

Índice

Introducción

Sistemas de Pago

Seguridad

Desarrollo de Software seguro de OWASP

Introducción

Durante los últimos 10 años, el comercio electrónico ha sido uno de los segmentos del

sector de venta al público que más rápido ha crecido. Eso podría parecer obvio para

cualquiera que haya realizado una compra online alguna vez, pero el tamaño y la velocidad

del crecimiento han sido asombrosos. Ya existen cientos de miles de tiendas online en la Red

y, según ciertos cálculos, los comerciantes abren 20.000 nuevas tiendas de comercio

electrónico cada semana.

La popularidad del mercado online no muestra ninguna señal de desaceleración, así que ahora

podría ser el momento ideal para empezar a vender en la Web. Existen más opciones que

nunca para crear un sitio de comercio electrónico. Puede trabajar con un proveedor de

plataformas de comercio electrónico para crear una tienda online o quizá prefiera dejar que

profesionales de la Web se encarguen del diseño y del desarrollo de su sitio de comienzo a fin.

Trabajar con servicios como éstos puede resultar cómodo, pero si desea más flexibilidad y

control, quizás sea más conveniente que cree su sitio usted mismo. Con unos pocos

conocimientos y unas herramientas fáciles de usar, puede desarrollar un sitio de comercio

electrónico que se vea y funcione exactamente como usted lo desea, ayudándole a

satisfacer las necesidades de sus clientes y de su negocio de manera más eficiente.

En este trabajo, aprenderá acerca de los elementos fundamentales que implica crear su propio sitio web de comercio

electrónico hecho por usted mismo (DIY), desde elegir las herramientas y los servicios

adecuados que necesitará para aceptar pagos de sus clientas, hasta incluso determinar

la mejor seguridad para su sitio.

2.2.6. Sistemas de Pago

Un sistema de pago electrónico es un sistema de pago que facilita la aceptación de pagos electrónicos para las transacciones en línea a través de internet.

Los sistemas de pagos electrónicos realizan la transferencia del dinero entre compradores y vendedores en una acción de compra-venta electrónica a través de una entidad financiera autorizada por ambos. Es, por ello, una pieza fundamental en el proceso de compra-venta dentro del e-commerce.

Como ejemplos de sistemas de pago electrónico nos encontramos las pasarelas de pago o TPV virtual para el pago con tarjeta, los sistemas de monedero electrónico y los sistemas que se conectan directamente con la banca electrónica del usuario.

Se distinguen dos tipos de instituciones para la ejecución de este sistema: El bancario y el de sitios web especializadas en pagos electrónicos que operan como una entidad financiera virtual. En el pago con tarjeta, el mecanismo de pago valida la tarjeta y organiza la transferencia del dinero de la cuenta del comprador a la cuenta del vendedor.

El monedero electrónico, sin embargo, almacena el dinero del comprador en un formato electrónico y lo transfiere al sistema durante el pago. El sistema de pago valida el dinero y organiza la transferencia a la cuenta del vendedor. También existe la posibilidad de que el sistema de pago transfiera el dinero electrónico al monedero electrónico del vendedor actuando en este caso como un intermediario entre ambos monederos electrónicos.

El pago a través de la banca electrónica, enlaza un número de operación o venta realizada en el comercio o tienda virtual con la cuenta bancaria del cliente en el mismo sitio del banco. Esto, reduce el riesgo de fraude al no transmitir información financiera personal por la red. Si el pago o transacción se desea hacer entre monedas diferentes, la misma institución financiera puede ofrecer un cambio de divisas, generalmente con un cargo adicional por el respectivo cobro de comisión por dicha operación.

2.2.7. Seguridad

La seguridad de las ventas es uno de los factores más importantes para los comercios electrónicos. Los dueños de una tienda online que no ponen en marcha los protocolos adecuados no solo ponen a sus clientes en peligro, sino también a su propio negocio.

Incluso las tiendas pequeñas que venden a un grupo reducido de personas corren riesgo si tienen lagunas en protección digital. De hecho, son los pequeños comerciantes los que mayores probabilidades tienen de ser atacados por los cibercriminales debido, precisamente, a la menor seguridad y la gran cantidad de datos confidenciales que manejan.

En 2017, un 32 % de grandes y medianas empresas españolas reconocieron haber sufrido al menos un ataque informático en los 12 meses anteriores al estudio realizado por la consultora Grant Thornton.

Además de las consecuencias económicas —como pagar recargos si debemos devolver un pago—, la filtración de datos perjudica la imagen de una tienda virtual, ya que, como es normal, los clientes no están dispuestos a seguir usando un sitio donde se haya visto comprometida su información.

Por no mencionar que, desde finales de 2017, Google ha adoptado una serie de medidas para forzar la seguridad en la Red: además de posicionar mejor las páginas protegidas mediante HTTPS, advierte claramente a los usuarios de que la «conexión no es segura» en la barra de direcciones de las páginas que recopilan contraseñas o datos de pago y no disponen de esta medida de protección online, lo que puede ahuyentar a gran cantidad de clientes potenciales.

Certificado SSL (Secure Socket Layer) o TLS (Transport Layer Security)

Un certificado SSL cifra la información confidencial que se envía entre usuarios para salvaguardarla, El certificado hace que todos los datos delicados por ejemplo contraseñas, números de tarjetas o nombres de usuario resulten ilegibles para todo el mundo salvo el servidor del destinatario.

Es de suma importancia un certificado SSL especialmente para los sitios que realizan transacciones. Adquirirlo no es tan difícil puede ser de un proveedor reconocido como Digicert, Comodo o Symantec.

Protocolo HTTPS

El HTTPS es el protocolo que se debería usar en todas las páginas en las que se generan datos personales. Con el protocolo HTTP, el que se venía usando desde que se creó internet, la información no se cifra; por el contrario, se envía en texto simple, por lo que, si alguien la llegara a interceptar, podría leerla sin más problemas.

Desde el año 2014 todas las páginas que no dispongan de HTTPS van a sufrir un deterioro en el posicionamiento de su web de forma que la visibilidad de su comercio online se puede ver muy afectada.

Cortafuegos

Un cortafuego o firewall es un sistema de software o hardware que sirve como compuerta entre dos o más redes, de modo que permite la entrada al tráfico autorizado y bloquea el acceso al que parece sospechoso.

Existen muchos tipos de cortafuegos, pero uno de los más efectivos para e-commerce son los proxys, que funcionan como programas intermediarios entre las redes, de esta forma el tráfico entrante no se conecta directamente a la red de nuestra tienda online.



Auditorias y Pruebas de seguridad

Realizar pruebas de ataque al sitio para poder visualizar posible huecos en la seguridad que se puedan tener y corregirlas de inmediato.

Utilizar un hosting confiable y dominio para su web

Un E-Commerce al igual que cualquier otro sitio de Internet, requiere estar alojado en servidores.

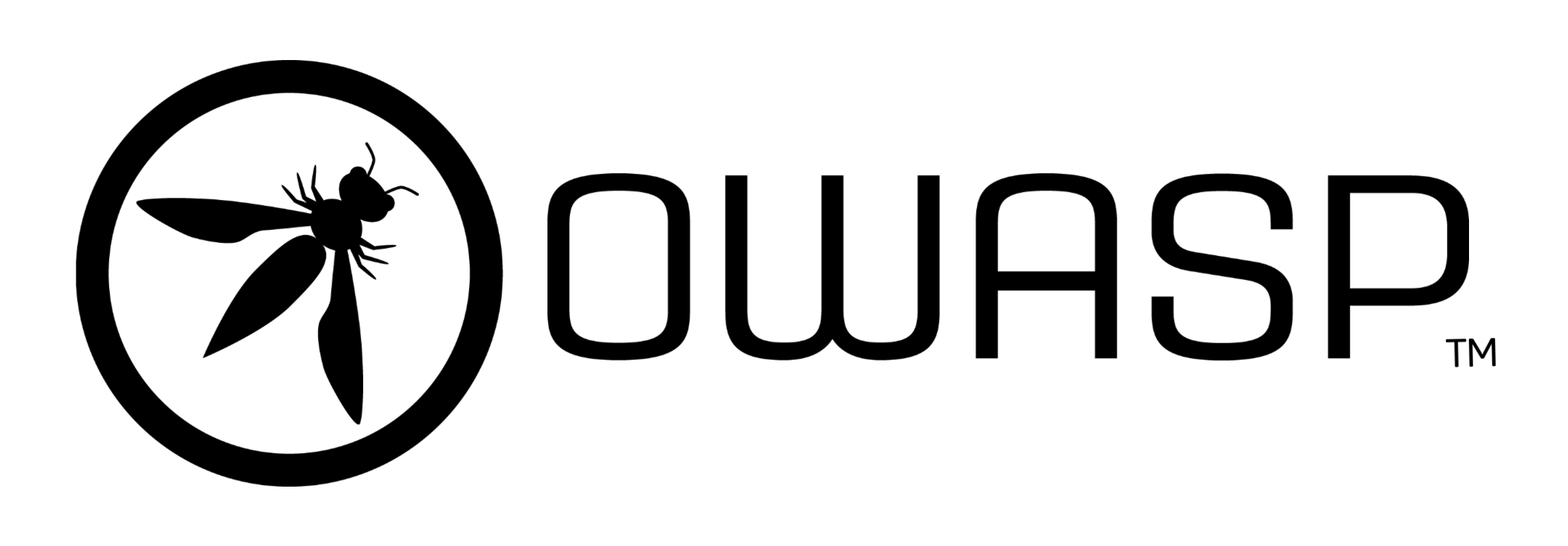
Algunos prefieren plataformas/sitios webs que permiten armar el e-commerce dentro de ellos, pero lo preferible es tener el control total del mismo, en vez de depender de una plataforma que le pertenece a terceros, por lo tanto es mejor utilizar un dominio privado.

Actualizaciones Constantes

El uso de plataformas como WooCommerce en WordPress o Magento, VTEX, facilitará la gestión del comercio online. Pero aunque se cumpla con la mayoría de los requisitos anteriores, todo podría fallar si no se aplica las actualizaciones críticas de estos sistemas.

Se recomienda revisar constantemente si existen nuevas versiones de estos software e instalarlas en el sitio tan pronto sea posible, ya que suelen contener parches de seguridad que pueden ser críticos.

2.1.7.1. Desarrollo de software de OWASP

¿Qué es OWASP?

Open Web Application Security Project (OWASP) es una organización sin ánimo de lucro a nivel mundial dedicada a mejorar la seguridad de las aplicaciones y del software en general. Su misión es hacer que la seguridad dentro de las aplicaciones sea más visible para que, así, las organizaciones y los particulares puedan tomar decisiones sobre conceptos de seguridad basándose en información verídica y contrastada.

Es importante destacar que cualquiera puede participar en OWASP y que todos sus proyectos, materiales y documentación están disponibles de forma gratuita. Del mismo modo, y algo importante, es que todos los productos y servicios recomendados no son productos comerciales, sino que son productos también libres y de código abierto.

Como organización, tienen una serie de valores:

* Transparencia: todo lo relativo a OWASP es transparente, desde sus finanzas (que pueden ser consultadas directamente desde su página web) hasta el código de sus proyectos (los repositorios de código también están accesibles).
* Innovación: promueven y favorecen la experimentación para aquellas soluciones a los nuevos desafíos de seguridad que aparecen.
* Global: cualquier persona de cualquier parte del mundo está invitada a participar en la comunidad de OWASP (se puede aplicar desde un formulario).
* Integridad: se declaran como una comunidad honesta y en la que se puede confiar. También se declaran neutrales sobre el aspecto comercial de los productos de seguridad disponibles en el mercado, no posicionándose sobre alguno de ellos.

Por lo tanto, OWASP pretende ser el centro de referencia de toda la información de seguridad enfocada a las aplicaciones web. Ya veremos que no sólo información sino también estudios, soluciones y proyectos con los que nos ayudarán a los desarrolladores a hacer que nuestras aplicaciones web sean más seguras.

Top 10 vulnerabilidades más comunes

OWASP, cada cierto tiempo, realiza un informe recogiendo las vulnerabilidades más comunes dentro de las aplicaciones web. Con este informe, podremos estar al tanto de dichas vulnerabilidades y podremos emplearlo para comprobar si nuestra aplicación tiene alguna de las que aparecen en dicho informe. También, ofrecen herramientas de detección y consejos sobre medidas a tomar para solucionar dicha vulnerabilidad.

A continuación, vamos a enumerar las 10 vulnerabilidades más comunes del informe realizado hasta 2013 (podéis acceder al documento íntegro desde aquí) y vamos a aportar una breve descripción sobre cada una de las vulnerabilidades:

1. Inyección: este ataque se produce cuando datos no confiables son enviados a un intérprete (ya sea del sistema operativo, de una base de datos o cualquier intérprete) como parte de un comando o consulta. Los datos hostiles introducidos por el atacante pueden engañar al intérprete haciendo que se ejecuten comandos no intencionados o accediendo a información sobre la que no se está autorizado. Uno de los ejemplos más significativos de este tipo de ataque es *SQL Injection*.
2. Pérdida de autenticación y gestión de sesiones: este tipo de ataque se produce cuando los mecanismos de la aplicación relacionados con la autenticación, autorización y control de sesiones son, frecuentemente, implementados de forma incorrecta o su configuración no se ha realizado de forma correcta. Esto provoca que un usuario malicioso pueda obtener las credenciales de un usuario, el identificador de la sesión o, incluso, el identificador de acceso y hacerse pasar por dicho usuario accediendo a todos sus datos. Uno de los ejemplos puede ser la gestión de la sesión mediante la propia página.
3. Secuencia de comandos en sitios cruzados (XSS): este tipo de ataque ocurre cuando se obtienen datos no confiables y se envían directamente al navegador web. Esto provoca que se puedan ejecutar comandos no deseados en el navegador del usuario. Estos comandos pueden obtener desde las credenciales de acceso del usuario como instalar ciertos programas maliciosos.
4. Referencia directa insegura a objetos: este tipo de ataque ocurre cuando no se controlan los accesos a recursos sobre los que un usuario no debería tener acceso. En las aplicaciones, la mayoría de las veces, existen distintos usuarios y cada usuario tiene una serie de recursos sobre los que tiene acceso y otros sobre los que no debería tener acceso. Un ejemplo podría ser el acceso a una tabla de base de datos sobre la que un determinado usuario no debería tener acceso (una tabla de gestión sobre la que sólo el administrador debería tener acceso).
5. Configuración de seguridad incorrecta: este tipo de ataque ocurre cuando se han realizado malas configuraciones en las aplicaciones, en los servidores de las aplicaciones, en las bases de datos o en la configuración del propio sistema operativo. Es importante tener todo el *software* bien actualizado con la última versión disponible (esperando a que no haya vulnerabilidades de día 0 ) y que todas las librerías o *frameworks* que use la aplicación también estén actualizadas ya que muchos cambios que se realizan en las versiones tienen que ver con aspectos de seguridad.
6. Exposición de datos sensibles: este tipo de ataque ocurre cuando se puede acceder de forma fácil a datos de carácter sensible almacenados en la aplicación. Cuando, por ejemplo, se almacenan las credenciales de los usuarios sin codificar o si la comunicación del servidor no es segura a la hora de realizar un pago con una tarjeta de crédito.
7. Ausencia de control de acceso a funciones: este tipo de ataque ocurre cuando se acceden a funciones del servidor sobre las que un usuario no debería tener permiso. Cuando, por ejemplo, el servicio de listado de usuario sólo debería estar disponible por la aplicación, pero cualquier usuario puede también acceder a esta información.
8. Falsificación de peticiones en sitios cruzados: este tipo de ataque ocurre cuando se realizan peticiones HTTP falsificadas del ordenador de la víctima a una aplicación web vulnerable.
9. Utilización de componentes con vulnerabilidades conocidas: este tipo de ataque ocurre cuando se emplean librerías o *frameworks* que contienen vulnerabilidades. Es por esto que es importante actualizar estos componentes o revisar el histórico de revisiones para comprobar las mejoras de seguridad implementadas.
10. Redirecciones y reenvíos validados: este tipo de ataque ocurre cuando, al redireccionar al usuario a otra página, no se comprueba que el destino sea válido. Es por esto que se puede redirigir a un usuario a una página que contenga contenido malicioso para robar las credenciales de dicho usuario.

Una vez se han visto los 10 ataques más comunes, es importante destacar que casi siempre se usan ataques combinados para aprovecharse de todas las vulnerabilidades. Se puede hacer un ataque de SQL Injection para acceder a una tabla sobre la que el usuario no debería tener permiso para tener acceso a credenciales no codificadas de los usuarios del sistema. Por lo que es importante centrarse en todas y cada una de estas vulnerabilidades.

Herramientas

OWASP también realiza una serie de proyectos con el objetivo de darnos herramientas para afianzar la seguridad de nuestras aplicaciones. Estos proyectos se pueden acceder desde el siguiente enlace.

A continuación, se muestran algunos de estos proyectos junto con una breve descripción de cada uno de ellos.

* Zed Attack Proxy: es una herramienta de pentesting que nos ayuda a encontrar vulnerabilidades en nuestras aplicaciones. Es recomendable el uso por gente con cierta experiencia en términos de seguridad.
* OWTF: es una herramienta de pentesting que es, quizás, un poco más sencilla que la herramienta anterior.
* Dependency Check: es una herramienta que nos permite analizar todas las dependencias de nuestra aplicación y comprobar si existen vulnerabilidades dentro de ellas.
* Mobile Security Project: es una herramienta que nos permite realizar pentesting sobre aplicaciones móviles.
* SSL advanced forensic tool: es una herramienta que nos permite mostrar información sobre SSL y los certificados.

Existen muchos proyectos más y es recomendable echar un vistazo a todos ellos ya que nos ayudan (y mucho) a nuestro objetivo de asegurar la seguridad en nuestra aplicación.

Conclusiones

Es importante tener en cuenta que cuantos más métodos o formas de pago ofrezcas en su eCommerce más posibilidades tendrás de convertir una venta, ya que de esta manera se adapta ante las necesidades de los clientes.

Por otra parte, nos encontramos con que un mayor coste en control de las diferentes maneras de pago, por lo que es importante conocer las formas de pago esenciales para tu tienda online; las demás serán un valor añadido a tu proceso de compra online.

La realidad es que depende de tu actividad, de tus productos y, sobre todo, de quién sea tu posible comprador. En función de ello será más recomendable o no implementar unas formas de pago u otras.

Aunque la seguridad no es gratis, resulta más económica que sufrir ataques de hack.

En última instancia, no existe una única solución unificada capaz de proteger y asegurar los sitios de comercio electrónico.

La mejor solución es combinar el software y la plataforma de hosting adecuados y logra mantener el sistema actualizado y protegido.

En cualquier caso, prepárese para las malas noticias. No olvide realizar copias de seguridad automáticas de su sitio.

Considere implantar un enfoque por capas usando distintas herramientas y no olvide que los fiables procedimientos escritos son cruciales para mantener su sitio seguro y protegido.

Ya hemos visto, muy por encima, qué es OWASP y todas las bondades que nos ofrece. Con esto en mente, es importante dedicarle tiempo a conocer las vulnerabilidades y a conocer también los mecanismos para corregirlas. En futuros tutoriales, analizaremos las vulnerabilidades más comunes y aportaremos una serie de soluciones para poder corregirlas. Del mismo modo, también analizaremos las distintas herramientas que nos proporciona OWASP para realizar análisis de nuestras aplicaciones.

Bibliografía

Páginas de referencia en las que nos basamos durante el desarrollo de este documento.

* <https://www.cloudflare.com/learning/security/threats/owasp-top-10/>
* <https://owasp.org/index.php/Main_Page>
* <https://owasp.org/>