CONSEJOS PARA DESARROLLADORES WEB CON ENFOQUE A COMERCIO ELECTRÓNICO

Jesús Mauricio Andrade Guzmán

CMS

numero-27

Este artículo está orientado para negocios pequeños y medianos, así como equipos de desarrollo que buscan tener presencia web. La demanda de comercios en línea se está incrementando considerablemente. El manejo de transacciones monetarias en línea, sin considerar aspectos de seguridad informática, pone en riesgo la información de clientes y vendedores, por lo que es necesario contar con un plan de desarrollo integral que considere al menos las cuestiones básicas de seguridad.

A continuación se mostrará un panorama general de los problemas de seguridad que se presentan durante el desarroll de una solución de comercio electrónico y se discutirán consejos básicos a tomar en cuenta. No se pretende profundizar sobre varios temas relacionados, pero se ofrecerán algunas referencias de consulta. Algunos de ellos pueden no aplicar al flujo de desarrollo de su empresa o equipo de trabajo por alguna razón, pero es importante que se consideren en lo general al menos. Del mismo modo, estas recomendaciones son suficientemente generales para aplicar en cualquier metodología de desarrollo, lenguaje de programación o enfoque que se adopte al desarrollar un sistema que pretenda ser tienda en línea.

INTRODUCCIÓN

Actualmente no sólo hay más dispositivos conectados a Internet, también confiamos más en ellos y hacemos todo a través de la red. El comercio en línea está creciendo de manera importante, sólo en México el comercio electrónico creció 34% en 2014 (AMIPCI, 2015). Debido a esta tendencia, una tienda de ropa, juguetes, alimentos o prácticamente lo que sea, si no está ya ofreciendo sus productos en línea, muy pronto buscará entrar al mundo del comercio electrónico.

Existen varias maneras de ofrecer productos y servicios por Internet, una empresa puede optar por:

A. Desarrollo libre. Este punto abarca tanto el diseño, desarrollo e implementación de una aplicación de comercio en línea, como el uso de herramientas de desarrollo prefabricadas para personalizar soluciones a través de un código (generalmente PHP, Java, JavaScript, CSS o HTML). Una empresa o un consultor externo puede desarrollar su propia plataforma utilizando herramientas como Magento, WooCommerce o PrestaShop e incluso desarrollar las funcionalidades completas con herramientas de programación como CodeIgniter, Zend, Bootstrap, entre otras.
B. Catálogo en línea. Es posible utilizar una plataforma para ofrecer productos como Amazon, MercadoLibre o eBay, las cuales ofrecen la gestión completa del proceso de venta, es decir, los métodos de pago, envío, seguimiento de usuarios, inventario, etcétera. Normalmente un usuario de estos servicios sólo debe crear una cuenta y proporcionar la información de sus productos para empezar a vender.
C. Software como Servicio. También pueden optar por soluciones SaaS (Software as a Service)como Shopify, Volusion, Square Space, entre otras. Estas ofrecen su plataforma a través de una cuota mensual de esta manera una empresa puede personalizar y publicar una tienda en línea sin tener que contar con infraestructura propia.

El comercio en línea es actualmente un mercado en crecimiento (Informe sobre la economía de la información, 2015). Existen muchas alternativas y los actores involucrados buscan satisfacer a usuarios que cada vez están más conectados y acostumbrados a las nuevas tecnologías. Los retos a los que se enfrentan los mercados en desarrollo como México también son nichos de oportunidad para empresas internacionales y la competencia a la que deben enfrentar las empresas de desarrollo en nuestro país es cada vez mayor.

Muchas empresas de tecnología dedicadas al desarrollo de software ofrecen actualmente soluciones de comercio electrónico, y si no lo harán pronto. Es muy importante que en el desarrollo de las soluciones se tomen en cuenta tanto la seguridad de las transacciones en línea que se realiza, así como la privacidad de los clientes a los que está dirigida esta tecnología.

CONSEJOS

Estos “consejos” pueden ser leídos como simples comentarios de situaciones generales a los que se puede enfrentar un desarrollador web con un proyecto de tienda en línea.

SOBRE EL USO DE HTTPS Y LA INYECCIÓN DE CÓDIGO

Utilizar HTTPS es un requisito indispensable para un comercio en línea pero no ofrece defensa para la mayoría de los ataques cibernéticos. El desarrollador debe estar consciente de las últimas tendencias en ataques y estrategias de defensa para sus sitios web.

No es suficiente activar el soporte para HTTPS en un sitio web, es necesario atender buenas prácticas de seguridad durante todo el ciclo de desarrollo del software, contemplar actualizaciones y pruebas de seguridad durante la vida del sistema.

En números anteriores de esta revista se ha discutido la utilización de un canal cifrado para transmitir tráfico web; también se han ofrecido consejos para evitar fraudes en línea. Actualmente resulta alentador saber que en la mayoría de los servicios en Internet ya se utiliza algún método de cifrado para la información que viaja por la red o al menos se ofrece la opción de usarlo. Sin embargo, basta con revisar las listas de 2010 o 2013 de OWASP de las principales amenazas que afectan a aplicaciones web, en las cuales la primera amenaza registrada desde hace varios años es la inyección de código.

La inyección de código ocurre cuando los datos de entrada a las aplicaciones no están debidamente validados, abriendo el paso a posibles ataques. Para "inyectar" código malicioso o consultas con intenciones maliciosas no es relevante si la aplicación web se transmite o no usando algún tipo de cifrado. Es importante distinguir esto, porque pensar que HTTPS protege de este modo a una aplicación puede resultar peligroso por la omisión de otras precauciones, como la validación y la detección de amenazas. Hablando de esto, también en números anteriores se ha discutido el tema de la detección y protección de aplicaciones utilizando un Firewall de Aplicación.

Por supuesto, estas medidas se aplican más a un enfoque de desarrollo de un sitio web propio, en el cual se tiene el control de las entradas y núcleo del sistema. Utilizar una plataforma como Magento o WooCommerce permite delegar esas funciones pero sólo si están actualizadas a la última versión, porque son precisamente esos problemas los que se corrigen en cada iteración.

DESARROLLAR CON CMS O SIN CMS

En estos días, el desarrollo web se ha orientado considerablemente a la utilización de gestores de contenido (CMS por sus siglas en inglés). El más popular para comercio electrónico es Magento, que ha sido la plataforma de desarrollo de comercio electrónico desde hace varios años. Los problemas de seguridad aplican también a este tipo de plataforma y es importante tener en cuenta las medidas preventivas que se pueden tomar. En números anteriores también se han discutido consejos de seguridad que se refieren a este tipo de tecnología.

Se puede argumentar que usando estas plataformas prefabricadas es "menos seguro" porque la aplicación web se expone a problemas conocidos por miles de personas y es posible explotarlos con mayor facilidad; esto es cierto, pero con reservas. Desarrollar una aplicación web sin usar gestores de contenido especializadas en comercio implica que se deben tomar las precauciones mínimas para el manejo de entradas para evitar problemas de inyección y otras vulnerabilidades.

Es cierto que el mayor número de vulnerabilidades se encuentran en los gestores de contenido por su popularidad, pero hacerlo sin ellos tampoco es garantía de que sea más seguro. La complejidad de las transacciones monetarias, la gestión de cuentas de clientes del comercio en línea, inventarios y otros

factores derivados de ser una tienda en línea, hacen que una aplicación derivada de un desarrollo propio sea difícil diseñar, implementar y mantener. Por un lado, parecería que al tener un mayor control del desarrollo se puede prevenir vulnerabilidades, pero en el caso particular de una tienda en línea, la complejidad y tamaño de este tipo de proyectos supera a una página web convencional. Además de esto, encontrar recursos humanos para el desarrollo propio no siempre es sencillo por las capacidades necesarias para llevarlo a cabo. Una aplicación personalizada puede fácilmente salirse de un presupuesto ajustado.

Por estas razones parece inevitable, al menos considerar, el uso de un gestor de contenidos para un proyecto de comercio en línea.

MERCADO DE COMPLEMENTOS Y PLANTILLAS

Si se decide usar un CMS debe tomarse en cuenta consideraciones de seguridad al utilizar plantillas (cf. *templates*) y complementos (cf. *plugins*). El uso de estos elementos en el desarrollo web a través de un CMS es común y en el caso de tiendas en línea, los complementos y plantillas normalmente tienen un costo; esto último es porque las plantillas y los complementos están orientados a generar un ingreso al ser para una tienda en línea.

El consejo de prevención que se da normalmente es tratar de mantener los complementos y plantillas siempre actualizados, del mismo modo que el motor principal del CMS. Éste es un buen consejo y debe ser el primer paso, pero también es importante elegir complementos con una reputación bien establecida y con soporte del autor o de la comunidad.

Para el caso particular de tiendas en línea también es importante considerar el mercado de complementos y plantillas comerciales. Por la naturaleza de la distribución de estos elementos, la piratería no es rara en este tipo de desarrollo y puede ser una preocupación más para el desarrollador y el dueño del recurso.

No se hablará de los problemas legales o éticos de piratear complementos o plantillas [1] ya que este tema puede tener muchas implicaciones a tratarse en otro momento. El tema es delicado pero es necesario hablar claro al respecto: en México la piratería es un problema común y un desarrollador con presupuesto restringido o con poca experiencia puede verse tentado a descargar una copia ilegal de estos elementos para construir una tienda en línea.

Una posible solución a este problema es transferir la responsabilidad de la infraestructura de la tienda a un tercero, de esta manera las actualizaciones, complementos y varias cuestiones de desarrollo se transfieren a esas entidades. Algunas plataformas que se pueden utilizar para ofrecer productos son Amazon, eBay o Mercado Libre. Esta alternativa permite la venta de productos en línea, pero restringe el formato en el que se mostrará y la manera de procesar los pagos. La elección de estas tecnologías dependerá del objetivo del negocio y de los productos que se quieren poner en venta. Por otro lado, se puede requerir cierto tipo de personalización en la tienda en línea, es ahí donde entra la alternativa de

Software como Servicio.

DESARROLLO CON SOFTWARE COMO SERVICIO

Las soluciones que ofrecen compañías como Shopify, Volusion, Square Space y muchas más transfieren la administración y mantenimiento de la infraestructura tecnológica a una de estas empresas. Para contar con una tienda en línea, el usuario sólo debe subir sus productos y personalizar el funcionamiento de acuerdo con sus necesidades.

Esta alternativa es un poco más restringida que el desarrollo personalizado que se analizó antes, pero tiene la ventaja de poder personalizar más que en comparación con los servicios de sitios como Mercado Libre o Amazon, que no lo permiten. El modelo de negocio de estos sitios generalmente incluye una cuota mensual y posiblemente una cuota adicional por transacción (un porcentaje de cada venta). Por otro lado, servicios como estos no permiten acceder al sistema operativo o a las características internas de la arquitectura.

La forma de monetizar el servicio en estas empresas da la percepción de ser más costosas que las opciones anteriores, principalmente porque tecnologías como Magento o WordPress son de código abierto y de distribución libre. Sin embargo, debe considerarse cuidadosamente el precio real de desarrollar una tienda con software libre. El conocimiento necesario para desarrollar un sitio con herramientas de código abierto es considerable si se compara con servicios como Shopify.

La ventaja de usar Software como Servicio desde el punto de vista de seguridad es que las actualizaciones, parches y mantenimiento en general corren a cargo de estas empresas. Si se toma en cuenta que una tienda tiene el propósito de generar ingresos, puede ser visto como una inversión para poder ofrecer productos en línea de manera segura.

CONCLUSIÓN

La decisión de ofrecer productos por Internet es un paso importante para una empresa en crecimiento y va de acuerdo con las tendencias del mercado global. Debe pensarse bien cuáles son los requerimientos y el objetivo de contar con una tienda en línea, para elegir el servicio que pondrá en marcha la tienda en línea.

La responsabilidad de las empresas de tecnología y equipos de desarrollo para cubrir esta necesidad es cuidar la información de sus clientes. Por ello es conveniente tomar en cuenta las recomendaciones mínimas para proteger la información durante todo el ciclo de desarrollo y mantenimiento de este tipo de sistemas.

REFERENCIAS

Aliysa. (2014, November 27). The Dangers of Pirate Plugins and Themes. *Tsohost*. Recuperado de https://www.tsohost.com/blog/the-dangers-of-pirate-plugins-and-themes

AMIPCI. (2015). Estudio de Comercio Electrónico. *AMIPCI (Asociación Mexicana de Internet)*. Recuperado de https://www.amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_versi

Coordinación de Seguridad de la Información/UNAM-CERT. (2014). Recomendaciones de seguridad para WordPress. *Seguridad de la Información*. Recuperado de http://www.seguridad.unam.mx/documento/?id=1927

Díaz, S. (2013, 5 de marzo). Firewall de Aplicación Web - Parte I. *Revista. Seguridad Cultura de Prevención para TI, 16*. Recuperado de http://revista.seguridad.unam.mx/numero-16/firewall-de-aplicaci%C3%B3n-web-parte-i

Espinosa, C. y Valdés, M. (2009, 9 de agosto). Tips para Evitar Fraudes en Línea. *Revista .Seguridad Cultura de Prevención para TI, 02*. Recuperado de http://revista.seguridad.unam.mx/numero-02/tips-para-evitar-fraudes-en-l%C3%ADnea

Hughes, M. (2014, May 20). How To Tell If Your WordPress Theme Is Legal (And Why You Should Care). *MakeUseOf*. Recuperado de http://www.makeuseof.com/tag/tell-wordpress-theme-legal-care/

OWASP. (2010). Top 10 2010. *OWASP*. Recuperado de https://www.owasp.org/index.php/Top_10_2010

———. (2013). Top 10 2013. *OWASP*. Recuperado de https://www.owasp.org/index.php/Top_10_2013

Ramírez, D. y Espinosa, C. (2011, 5 de marzo). El Cifrado Web (SSL/TLS). *Revista .Seguridad Cultura de Prevención para TI, 10.* Recuperado de http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

UNCTAD. (2015). Informe sobre la economía de la información. *United Nations Conference on Trade and Development (UNCTAD)*. Recuperado de http://unctad.org/es/PublicationsLibrary/ier2015_es.pdf

Wikipedia. (2016). Sistema de gestión de contenidos. *Wikipedia, la enciclopedia libre*. Recuperado de https://es.wikipedia.org/w/index.php?title=Sistema_de_gesti%C3%B3n_de_contenidos&oldid=90567306

———. (2016). Software as a Service. *Wikipedia, the Free Encyclopedia*. Recuperado de https://en.wikipedia.org/w/index.php?title=Software_as_a_service&oldid=708416639

SI QUIERES SABER MÁS CONSULTA:

- Tips para Evitar Fraudes en Línea
- Fraude Electrónico
- ¿Intermedios para Transferencias Monterias?

[1] Pero puede consultar fuentes como The Dangers of Pirate Plugins and Themes (2014) o How To Tell If Your WordPress Theme Is Legal (And Why You Should Care) (2014).
