Universidad Autónoma de Nuevo león

Facultad Ciencias Fisco Matemático

DOO

LSTI

Miguel Salazar

Edgar Vázquez Márquez

1657462 Grupo: 006 Aula: 101

Domingo 03 de Septiembre de 2017

San Nicolas, Nuevo León

Los riesgos/aspectos de seguridad con html y/o javascript

Hay algunas amenazas que evolucionan con el paso del tiempo, como la tecnología que intentan comprometer. La CVE incluye más de 50000 amenazas conocidas contra la seguridad de la información.

Mientras que las técnicas usadas para acceder a datos y modificar código varían considerablemente, por lo general una infracción de seguridad tiene uno de los siguientes cuatro objetivos:

- Acceso a bases de datos y robo o corrupción de datos personales o confidenciales
- Modificar el código de un sitio web con el fin de cambiar lo que los usuarios ven
- Interceptar datos personales y confidenciales
- Ataques de denegación de servicio (DoS) que deshabilitan la disponibilidad de los servicios

Algunos riesgos serian:

Datos e información valiosa

Cuanto más valiosa sea la información en la base de datos, mayores serán las probabilidades de que la información sea blanco de muchos ataques. La base de datos es más atractiva para los hackers que puedan utilizar o vender esta información para su propia conveniencia. Algunos comercios electrónicos y otros sitios web cobran para proteger a los consumidores contra este tipo de amenazas.

Espionaje industrial y político

La información en sus bases de datos o servidores de su empresa puede no resultar útil para los defraudadores, pero puede ser muy útil para empresas, industrias o hasta gobiernos relacionados con su compañía o que compiten con usted. Los datos o nombres de usuario y contraseñas robadas pueden darle acceso a alguien a las cuentas y los datos de sus clientes, o a la inteligencia, archivos o correos electrónicos confidenciales de su organización.

Ataques “springboard”

Las pequeñas empresas tampoco son inmunes al espionaje. Las empresas con poca protección son cada vez más a menudo el trampolín a ataques más importantes contra organizaciones más grandes de las cuales son proveedores.

Riesgos en Javascript

Deshabilitar JavaScript previene que estas vulnerabilidades sean explotadas y reduce el riesgo de ataque. Si se hace esto a versiones actualizadas de Adobe Reader y Acrobat, puede proteger de futuras vulnerabilidades.

Conclusion

En conclusión, no se mucho de tema así que investigue y navegue en algunas páginas confiables y algunos no tanto. No encontré en si los riesgos asi que puse algunas que en mi opinio son algunos objetivos o lo que quieren los que están detrás del ataque.

Bibliografia

Garfinkel, S., Spafford, G., & Riverol, M. C. (1999). *Seguridad y Comercio en el Web*. McGraw-Hill.

https://www.seguridad.unam.mx/historico/documento/index.html-id=17

http://blog.iweb.com/es/2014/02/seguridad-web-amenazas/2457.html