



Que es el análisis de vulnerabilidades?

Consiste en una auditoría ciega donde se realiza un sistema, el caso de una web en busca de posibles fallos por los que se podría producir un ataque sobre la misma. Con este análisis se conocerán los posibles agujeros de seguridad y vulnerabilidades de la aplicación web sobre los que se debería actuar para mitigar los ataques al sistema de información.

La auditoría ciega o de caja negra, consiste en realizar comprobaciones en lo relativo a la seguridad sin disponer de conocimientos previos de la aplicación ni su código fuente. Esta metodología permite realizar a priori comprobaciones de seguridad y realizar las explotaciones más comunes que un atacante emplearía para vulnerar la seguridad del sistema. Muchos de estos ataques están entre los ataques más explotados y vienen catalogados en el archivo CWE (Common Weakness Enumeration) dependiente de la División de Ciberseguridad Nacional del Gobierno de EEUU. En concreto, se comprueban los siguientes grupos de ataques:

- Correcta gestión de las sesiones. (expiración, predictabilidad, etc.)
- Inyección SQL [CWE-89]
- Scripting cruzado (XSS) [CWE-79]
- Creación de peticiones cruzadas (CSRF) [CWE-352]
- Anti automatización insuficiente en procedimientos de registro
- Fallos de configuración
- Tratamiento incorrecto de redirecciones
- Comprobaciones insuficientes
- Vulnerabilidades conocidas en bibliotecas
- Pasarelas de pago, seguridad, correcta implementación, evaluación de la misma
- Conexiones a WebServices
- Divulgación de información confidencial no intencionada
- Falta de uso de criptografía en datos sensibles o uso de algoritmos criptográficos obsoletos [CWE-311] [CWE-327]
- Inyección de código, comandos del sistema o librerías externas [CWE-98] [CWE-78]

Este análisis es de vital importancia en portales web en los que la información que se trata en ellos tiene un alto valor, o tienen la imposición legal de aplicación de medidas de seguridad, como es el caso de los datos personales (les afecta a la gran mayoría de empresas).

Por otro lado, se trata de un análisis fundamental cuando la web dispone de venta online, ya que existe un elevado porcentaje de fraudes en internet.

Que es el análisis SEO/SEM?

Del ingles Search Engine Optimization (SEO, Optimización para Motores de Búsqueda) y Search Engine Marketing (SEM, Marketing en los Motores de Búsqueda). Estos términos se emplean cuando nos referimos a la optimización de las páginas web, a nivel de programación informática, para mejorar la visibilidad de las mismas en los resultados de los principales



buscadores.

Realmente el SEO se engloba como método de partida para realizar un buen SEM, esto es debido a que un portal web debe de estar bien optimizado para que surjan efecto las campañas de marketing SEM, ya que estas se deben realizar pagando.

El diagnóstico inicial de una sitio web está dirigido a valorar su relevancia en los principales buscadores con el fin de detectar las carencias del mismo. Para ello se llevan a cabo las siguientes tareas:

Análisis de los contenidos del sitio web

Determinar la relevancia de los contenidos en función de las palabras claves y descripciones utilizadas, las etiquetas empleadas, las páginas indexadas y las tecnologías que se usan.

Análisis de errores comunes

Búsqueda de disfuncionalidades frecuentes como son el contenido duplicado, enlaces rotos, enlaces con javascript, la disponibilidad del servidor web, imágenes empleadas para mostrar texto, contenido o elementos de navegación dentro de películas Flash.

Haciendo uso de herramientas de medición de tiempos de carga se estimará el coste de términos de velocidad, los principales errores en este sentido suelen ser: dispersión de código javascript y css en múltiples archivos, uso de la propiedad "width" de la etiqueta "img" y finalmente diversos aspectos de configuración en el lado del servidor.

Análisis de difusión del sitio web

Determinar la repercusión del sitio, que vendrá determinada por la referencia de la misma desde enlaces externos, su presencia en foros y redes sociales y el PageRank asignado.

Análisis del seguimiento actual

Estudio del uso hecho de las estadísticas obtenidas con Google Analytics. Mediante el empleo de Google Trends determinar que patrones de búsqueda se han utilizado para encontrar a este sitio web o sitios web relacionados.

Análisis de palabras clave para enlaces de pago

En cualquier campaña de posicionamiento en buscadores habrá términos de búsqueda o palabras clave para las que resultará imposible lograr ser primeros en un corto plazo de forma natura. Para lograr estar presente en estas páginas de resultados de alta competitividad, así como para contar con tráfico procedente de los buscadores desde el primer momento tenemos que contar con los enlaces patrocinados.