¿Qué es la seguridad web? Definición, significado, concepto

¿Qué es la seguridad web? Definición, significado, concepto. Prosigue nuestro viaje tratando de entender la terminología básica como webmasters o como propietarios de sitios web.
La seguridad del sitio web es un componente crítico para proteger sitios web y servidores. Los sitios web se analizan en busca de posibles vulnerabilidades y malware a través del software de seguridad del sitio web.

Este software puede buscar hacks de puerta trasera, redirigir hacks, troyanos y muchas otras amenazas. Un software de seguridad del sitio web notifica al usuario si el sitio web tiene algún problema y brinda soluciones para solucionarlo.

Las redes empresariales siempre tienen un alto riesgo de vulnerabilidad y es vital garantizar la seguridad del sitio web. Si la red se ve comprometida, el servidor y el sitio web también se ven comprometidos, lo que permitiría que el malware se infiltre a través de la red empresarial e introducir actividades de malware.

Lo que significa

Ha lanzado su sitio web y ha hecho todo lo posible para garantizar su éxito, pero es posible que haya pasado por alto un componente crítico: la seguridad del sitio web. Los ataques cibernéticos causan una limpieza costosa , dañan su reputación y desalientan a los visitantes a regresar . Afortunadamente, puede evitarlo con una seguridad efectiva del sitio web. Discutiremos los conceptos básicos de la seguridad del sitio web y las soluciones que ayudarán a garantizar que su sitio web no sea eliminado por un ataque cibernético.

La seguridad del sitio web es cualquier acción o aplicación tomada para garantizar que los datos del sitio web no estén expuestos a los ciberdelincuentes o para evitar la explotación de los sitios web de cualquier manera.

La seguridad web, también conocida como «seguridad cibernética», implica proteger el sitio web o la aplicación web al detectar, prevenir y responder a los ataques.
Los sitios web y las aplicaciones web son tan propensos a las infracciones de seguridad como los hogares físicos, las tiendas y las ubicaciones gubernamentales. Desafortunadamente, los delitos cibernéticos ocurren todos los días, y se necesitan grandes medidas de seguridad web para proteger los sitios web y las aplicaciones web para que no se vean comprometidos.

Eso es exactamente lo que hace la seguridad web: es un sistema de medidas de protección y protocolos que pueden proteger su sitio web o aplicación web para que no sea pirateado o ingresado por personal no autorizado. Esta división integral de seguridad de la información es vital para la protección de sitios web, aplicaciones web y servicios web. Todo lo que se aplique a través de Internet debe tener algún tipo de seguridad web para protegerlo.

Detalles de seguridad web

Hay muchos factores que intervienen en la seguridad web y la protección web. Cualquier sitio web o aplicación que sea seguro está seguramente respaldado por diferentes tipos de puntos de control y técnicas para mantenerlo seguro.

Hay una variedad de estándares de seguridad que deben seguirse en todo momento, y estos estándares están implementados y resaltados por OWASP. La mayoría de los desarrolladores web con experiencia seguirán los estándares de OWASP y también vigilarán la base de datos de incidentes de piratería en la web para ver cuándo, cómo y por qué diferentes personas están

pirateando diferentes sitios web y servicios.

Tecnología disponible

Existen diferentes tipos de tecnologías disponibles para mantener los mejores estándares de seguridad. Algunas soluciones técnicas populares para probar, construir y prevenir amenazas incluyen:

- Herramientas de prueba de caja negra
- Herramientas de fuzzing
- Herramientas de prueba de caja blanca
- Cortafuegos de aplicaciones web (WAF)
- Escáneres de seguridad o vulnerabilidad
- Herramientas de craqueo de contraseña
- Probabilidad de amenaza

La seguridad de su sitio web o aplicación web depende del nivel de las herramientas de protección que se han equipado y probado en él. Existen algunas amenazas importantes a la seguridad, que son las formas más comunes en las que un sitio web o una aplicación web se piratea. Algunas de las principales vulnerabilidades para todos los servicios basados en web incluyen:

- Inyección SQL
- Violación de contraseña
- Secuencias de comandos entre sitios
- Violación de datos
- Inclusión remota de archivos
- Inyección de código

La prevención de estas amenazas comunes es la clave para asegurarse de que su servicio basado en la web está practicando los mejores métodos de seguridad.

Las mejores estrategias

Hay dos grandes estrategias de defensa que un desarrollador puede usar para proteger su sitio web o aplicación web. Los dos grandes métodos son los siguientes:

Asignación de recursos : al asignar todos los recursos necesarios a causas dedicadas a alertar al desarrollador sobre nuevos problemas y amenazas de seguridad, el desarrollador puede recibir un sistema de alerta constante y actualizado que les ayudará a detectar y erradicar cualquier amenaza antes de que la seguridad sea oficialmente violada.

Escaneo web : ya existen varias soluciones de escaneo web que están disponibles para comprar o descargar. Sin embargo, estas soluciones solo son buenas para amenazas de vulnerabilidad conocidas; la búsqueda de amenazas desconocidas puede ser mucho más complicada. Sin embargo, este método puede proteger contra muchas infracciones y se ha comprobado que mantiene los sitios web seguros a largo plazo.
La seguridad web es extremadamente importante, especialmente para sitios web o aplicaciones web que tratan con información confidencial, privada o protegida. Los métodos de seguridad están evolucionando para coincidir con los diferentes tipos de vulnerabilidades que surgen.

Características de un buen plan de seguridad del sitio web

- Escaneo de malware
- Eliminación de malware
- Eliminación manual de malware y hackeo.
- Monitoreo de cambios de archivos
- Lista negra / monitoreo de spam
- Eliminar lista negra
- Monitoreo de seguridad

- Mitigación avanzada de DDoS
- Cortafuegos de aplicaciones web (WAF)
- Red de entrega de contenido (CDN)
- Sello del sitio

Problemas de seguridad del sitio web

Su sitio web maneja los datos confidenciales personales de los clientes, como las credenciales bancarias, los números de seguridad social y otra información vital como los detalles de la tarjeta de crédito. Hay muchos problemas de seguridad del sitio web que pueden ocurrir de muchas maneras:

Código fuente del sitio web

Cuando el código del sitio web no está bien desarrollado, hay muchos problemas de seguridad. Si su servidor web y sus aplicaciones web son complejas de administrar, las debilidades, los errores y las fallas de seguridad son una cosa segura. Cuanto más dinámico sea el sitio, más posibilidades de errores y agujeros de seguridad.

Acceso a visitantes de sitios web

Hay sitios web que crean un espacio para la interacción de los visitantes, como una sala de chat o cualquier otra opción para que sea fácil de usar. Sin embargo, esto trae una mayor probabilidad de que el sitio web sea vulnerable. Cuando hay una avenida a través de la cual los visitantes pueden acceder a los recursos corporativos, se vuelve más complejo identificar y distinguir entre los visitantes genuinos y los intencionados con malware. Por lo tanto, restringir o detener a los malos no autorizados es un desafío.

Software de seguridad del sitio web

El software de seguridad del sitio web equipa el sitio web para la protección contra ataques cibernéticos. El servicio de

seguridad del sitio web funciona al implementar la seguridad administrada como un modelo de servicio. Estos software son utilizados por los proveedores para proporcionar un servicio de seguridad del sitio web, generalmente como un modelo de seguridad como servicio administrado (SaaS).

El malware no se diferencia

El malware no está sesgado. Los ataques de seguridad son automáticos y todos los sitios web son propensos a ser atacados. No hay un objetivo específico en los sitios web. La seguridad del sitio web construye la reputación del sitio web y la confianza del cliente. Esto garantiza que el sitio web esté protegido contra malware y que los datos de los clientes estén bien protegidos.

Los ataques a la seguridad del sitio web son cada vez más sofisticados

Los hackers encuentran nuevas e innovadoras formas de atacar un sitio web. El malware está diseñado y desarrollado para identificar sitios web vulnerables. La intención de tales actividades maliciosas es distinta: si bien el propósito de algunos ataques malintencionados es robar los datos, algunos son para extender la actividad maliciosa por más tiempo.

Leer también: ¿Porqué se cae un servidor web o una página web?; Consejos para prevenir el Ransomware, cómo prevenirlo