vulnerable, fácilmente puede ser aprovechada por los hacker o personas mal intencionadas, lo que podría generar un caos en el servidor, ya que provocaría posibles daños al servidor web, o pérdida de información almacenada en la base de datos o en el mismo servidor.

La fragilidad de un sistema de información hace parte de una falla: en el diseño, implementación, operación o controles dentro de un proceso, esto permitiría que se violara la seguridad del sistema.

Figura 1. Vulnerabilidades de las aplicaciones web.
Fuente: http://kybalion.es/wp-content/uploads/vulenrabilidad-informatica-contrasenas.jpg

Es importante tener en cuenta que todo sistema de información tiene cierto nivel de vulnerabilidad y que estos, en ocasiones se presentan por la misma complejidad de la aplicación, el desconocimiento o el costo que tiene el monitoreo y control.

Las aplicaciones web deben contar con niveles altos de seguridad, hoy día muchas organizaciones realizan transferencias a través de internet, para facilitar la comunicación con sus clientes o ciudadanos, tales programas vienen asociados con muchas vulnerabilidades de seguridad, estas son concebidas de tal manera que es casi inútil estimarlas durante el desarrollo de las aplicaciones siendo la seguridad el principal objetivo a conseguir de quienes administran recursos y datos para defenderlos de los atacantes.

Causas de las vulnerabilidades:

- Debilidad en los protocolos de red, algunos se han diseñado sin prever un mal comportamiento de los usuarios en internet, que fácilmente pueden provocar

anomalías en la comunicación, un ejemplo claro es: un ataque de denegación (Dos).

- Errores de programación: consiste en la falla de codificación en la programación, uno de los casos más comunes son los parches y las actualizaciones de seguridad, las mayores dificultades se presentan cuando se han instalado parches en servidores cuyas versiones vienen en idioma distinto al inglés.

- Configuración inapropiada: esto se da muchas veces porque la documentación del sistema es poca, inclusive inapropiada, además cuando se configura una aplicación con las opciones por defecto de fábrica, algunos dispositivos y servicios son pocos seguros.

- Desconocimiento por parte de los usuarios: en una organización se puede contar con todas las herramientas y técnicas para prevenir las vulnerabilidades (cortafuegos, antivirus, sistemas de detección), pero sí contamos con recurso humano, mal intencionado, desleal o se cuenta con personas que desconocen la aplicabilidad de técnicas o el uso de estas herramientas, por obvias razones vamos a estar expuestos.

- Herramientas en internet: hoy día encontramos muchos tutoriales en la web sobre herramientas que facilitan los ataques web, con el rótulo de hacking ético, encontramos el link donde descargarlas, software libre, tutoriales y manuales, sin ningún tipo de responsabilidad, esto permite que muchas personas se sientan seducidas a realizar pruebas, y por este motivo se han incrementado los delitos informáticos, es importante resaltar que inicialmente se inicia por pura curiosidad, pero si la persona no controla sus impulsos esto termina en delito.

Pero para evitar este tipo de riego, se contemplan tres normas que fortalecidas continuamente servirán para reducir falencias ligados al uso de la web para negocios y al uso privado, estas son:

1. Control de acceso a la información delicada: los desarrolladores de aplicaciones deben evitar poner información delicada en cualquier sitio web de acceso libre, en un registro de internet.

2. En el ciclo de vida del desarrollo del sistema instaurar pruebas de debilidades: para permitir conocer la vulnerabilidad en seguridad que admite a los intrusos entrar a la aplicación web y al BD para implementar un sistema o cambio en el ámbito de producción.

3. Fundar un Control excesivo sobre la entrada: fijación de validación y revalidación en los controles de entrada ya que nunca se debe depositar confianza en la difusión de datos entre browser, servidor web y hardware de red.

Los resultados más recientes de testeos en aplicaciones web han dado como conclusión grados altos de afectación en ellas, dándose así niveles de vulnerabilidades en las aplicaciones web, que a continuación, analizaremos:

- Fragmentación de la autenticación: incluye distintos defectos en el inicio de sesión de la aplicación donde admite que el intruso acceda a las contraseñas y lance un inminente ataque.

- Fragmentación de los controles de acceso: fallos en la protección de la aplicación, en donde concede al intruso visualizar datos débiles de otro usuario alojado en el servidor y también llevar a cabo actos privilegiados.

- Inyección de SQL: concede al intruso provocar interferencia entre la aplicación, su interacción y la base de datos, haciendo posible que este bloquee la lógica y realice comandos sobre el servidor de base de datos.

- Cross-site scripting: permite que el intruso llegue a los datos de los usuarios donde ejecuta movimientos ilegales a nombre de estos o desarrollando ataques en contra de los mismos.

- Fuga de información: admite que el intruso desencadene agresiones en contra de la aplicación cuando esta da a conocer información sensible por medio de una falla consecuente de un defecto.

Figura 2. Autenticación/autorización.
Fuente: https://bit.ly/2zpcVDB

La autenticación de usuarios permite a los sistemas informáticos apropiarse con una seguridad lógica de que quien se está conectando es quien dice ser, para que posteriormente las acciones que se ejecuten en el sistema puedan ser reseñadas luego a esa identidad y fijar los medios de autorización y auditoría pertinentes.

El primer componente necesario por tanto para la autenticación es la existencia de identidades unívocamente identificadas con un registro, el reconocimiento de usuarios puede ser de varias maneras siendo la más conocida el login o serie de caracteres.

Existen ciertos pasos en el proceso de autenticación como lo son:

- Solicitud de acceso al sistema por parte del usuario.
- El sistema solicita al usuario documentación para identificarlo.
- El usuario proporciona documentación para que se le identifique y constate la autenticidad de la identificación.
- El sistema según sus normas corrobora si la identificación es suficiente para dar acceso o no al usuario.

Algunos ejemplos del control de acceso que conllevan a una autentificación pueden ser:

- Retirar dinero de un cajero automático.
- Control de un computador remoto sin Internet.
- Uso de un sistema Internet banking.

Hoy día se utilizan funciones y esquemas de autenticación como la autenticación mediante el cifrado de mensajes con criptografía.

La criptografía se usa no sólo para proteger la confidencialidad de los datos, sino también para garantizar su integridad y autenticidad, existen tres tipos de criptografía, los cuales se enuncian a continuación:

Criptografía simétrica	(Clave privada) se usa para cifrar y descifrar un documento, las dos partes que se comunican emisor y receptor deben acordar la clave a usar manteniendo está en secreto.
Criptografía asimétrica	(Clave pública) este tipo de cifrado utiliza dos claves distintas Una es la clave pública y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella.
Criptografía híbrida	Soluciona los inconvenientes de privacidad que podría considerar el uso del cifrado simétrico y el tiempo de procesado del uso del cifrado asimétrico, de esta manera aliar las ventajas de las dos para emplearlas.

Tabla 1. Tipos de criptografía
Fuente: propia

Video

Se recomienda ver el siguiente video:

Seguridad en aplicaciones

https://vimeo.com/240863734

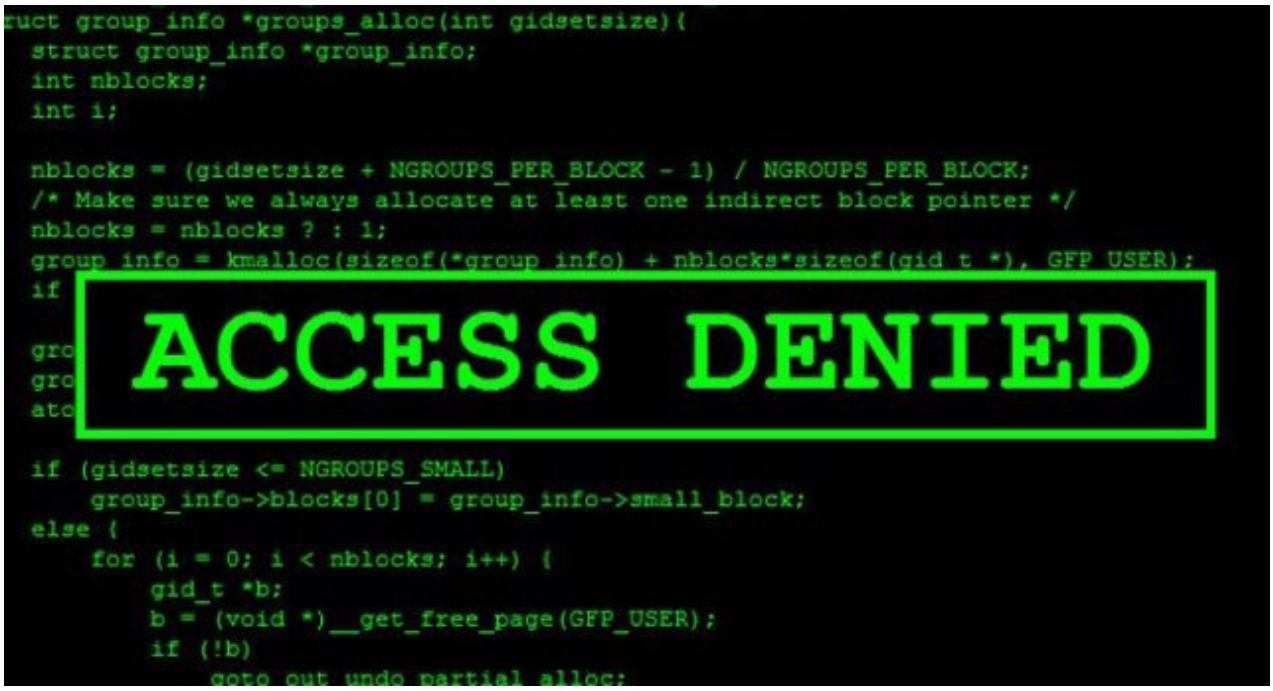

Figura 3. Anatomía de un ataque a una aplicación web
Fuente: https://bit.ly/2P2T47N

Los desarrolladores al momento de programar aplicaciones web se concentran en las funciones de este y no se enfocan lo suficiente en la seguridad, allí es cuando los intrusos o atacantes sacan provecho, por eso conocer la anatomía que constituye un ataque informático a una aplicación web nos da una visión sobre la forma de pensar de los atacantes y a no menospreciar su mentalidad, a continuación, se aclarara este tema:

Anatomía:

- Reconocimiento: examina el posible perjudicado a través de métodos que generan sólo los datos necesarios para atacar.
- Inspección: los datos son usados para obtener otros datos notables como: contraseñas, dirección IP, host y muchos más.
- Conseguir acceso: estudio de vulnerabilidades del sistema, admitiendo la preparación del ataque.
- Sostener el acceso: el intruso usa elementos como: gusanos y puertas traseras etc., para continuar fijamente con el acceso y así usarlo cuando se quiera.
- Eliminación de huellas: una vez logre sus propósitos el intruso eliminará cualquier señal de lo que hizo, para no ser descubierto.

Lectura recomendada

Se invita al estudiante a realizar la siguiente lectura:

Amenazas Informáticas y Seguridad de la Información

Tarazona, C.

Los ataques de aplicaciones web pueden dañar varias funciones dentro de un sitio, pretendiendo atacar a la misma aplicación web o hacer reenvíos lógicos al BD, si se guardan datos confidenciales en un sitio web propio o se posee uno comercial los ataque enviados tendrán efectos negativos, no solo en el rendimiento comercial sino también en el buen nombre, ahora conozca cuáles son:

Existen tres tipos de ataques:

1. De Inyección SQL: consultas ficticias enviadas al BD usadas para introducirse en las aplicaciones y BD principales.
2. Filtro de scripts de sitios (XSS) donde las debilidades del XSS admite a que los atacantes filtren un script que se ejecuta en el navegador del usuario.
3. Ejecución de archivos maliciosos: los atacantes incluyen datos y código adverso por medio de la obtención de debilidades y la instalación de archivos remotos.

Figura 4. OSWASP.
Fuente: https://bit.ly/2Q2o2sR

OWASP es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro, se inició ayudando a las organizaciones que utilizaban tarjetas de crédito y débito para proteger los datos sensibles asociados a las cuentas de los clientes, surge como síntesis de distintos programas que las marcas de tarjetas utilizaban para proteger la información.

Video

Se recomienda ver el siguiente video:

Seguridad en aplicaciones

https://vimeo.com/240861005

Este proyecto contempla: requerimientos de gestión de seguridad, políticas, procedimientos, arquitectura de red, diseño y desarrollo de software y medidas de protección de datos críticos contemplando las siguientes exigencias:

- Desarrollar y mantener una red segura.
- Proteger los datos del titular de la tarjeta.
- Programa de administración de vulnerabilidades.
- Implementar medidas sólidas de control de acceso.
- Supervisar y evaluar las redes con regularidad.
- Mantener una política de seguridad de la información.

Además de esto proporciona los siguientes documentos de consulta:

1. DBMS Fingerpriting.
2. Testing Oracle.
3. Testing SQL Server.
4. Testing MySQL.
5. Testing PostgresSQL.
6. LDAP segurity testing.

Se cuenta con una serie de herramientas para probar la penetración, encontrar y explotar inyecciones SQL en una aplicación WEB, las cuales se mencionan a continuación:

1. SQL Ninja.
2. SQL map.
3. OWASP SQLiX.
4. Scuba.
5. Squid SQL Injection Digger.
6. SQLDumper.
7. SQL Power Injector.
8. BobCat.

Además de esto, este proyecto cuenta con transport layer protection cheat sheet (Capa de protección de transporte hoja de trucos), que busca proporcionar protección de la capa de transporte con SSL/TLS, permitiendo la protección de la capa del transporte para el backend y otras conexiones aplicando:

- Beneficios.
- SSL vs. TLS.
- Diseño de servidor Segure.
- Certificado de servidor y configuración de protocolo.
- Configuración de Cliente (Navegador).
- Control adicional.

Adicionalmente, se proporciona una guía de criptografía: para asegurar que se dé uso la criptografía para proteger la seguridad de la integridad y confidencialidad de la información confidencial del usuario.

Usos

- Autenticación.
- No repudio.
- Confidencialidad.
- Integridad.
- Algoritmos criptográficos.
- Almacenamiento de claves.

Objetivos:

- transmisión segura, uso de tokens en los procesos de autenticación, generación segura de UUID.
- Contiene un mapeo general sobre prácticas de desarrollo seguro de software.
- Utiliza un formato de checklist lo que permite de manera fácil integrarlo al ciclo de vida de desarrollo de software.
- Se enfoca en garantizar la definición de adecuados requerimientos de seguridad, en lugar de la identificación de vulnerabilidades o ataques.
- Incluye una introducción a los principios de software de seguridad de términos claves.

Contenido de la guía de revisión de código OSWASP

- Revisión del código Security en el SDLC.
- Revisión de código y PCI DSS.
- Revisión por control técnico: autenticación, autorización, ampliación de la sesión, etc.
- Metodología.
- Código de rastreo.
- Revisiones del código y PCI.
- Ejemplos de técnica.
- Ejemplos por vulnerabilidad.

- Buenas prácticas para lenguajes específicos.
- Ejemplos de informes.
- Autenticación de códigos.

Clasificación de amenazas

Esta clasificación de amenazas a la seguridad evoluciona tan rápido como la tecnología que intentan comprometer, por esto, los socios de WASC Web Application Security Consortium crearon este proyecto para desarrollar y promover una terminología estándar para la industria que describa estos asuntos, por esto, desarrolladores de aplicaciones, profesionales de la seguridad, diseñadores de software y auditores, estarán en la capacidad de disponer de un lenguaje consistente para tratar los aspectos relacionados con la seguridad web, una parte importante del proceso de programación de aplicaciones más seguras consiste en ser capaz de anticipar las amenazas que se puede sufrir, algunas de las amenazas son las siguientes:

- Autenticación insuficiente.
- Autorización insuficiente.
- Desbordamientos de enteros.
- Insuficiente protección en la capa de transporte.
- Inclusión de archivos remotos.
- Formato de cadenas.
- Desbordamiento de búfer.
- Cross-Site Scripting y Cross-Site Request Forgery.
- Denegación de Servicio DOS.
- Fuerza bruta.
- Configuración errónea del servidor y de la aplicación.
- Indexación incorrecta de directorios.
- Permisos indebidos al sistema de archivos.
- Predicción de credenciales y/o sesión.
- Inyección de SQL e inyección SSI.
- XML inyección.
- inyección XPth.

Figura 5. Amenazas
Fuente: https://bit.ly/2yGtLxY

Herramientas de intrusión

Las herramientas de intrusión son aquellas que permiten sabotear un sistema o aplicación, incluyendo el robo de información de maneras diferentes. Existen distintos métodos que permiten la infiltración a un sistema informático que busca cómo proteger el sistema.

Figura 6. Intrusión
Fuente: https://bit.ly/2AB36Ek

Normalmente un hacker que pretenda realizar una infiltración inicia con la comprobación de fallas en la misma, es decir evidenciar las debilidades que afecten los sistemas de seguridad como: protocolos, seguridad o aplicaciones.

Existen estructuras que explican la misma como un proceso cíclico iniciando así:

- Recogida de información.
- Análisis.
- Reparación de fallas.
- Intrusión.
- Extensión de privilegios.

- Poner en riesgo.
- Eliminación de rastros.

Instrucción

Se invita al estudiante a realizar el recurso de aprendizaje: infografía.

Los pasos que tiene un hacker para hacer un intento de intrusión son los siguientes:

1. Ingeniería social, consta de sacar información con el contacto directo de los usuarios como: claves de accesos y demás. Esto pasa normalmente, cuando se hace pasar como administrador.
2. La consulta del directorio o de los servicios de mensajería o de uso compartido de archivos permite encontrar nombres de usuario válidos.
3. Se aprovecha de la vulnerabilidad de los comandos Berkeley.
4. Irrumpir por la fuerza para obtener claves y accesos o una lista de estos.

Es muy importante adquirir conocimientos sobre seguridad informática con el objeto de verificar la cantidad de pruebas, intentos o técnicas de intrusión se pueden aplicar, esto permite desarrollar una capacidad adecuada para desarrollar aplicaciones más seguras, sin embargo, es necesario entender que los intrusos son personas que también se capacitan y desarrollan nuevos mecanismos para atacar y de esta forma vulnerar los sistemas de información de las organizaciones, por este motivo, es que últimamente ha cogido auge lo que llamamos hacking ético o sombrero blanco (pentester) examen de penetración, esto lo hace la persona encargada de realizar la auditoría a los sistemas de información, lo que fácilmente le permite encontrar errores, y de esta forma, poder subsanarlos de la mejor forma para impedir pérdida de información, es importante que se tenga conciencia que no todos los hacker son ciberdelincuentes.

Sino que opuestamente desempeñan un papel importante brindando ayuda sobre seguridad en las compañías. Por otro lado, existe black hat o hacker negro que lo que hace es vulnerar los sistemas en las organizaciones con el único objetivo de probar su capacidad.

Los hackers y crackers son personas expertas que conocen el área tecnológica e informática, pero existe una gran diferencia entre los dos: que los hacker crean y modifican software y hardware de computadoras para desarrollar nuevas funciones o adaptar las antiguas, sin que estos cambios afecten al usuario del mismo y el cracker, es un ciberdelincuente que emplea sus conocimientos para intervenir sistemas, descifrar claves y contraseñas de programas y algoritmos de encriptación, robar datos personales, o cometer otros ilícitos informáticos.

Técnicas de ataque directo al usuario

Una técnica de ataque es aquella que tiene como fin violar la seguridad de un sistema, hay variedad de técnicas de ataque directo usadas por hackers para obtener beneficios económicos de cualquier usuario y depende de él estar vigilante para no ser víctima, a continuación, se mencionan algunas de ellas:

Troyano o caballo de Troya: son programas aparentemente inofensivos, por medio de este se producen ataques para hacer instalaciones de programas espías dentro del computador afectado, con el cual se hacen cambio de archivos, saqueo de información y recolección de datos personales, entre otras.

Phishing (pesca de datos): esta técnica suplanta la identidad aplicando ingeniería social, capta información bancaria como: claves y el número de tarjeta de los usuarios a través de la sustitución en la imagen de una la entidad financiera.

Spoofing: mediante el uso de técnicas, un atacante, generalmente con usos maliciosos o de investigación se suplanta la identidad de una persona, falsificando el origen de los paquetes, haciendo que la víctima piense que estos son de un host de confianza o autorizado para evitar que sea detectado.

Scam: son técnicas para realizar estafas por medios electrónicos. Uno de los medios más particulares es el correo electrónico fraudulento, el ataque hace alusión a recompensas, herencias de origen desconocido o premios de otros países, los cuales para ser reclamados tienen que dar una suma de dinero inferior a la que se recibirá a cambio.

Ingeniería social: es una técnica que utilizan los delincuentes informáticos para suplantar personas y entidades con el objeto de obtener datos personales, por lo general, estos ataques se realizan mediante: llamadas telefónicas, mensajes de texto o falsos funcionarios, cabe aclarar que lo que se busca son datos importantes para manipularlos y usarlos en contra de la persona, también se busca estafar a éstas con falsos correos que prometen premios.

Se podría nombrar otros tipos de ataques, pero todos en común quieren usurpar la información para encontrar la que represente valor y ganancia para los atacantes, pero para que no logren sus objetivos debemos ser preventivos y realizar algunas tácticas como:

- Instalar y actualizar un antivirus adecuado.
- Ejecutar y activar el Firewall de Windows.
- Usar cortafuegos.
- Actualizar los Drivers del sistema de una fuente confiable.
- Revisar y tener claro la procedencia de los mensajes que recibimos dado que ahí es la principal fuente de envío de virus y software malicioso.

Lectura recomendada

Se invita al estudiante a realizar la siguiente lectura:

Ataques informáticos

Mieres, J.

Debilidades de las aplicaciones web

Las aplicaciones web vienen incursionando con el uso masivo de internet las cuales se utilizan en cualquier tipo de actividad que se quiera hacer comúnmente, las cuales trabajan en un servidor, lo que hace que exista dinamismo para los usuarios haciendo posible que el usuario al momento de la ejecución pueda utilizar cualquier sistema operativo, pero resulta que las aplicaciones cuentan con debilidades, algunas de ellas son:

- Incompatibilidad versiones de navegadores.
- Falta de flexibilidad al cambio tecnológico.
- Imposición de nueva versión.
- Dependencia de red.
- Seguridad.

Entre los ataques cibernéticos podemos encontrar:

- Ataques de inyección: que buscan infiltrarse en las bases de datos para el robo de información y bloqueos a las aplicaciones.
- Ataque al apartado de autenticación y sesiones que busca acceder a la aplicación y usurpar la identidad del usuario.
- Falsificación de sitios, donde se busca que los usuarios caigan en páginas engañosas facilitando su información personal.
- Exposición inadecuada de partes de las aplicaciones: los atacantes aprovechan estas para infiltrarse dentro de la aplicación con las respectivas consecuencias que esto implica.

Teniendo identificadas las debilidades, estas deben analizarse, para evaluar posibilidades y consecuencias de cada circunstancia de riesgo y las de un mayor efecto sobre las aplicaciones, a las que debemos centrar nuestra atención, apoyándonos en el juicio, en la experiencia o en la intuición para decidir cuál es el, esquema correcto de seguridad y configuración que necesitamos para cuidar nuestras aplicaciones y que no sean blanco fácil para intrusos.

Instrucción

Se invita al estudiante a realizar la actividad de aprendizaje: prueba objetiva.

Análisis de técnicas de defensa directa y prevención de ataques

Se debe tener presente la seguridad en el desarrollo de aplicaciones informáticas, debido a que todo programa, sitio web o aplicación es vulnerable a un ataque informático, esto puede traer serios problemas a los encargados del desarrollo debido a que son los responsables de que lo que están realizando sea lo más seguro posible.

Las organizaciones deben mantener segura la información de sus clientes, para esto las diferentes aplicaciones desarrolladas para una organización debe contar con técnicas que permitan la defensa y prevención de ataques informáticos. Estas

son algunas de las técnicas de defensa más usadas:

- Firewall.
- Antivirus.
- Antimalware.
- Servidores de seguridad.
- Consolas de información y seguridad.
- Encriptación de discos duros.
- Manejo de usuario en directorio activo, control de servidores.
- Control en acceso remoto.

Y algunas otras que cumplan la misma actividad de protección ante ataques.

Prevención de ataques

Actualizar el sistema operativo y aplicaciones: para evitar amenazas se debe mantener actualizados los últimos parches de seguridad y software del sistema.

No ingresar a enlaces sospechosos: evitar hipervínculos o enlaces dudosos para prevenir el acceso a páginas web que posean amenazas informáticas. Estos enlaces pueden estar presentes en un correo electrónico, una ventana de chat o un mensaje en una red social.

No acceder a sitios web de dudosa reputación: estar pendientes de mensajes como: descuentos en la compra de productos, premios, ofrecimientos gratuitos, primicias o materiales exclusivos de noticias de actualidad o material multimedia, etc. No ingresar a los que contengan este tipo de características.

Uso de contraseñas seguras: crear estas contraseñas con distintos tipos de caracteres y una longitud no menor a los 8 caracteres, es ideal para contrarrestar los ataques.

Descargar aplicaciones desde sitios web oficiales: para descargar aplicaciones hacerlo desde páginas web oficiales. Esto se debe a que muchos sitios simulan ofrecer programas que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware y descargan el código malicioso al momento que el usuario lo instala en el sistema.

Solo admitir contactos conocidos: evitar acceder a los perfiles creados por los atacantes para comunicarse con las víctimas y exponerlas a ataques, ejemplo de ello, son los clientes de mensajería instantánea como en redes sociales.

Evitar la ejecución de archivos sospechosos: la propagación de malware suele realizarse a través de archivos ejecutables. Si no se conoce la seguridad y la procedencia no realizar la ejecución.

Tecnologías de seguridad: las soluciones antivirus, firewall y antispam representan las aplicaciones más importantes para la protección del equipo ante amenazas que se propagan por Internet. Utilizar estas tecnologías disminuye el riesgo y exposición ante ataques.

Evitar el ingreso de información personal en formularios dudosos: cuando el usuario se enfrente a un formulario web que contenga campos con información sensible (por ejemplo, usuario y contraseña), es recomendable verificar la legitimidad del

sitio. Una buena estrategia es corroborar el dominio y la utilización del protocolo HTTPS para garantizar la confidencialidad de la información.

Tener precaución con los resultados arrojados por los buscadores web: a través de técnicas de Black Hat SEO, los atacantes suelen posicionar sus sitios web entre los primeros lugares en los resultados de los buscadores, especialmente en los casos de búsquedas de palabras clave muy utilizadas por el público. Ante cualquiera de estas búsquedas, el usuario debe estar atento a los resultados y verificar a qué sitios web está siendo enlazada.

Cierre:

Es importante enfatizar en que la debilidad en aspectos de seguridad de las aplicaciones, son más proclives a ser explotadas por personas malintencionadas, situación que podría generar daños, pérdidas de información, por tanto, desde el diseño y el desarrollo de aplicaciones, se deben agregar los elementos para garantizar un esquema de seguridad que cumpla con los estándares. Se invita al estudiante a realizar la actividad evaluativa.

Instrucción

Ahora se invita al estudiante a realizar la actividad evaluativa.

BIBLIOGRAFÍA

Agulló, D., Guerra, M., Silva, F., y Vivanco, F. (2012). Seguridad e Integridad de la transferencia de datos. Recuperado de http://www.profesores.elo.utfsm.cl/~agv/elo322/1s12/project/reports/AgulloVivancoGuerraSilva.pdf

Medero, G. (2009). Internet: una herramienta para las guerras en el siglo XXI. Recuperado de http://www.politicayestrategia.cl/index.php/rpye/article/view/177

Mieres, J. (2009). Ataques informáticos Debilidades de seguridad comúnmente explotadas. Recuperado de https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

Montesino, R., Balija, W., y Porven, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. Recuperado de http://scielo.sld.cu/scielo.php?pid=S1815-59282013000100004&script=sci_arttext&tlng=pt

Muñoz, M., y Mejía, J. (2015). Tendencias en Tecnologías de Información y Comunicación. Recuperado de http://www.scielo.mec.pt/scielo.php?pid=S1646-98952015000100001&script=sci_arttext&tlng=pt

Tarazona, C. (2013). Amenazas informáticas y seguridad de la información. Recuperado de http://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915

Temperini, M. (2014). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. Recuperado de http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_en_latinoamerica.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica