

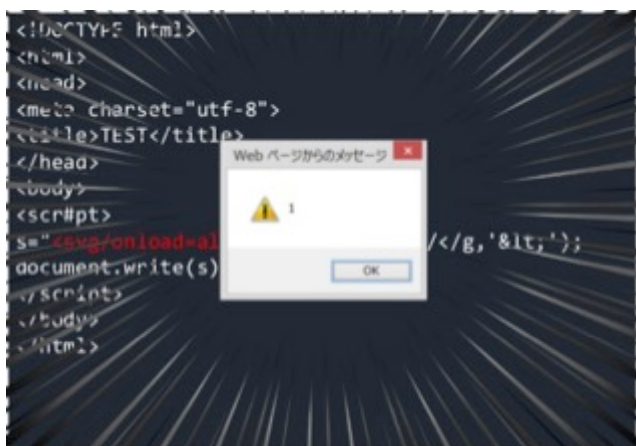


Hasta Google necesita una auditoría de seguridad informática

Un cambio realizado hace meses en una librería de código abierto de JavaScript provocó una vulnerabilidad Cross-site Scripting (XSS) en el buscador de Google y en otros de sus productos

¿Qué es un Cross-site Scripting (XSS)?

Es un tipo de vulnerabilidad informática, a través del cual el atacante inyecta sus propios “scripts” maliciosos en sitios web de confianza. Estos “scripts” pueden robar información personal, como credenciales de acceso (usuario, contraseña...); cookies y otros datos sensibles.



¿Qué ha pasado con Google?

El investigador de ciberseguridad japonés Masato Kinugawa descubrió lo que parecía ser una vulnerabilidad XSS en el motor de búsqueda de Google.

En otras palabras, Google era vulnerable a XSS, por lo que un cibercriminal podía realizar diversos ataques basándose en la confianza que inspira este gigante en el usuario. Jugar con la confianza permitía al atacante redirigir al usuario a otro sitio web para robar información mediante phishing o, entre otros métodos, que descargue una amenaza y la ejecute en su sistema.

Aparentemente, la vulnerabilidad se introdujo en septiembre de 2018 y se intervino el 22 de febrero de 2019.

LiveOverflow publicó un video de 13 minutos detallando la vulnerabilidad y sus principales causas y efectos.

¿Cómo evitar todo esto?

En primer lugar, a nivel de usuario, es esencial que tengas instalada y actualizada una solución en ciberseguridad. Si se ejecutara alguna aplicación maliciosa sin tu consentimiento, malware o exploits, automáticamente sería bloqueada.

A nivel de empresa, es de vital importancia que realices periódicamente auditorías de tus sistemas informáticos con una **empresa de seguridad informática** especializada en estos servicios informáticos.



Nosotros recomendamos **Dolbuck Seguridad Informática**, son expertos en **auditorías web**(seguridad de aplicaciones y servicios web), **auditorías de código** (vulnerabilidades en el código fuente de una web) o **auditoría forense**(recopilar evidencias digitales para establecer las causas que producen un ciberataque). Trabajan todo tipo de incidentes informáticos, y bajo estándares como las normas ISO 27001 y ENS.

¿Qué ganan las empresas con una auditoría de seguridad informática?

Además de reducir los **riesgos** y **vulnerabilidades**, que podrían traducirse en pérdida de información de clientes, pedidos, y proveedores, se mejora la **imagen externa** de su empresa, se aumenta la **seguridad** de su empresa, protegiendo así la confidencialidad de la información de su organización.

En definitiva, las nuevas tecnologías ofrecen muchísimas ventajas y soluciones, pero también implica una mayor exposición a ciberataques, amenazas y vulnerabilidades. Su empresa debe estar protegida y periódicamente auditada por empresas de ciberseguridad como Dolbuck Seguridad Informática.