Universidad Católica de Honduras
Nuestra Señora Reina de la Paz

"Campus Global"

Asignatura:

Seguridad informática y gestión de riesgos

Catedrática:

Ing. Patricia Medina

Alumno:

Roberto Carlos Castillo Castellanos

Fecha:

22 de Octubre de 2022

Índice

Amenazas en un sistema de información

Inyección SQL

Las vulnerabilidades suelen ocurrir cuando una página contiene un fallo de seguridad en el código que permite que aquellos con intenciones maliciosas ataquen o consigan el control.
Esto es comúnmente causado por problemas en plugins de WordPress desactualizados u otras herramientas utilizadas en tu web.
La Inyección SQL es un tipo de ciberataque que involucra declaraciones SQL maliciosas o códigos de aplicación que se inyectan en los campos de entrada del usuario. Este proceso permite a los atacantes obtener acceso al backend de la web o al contenido corrupto de la base de datos.
Si el ataque se completa con éxito, pueden robar información del cliente, modificar o eliminar datos, o para conseguir un control absoluto de la web.
Esta es una de las amenazas informáticas más extendida en el mundo.
Un firewall de aplicaciones web (WAF), incluido en el paquete de Seguridad de la página web de GoDaddy, puede proteger tu web contra ataques de Inyección SQL.
Un WAF es un servicio de firewall basado en la nube que criba y protege el tráfico de tu web en tiempo real contra amenazas tales como ataques de Inyección SQL y spammers, a la vez que evita los ataques DDoS.

Cross-site scripting (XSS)

Este tipo de vulnerabilidad, también denominada XSS, es otro de los tipos comunes de amenazas informáticas más habituales que puede sufrir tu web.
A diferencia de la Inyección SQL, XSS ocurre cuando las líneas de código JavaScript malicioso se inyectan en una página para dirigirse a los usuarios de dicha web, manipulando scripts del lado del cliente.
Estos scripts secuestran las sesiones de los usuarios a través de la barra de búsqueda de una página web o comentarios (a través del backend).
Esto puede alterar la web y redirigir a los usuarios a otras páginas maliciosas que pueden manifestarse como páginas aparentemente de apariencia normal, pero que, en realidad, pueden robar su información.

Intercepción

Un ataque por Intercepción ocurre cuando un hacker captura datos que los usuarios envían a una web, y luego los utiliza para su propio beneficio. Puede ser información de contacto o datos sensibles como la tarjeta de crédito.
Los ciberdelincuentes luego venden estos datos o hacen sus propias compras.

Entre muchos ejemplos, un grupo de ciberdelincuentes hackeó en Bélgica varias empresas europeas en 2015 para acceder a datos financieros confidenciales. Robaron 6 millones de euros como resultado de estas actividades criminales.
Es importante instalar en tu web un certificado SSL para proteger los datos confidenciales.
El certificado SSL encripta las conexiones entre el navegador del visitante y el servidor web, para establecer una sesión segura. Esto protege a los compradores de ataques cibernéticos, como el de Intercepción.
Entonces, ¿tu web necesita un certificado SSL aunque no vendas online? La respuesta es sí.

Ataques de contraseñas

Algunos hackers adivinan contraseñas o usan herramientas y programas de diccionario para probar diferentes combinaciones hasta que las encuentran.
En algunos casos, el registro de teclas también se usa para conseguir el acceso a cuentas de usuario. El registro de teclas reconoce cada golpe de teclado realizado por un usuario. Los resultados se comunican nuevamente a los hackers que inicialmente instalaron estos programas.
¡Ojo! Ten cuidado al usar los ordenadores y redes de WIFI públicas.
Muchas webs carecen de contraseñas seguras, lo que hace que los intentos de iniciar sesión sean increíblemente fáciles. Estas son algunas formas de proteger tu página web:
Solicita una combinación segura y única de contraseñas.
Pídeles a los usuarios que cambien regularmente sus contraseñas.
Requiere autenticación de dos pasos para confirmar el acceso del usuario.
Y, por favor, no dejes “admin” como tu nombre de usuario en WordPress.

Configuración de seguridad incorrecta

Este ataque ocurre cuando las configuraciones de seguridad de una web tienen agujeros de seguridad que pueden conducir a varias vulnerabilidades.
Esto ocurre a menudo debido a la falta de un mantenimiento adecuado de tu página o una configuración inadecuada de la aplicación web.
Una configuración de seguridad incorrecta permite a los piratas informáticos acceder a datos privados o funciones de la web que pueden comprometer completamente el sistema. En estas situaciones, los datos también pueden ser robados o modificados.

Adware

Otro campeón de popularidad entre los usuarios. Y es que los efectos de un adware no pasan inadvertidos. ¿Quién no ha sufrido las molestias de navegar por Internet envuelto en un mar de anuncios spam y ventanas emergentes que se abren en el navegador de forma descontrolada?

El adware es un tipo de software aparentemente inofensivo si se compara con alguno de los anteriores tipos de malware, pero que puede bajar drásticamente el rendimiento de los trabajadores que necesitan navegar por Internet para realizar sus tareas.

A veces el adware incluye un “antivirus” o cualquier otra opción de registro mediante pago que elimina el problema. Se trata de un engaño perpetrado por los mismos autores del adware a erradicar.

Hace tiempo localicé un limpiador para este software que utilizamos desde hace tiempo y este si es gratuito, eso sí te recomiendo que lo hagas con un técnico especializado, alguna vez que otra borra algún servicio si tocas o activas alguna opción que no debes activar. Se llama adwcleaner.

Rootkit

Es un software que permite a los ciber intrusos acceder a equipos sin ser detectados para robar información sensible. Los rootkits permiten acceso privilegiado a un usuario (el hacker) ,que se conecta de forma remota, alterando el sistema operativo para ocultar la maniobra.

Un auténtico riesgo para empresas y usuarios, que pueden ver sustraídas sus claves de acceso, datos bancarios, etc.

Keylogger

Aunque también existen versiones que funcionan a través de dispositivos o complementos para hardware, hablamos básicamente de programas que pueden llegar a un equipo a través de virus, troyanos, etc., y que se dedican a memorizar las pulsaciones de teclado que realiza el usuario. La información queda registrada en un archivo y puede ser enviada a través de Internet.

Como puedes imaginar, los ciberdelincuentes pueden hacerse con todo tipo de contraseñas, datos bancarios y cualquier otro tipo de información privada.

¿Qué puedo hacer para prevenir robos de información y otros problemas de seguridad informática?

Nos gustaría tranquilizarte recomendándote el último antivirus en el mercado… Pero por desgracia, ¡instalar un antimalware no es suficiente!

Para garantizar la seguridad informática de tu empresa y prevenir amenazas, robos de identidad, usurpación de datos, extorsión, espionaje industrial y una larga lista de problemas, lo mejor es implementar unos protocolos de seguridad.

La variedad de medidas que se pueden tomar para prevenir amenazas de seguridad va desde la actualización de todo el software hasta la configuración y gestión de servidores, pasando por la instalación de antivirus, software de seguridad y la instalación y configuración de firewalls.