UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Universidad Autónoma de Nuevo León

Facultad de Ciencias Físico Matemáticas

Diseño Orientado a Objetos

Riesgos de Seguridad con JavaScript

Estudiante: Mario Erick Ayala Torres

Matrícula: 1678264

Grupo: 006 Aula: 413

San Nicolás de los Garza, N.L. A 04 de Octubre del 2017

Riesgos de Seguridad con Javascript

En un principio, JavaScript fue creado para hacer de las páginas web más “dinámicas”, haciendo que sus usuarios vean más “viva” la página, teniendo un mayor atractivo visual, lamentablemente también es el blanco más preferido para la mayoría de los cibercriminales hoy en día, presentaremos algunos de los problemas que puede presentar una página cuando de tienen riesgos de seguridad con javascript.

Fraude

Existen formas en las que se utiliza JavaScript para engañar a los usuarios creyendo que entran a páginas completamente legítimas cuando realmente entran en una fabricada. En este caso no hay alternativa para este, ya que con tan solo copiar el código fuente de la página ya están prácticamente reconstruyendo la página web original, el resto es disfrazar y convencer a con ingeniería social para obtener sus datos.

Riesgos para el Usuario

Generalmente los riesgos del uso de javascript hacia un usuario, se refiere a que aquella página que tiene javascript en su interior puede perjudicar a la

información del usuario o al propio equipo, es decir, si entra en una página mal intencionada, con javascript habilitado se pueden hacer descargas en el browser y instalación de estas sin intervención del usuario, haciendo que se contagie de algún tipo de virus desconocido, aún este tipo de contagio puede ocurrir cuando hay anuncios en páginas que conectan a una página y a otra sucesivamente hasta llegar a una página que tiene estas instrucciones.

Esto sucede gracias a que Javascript tiene la particularidad de poder saltarse las herramientas de seguridad como extensiones o programas que bloquean pop-ups (elementos emergentes), afortunadamente muchos de estos podrían evitarse si se evitan bowsers como internet explorer, que no está preparado para la mayoría de este tipo.

Otro problema menor grave pero existente es al momento de entrar a una página, la ejecución de scripts pueden hacer que el celular se tarde en responder, hay páginas de juegos por ejemplo, que en una computadora normal puede correr un juego perfectamente, pero en celulares esto hace que se afecte la jugabilidad y la experiencia del usuario (UX) no sea grata al no estar bien adaptado como aplicación.

Ataques

Hay ataques que utilizando JavaScript hacen que desde la página web solicitada se generen instrucciones al servidor, inyectando código en espacios como formularios que, de no estar programada la página correctamente, se puede generar entre otras cosas consultas a la base de datos

Tomando en cuenta que JavaScript es una de las herramientas más habladas y utilizadas hoy en día, no es posible simplemente alejarse de estas tecnologías o crear una nueva. Estos riesgos en principal medida es un tema de actualización y buena programación por parte de los que administran la página, los programadores deben de ser más exigentes en el desarrollo de código seguro para estar más preparados, el usuario debe ser más consiente de las posibilidades que genera el entrar a páginas sospechosas y la ejecución de scripts de todo tipo.

Lamentablemente no existimos en un mundo completamente seguro, esto quiere decir que siempre se encontrarán nuevos riegos, nuevas amenazas y nuevos tipos de ataques entorno a la seguridad informática.

Bibliografía:

https://www.welivesecurity.com/la-es/2014/09/25/ataque-jquery-javascript-arma-doble-filo/

https://www.welivesecurity.com/la-es/2008/03/04/saltando-herramientas-seguridad-javascript/

http://letras-diferentes.info/computadoras/programacion-de-ordenadores/los-riesgos-con-javascript.php