**El Top 10 de OWASP**

A fin de prepararse para futuros riesgos, los profesionales de seguridad deben mantenerse informados. Ya aprendiste sobre la **lista CVE®**, un diccionario de acceso abierto de vulnerabilidades y exposiciones conocidas. La lista CVE® es una fuente importante de información que la comunidad de seguridad global utiliza para compartir información entre sí.

En esta lectura, aprenderás sobre otro recurso importante que los profesionales de seguridad utilizan como referencia, el Open Web Application Security Project® (Proyecto Abierto de Seguridad de Aplicaciones Web, u OWASP). Aprenderás sobre el papel de OWASP en la comunidad de seguridad global y cómo las empresas utilizan este recurso para centrar sus esfuerzos.

**¿Qué es OWASP?**

El Open Web Application Security Project® es una fundación sin fines de lucro que trabaja para mejorar la seguridad del software. OWASP es una plataforma abierta que los profesionales de seguridad de todo el mundo utilizan para compartir información, herramientas y eventos que se centran en proteger la web.

**El Top 10 de OWASP**

Uno de los recursos más valiosos de OWASP es su Top 10. Desde 2003, la organización publica esta lista como una manera de difundir el conocimiento de las vulnerabilidades más específicas de la web. El Top 10 refiere principalmente a software nuevo o por encargo. Muchas de las organizaciones más grandes del mundo consultan el Top 10 de OWASP para ayudar a garantizar que sus programas se desarrollen teniendo en cuenta los errores de seguridad más comunes.

**Consejo profesional:** El Top 10 de OWASP se actualiza cada algunos años, a medida que evolucionan las tecnologías. El orden se basa en la frecuencia con la que se descubren las vulnerabilidades y el nivel de riesgo que estas presentan.

**Nota:** Los auditores también utilizan el Top 10 de OWASP como un punto de referencia para verificar el cumplimiento normativo (compliance).

**Vulnerabilidades comunes**

A menudo, las empresas toman decisiones de seguridad críticas con base en las vulnerabilidades enumeradas en el Top 10 de OWASP. Este recurso influye en la forma en que las empresas diseñan el nuevo software que estará en su red, a diferencia de la lista CVE®, que las ayuda a identificar mejoras en programas ya existentes. Las vulnerabilidades que aparecen con mayor frecuencia en el ranking son:

**Pérdida de control de acceso**

Los controles de acceso limitan lo que los usuarios pueden hacer en una aplicación web. Por ejemplo, un blog puede permitir a sus visitantes publicar comentarios sobre un artículo reciente, pero les impide eliminar el artículo por completo. Las fallas en estos mecanismos pueden conducir a la divulgación, modificación o destrucción de información no autorizada. También pueden dar a alguien acceso no autorizado a otras aplicaciones de la empresa.

**Fallas criptográficas**

La información es uno de los activos más importantes que las empresas deben proteger. Las leyes de privacidad, como el Reglamento General de Protección de Datos (RGPD), requieren que los datos confidenciales estén protegidos por métodos de cifrado efectivos. Por ejemplo, pueden ocurrir vulnerabilidades cuando las empresas no cifran la información personal identificable (PII). También, si una aplicación web utiliza un algoritmo de hashing débil, como el MD5, está más expuesta a sufrir una violación de datos.

**Inyección**

Un ataque de inyección se produce cuando se inserta un código malicioso en una aplicación vulnerable. Si bien la aplicación pareciera funcionar con normalidad, se comporta de una manera diferente a la que debería. Este tipo de ataque puede dar a los agentes de amenaza una puerta trasera al sistema de información de una organización. Un objetivo habitual es el formulario de inicio de sesión de un sitio web. Si estos formularios son vulnerables a la inyección, los atacantes podrían insertar código malicioso que les permita acceder y modificar o robar credenciales de usuario.

**Diseño inseguro**

Las aplicaciones deben diseñarse de tal manera que sean resistentes a ataques. Cuando esto no sucede, se vuelven mucho más vulnerables a amenazas, como ataques de inyección o infecciones de malware. El diseño inseguro refiere a la carencia o deficiente implementación de una variedad de controles de seguridad, que deberían haberse programado en una aplicación durante su desarrollo.

**Configuración de seguridad incorrecta**

Esta vulnerabilidad se produce cuando la configuración de seguridad y su mantenimiento no se realizan correctamente. Las empresas utilizan una variedad de sistemas interconectados y los errores suelen ocurrir cuando estos no están correctamente configurados o auditados. Un ejemplo común es cuando las empresas implementan equipos, como un servidor de red, utilizando los ajustes de fábrica. Esto puede llevarlas a utilizar configuraciones que no cumplen con los objetivos de seguridad de la organización.

**Componentes vulnerables y desactualizados**

Se trata de una categoría que se relaciona principalmente con el desarrollo de aplicaciones. En lugar de codificar todo desde cero, la mayoría de los desarrolladores utilizan bibliotecas de código abierto para completar sus proyectos de una forma más rápida y fácil. Este software disponible públicamente lo mantienen comunidades de programadores, de forma voluntaria. Las aplicaciones que utilizan componentes vulnerables a los que no se les realizaron tareas de mantenimiento corren un mayor riesgo de ser explotadas por agentes de amenaza.

**Fallas de identificación y autenticación**

La identificación es la palabra clave de esta categoría de vulnerabilidad. Cuando las aplicaciones no reconocen quiénes deben tener acceso a ellas y lo que están autorizados a hacer, pueden generarse problemas graves. Por ejemplo, un router Wi-Fi doméstico suele contar únicamente con un formulario de inicio de sesión sencillo para mantener a los huéspedes no deseados fuera de la red. Si esta defensa falla, un atacante puede invadir la privacidad de un propietario.

**Fallas en el software y la integridad de los datos**

Se trata de instancias en que las actualizaciones o parches no se revisan adecuadamente antes de su implementación, por lo cual, los atacantes podrían explotar estas debilidades para distribuir software malicioso. Cuando eso ocurre, pueden producirse efectos graves de flujo descendente. O sea, basta con que un solo sistema se vea comprometido, para que otros sistemas también sean infectados. A este tipo de ataque se lo conoce como ataque a la cadena de suministro.

Un ejemplo famoso es el [ataque cibernético de SolarWinds (2020),](https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic) en el que un grupo de hackers inyectaron código malicioso en las actualizaciones de software que la empresa lanzó, sin saberlo, a sus clientes.

**Fallas en el registro y monitoreo**

En seguridad, es importante registrar eventos y rastrear su origen. Tener un registro de eventos como los intentos de inicio de sesión de usuarios es fundamental para encontrar y solucionar problemas. El monitoreo efectivo es tan importante como la respuesta a incidentes.

**Falsificación de solicitudes del lado del servidor**

Las empresas tienen información pública y privada almacenada en servidores web. Cuando utilizas un hipervínculo o haces clic en un botón en un sitio web, se envía una solicitud a un servidor que debe validar quién eres, obtener los datos apropiados y luego devolvértelos.



Las falsificaciones de solicitudes del lado del servidor (SSRF) suceden cuando los atacantes manipulan las operaciones normales de un servidor para leer o actualizar otros recursos de aquel. Esto es posible cuando hay una aplicación vulnerable en el servidor. Esta transporta el código malicioso a un servidor host que obtendrá datos no autorizados.

**Conclusiones clave**

Estar al tanto y conocer en profundidad las últimas tendencias de ciberseguridad puede ser una forma útil de ayudar a defenderte de los ataques y prepararte para riesgos futuros en tu carrera de seguridad. [El Top 10 de OWASP](https://owasp.org/www-project-top-ten/) es un recurso útil con el que puedes obtener más información sobre estas vulnerabilidades.