UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Laboratorio de Diseño Orientado a Objetos

Riesgos/aspectos de seguridad con HTML y/o JavaScript

Nombre: Luis Guillermo Hernández Araujo

Matricula: 1682364

Fecha: 1/Septiembre/2017

Vulnerabilidades con HTML

HTML5 es una especificación muy conocida que permite a los desarrolladores crear aplicaciones del tipo RIA (Rich Internet Applications) y aunque incluye características que se encuentran soportadas en prácticamente todos los navegadores representa problemas de seguridad muy serios que en versiones previas de HTML5 no se presentaban.

CORS y ataques CSRF

SOP (Same Origin Policy) es una política que ha sido bastante efectiva a la hora de impedir que un dominio concreto pueda acceder a recursos de un dominio distinto. Por este motivo, gracias a SOP un dominio determinado no puede acceder directamente a los recursos (cookies, árbol DOM, comunicaciones, etc.) de un dominio distinto del suyo.

Ejemplo: Suponiendo que la víctima tiene abierto en su navegador varias pestañas con sitios web en los que se encuentra navegando, uno de dichos sitios tiene CORS habilitado y las respuestas a las peticiones incluyen la cabecera “Access-Control-Allow-Origin” con el valor “*” y otro de dichos sitios web es controlado por un atacante en internet

CORS y CORJacking

Otro tipo de vulnerabilidad que se presenta en las aplicaciones web RIA con HTML5 es la conocida como CORJacking, la cual consiste en la capacidad que tiene un atacante de modificar dinámicamente la estructura DOM de un sitio web con CORS habilitado y mal configurado. De esta forma. El atacante podrá modificar algunos atributos de los elementos cargados en el árbol DOM del sitio web con CORD habilitado e incorrectamente configurado, para controlar la interacción del usuario con los contenidos del sitio web vulnerable

En que afecta a los usuarios

Muchas de estas nuevas características recaen directamente sobre el navegador del cliente y habilitan un espectro de ataque mucho más amplio que con versiones antiguas de la especificación, algo que los atacantes en internet ahora buscan y explotan diariamente.

Vulnerabilidades con JavaScript

JavaScript es un lenguaje de programación que fue desarrollado justamente para hacer que paginas estáticas tengan un "comportamiento dinámico". Permite ejecutar códigos directa y automáticamente gracias a su interacción con el navegador utilizado para visitar la página.

Aunque de esta forma de ejecutar códigos sea más atractiva para el sitio y el usuario por cuestiones de velocidad, costos y la posibilidad de saltar pasos que muchas veces son molestos (como permitir o denegar la ejecución de ActiveX), sucede que para un atacante, JavaScript es ideal para hacer precisamente lo que recién litábamos como una función benigna: saltar herramientas de seguridad

Ataque a jQuery

JQuery es una de las librerías online gratuitas de JavaScript más conocidas, permite a programadores utilizar su interfaz de programación y ofrecer contenido para una multitud de navegadores de forma simplificada.

El sitio RiskIQ reporto un ataque que redirigía a los visitantes de jQuery a un exploit kit conocido como RIG. Este exploit es utilizado por los atacantes para hacer que sitios legítimos infecten usuarios con malware sin que lo noten.

JQuery admite que hubo un ataque el 18 de septiembre, y que el sitio estuvo fuera de servicio para la búsqueda y eliminación de posibles amenazas. Sin embargo, también afirma que, hasta el momento, no hubo reportes de malware distribuido a través de su sitio

En que afecta a los usuarios

Los códigos pueden explotar múltiples vectores al mismo tiempo, según las características del navegador utilizado y su interacción con la página web. En otras palabras, no hace falta propagar el código a varios sitios; con tan solo estar presente en un sitio de uso masivo, es posible atacar a muchas víctimas y robar nombres de usuarios y contraseñas o capturar contraseñas ingresadas en el teclado, entre otras cosas.

Como evitarlo

- Evitar hacer clic en enlaces sospechosos
- Ningún banco solicita actualización de datos por correo
- No escribir número de tarjetas ni contraseñas por correo
- Evitar usar ciber para entrar a las cuentas de correo
- Las preguntas de seguridad en caso de olvido de contraseña no deben des obvias
- No instalar programas de dudosa procedencia
- Mantener actualizado el antivirus y software
- Utilizar contraseñas seguras

Bibliografía

https://thehackerway.com/2014/10/08/vulnerabilidades-comunes-en-html5-configuraciones-inseguras-con-cors-parte-1/

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

https://es.linkedin.com/pulse/15-consejos-para-evitar-ser-hackeado-fernando-men%C3%A9ndez-cu%C3%A9llar