

U.A.N.L.

Facultad de ciencias Físico-Matemático

Nombre del alumno: Jorge Mario Quintanilla Rios

Nombre del maestro: Ing. Miguel Salazar

Nombre de la asignatura: DOO(Diseño Orientado a Objetos)

Grupo:

Salón:

Numero de tarea: #2

# Riesgo y Vulnerabilidades presentes en html y / o javascript:

Primero que nada se tiene que explicar que es un riesgo y una vulnerabilidad:

El riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

El riesgo se utiliza sobre todo el análisis de riesgos de un sistema informático. Esté riesgo permite tomar decisiones para proteger mejor al sistema. Se puede comparar con el riesgo límite que acepte para su equipo, de tal forma que si el riesgo calculado es inferior al de referencia, éste se convierte en un riesgo residual que podemos considerar cómo riesgo aceptable.

Vulnerabilidad:

Una vulnerabilidad es el concepto que se aplica a un hueco de seguridad ya bien conocido y que si no se es manejado con cuidado es posible aprovecharte de tal vulnerabilidad para tu aprovechamiento es muy bien sabido los tipos de vulnerabilidades que a continuación se verán.

|  |  |
| --- | --- |
| HTML | JAVASCRIPT |
| La agencia europea ENISA  Analizo la infraestructura del html5 y detecto 50 vulnerabilidades a explotar en un reporte de 61 hojas (solo se pondrán las primeras 3 ):  Deshabilitando la protección de click-jacking:  Se refiere a un elemento Window es vulnerable al click-jacking osea al redierccionamiento de pagina por lo general a una pagina maliciosa  HTML5 Form Tampering:  Debido a que en html 5 ahora se permite meter botones afuera del form usando una inyección de html es mas fácil atraer al usuario final a rellenar campos con fines maliciosos  Geo-Location Cache polling : Se puede acceder a la cache de la api de la geolocalización que permote literalmente extarer la ultima localización del usuario final  Link de la lista de vulnerabilidades (sitio oficial): <https://www.enisa.europa.eu/publications/a-security-analysis-of-next-generation-web-standards> | Xss: cross-site-scrpting es uno de los mas utilizados hoy en dia y el chiste es hayar alguna vulnerabilidad dentro de la pagina web por malas practicas ejemplo el no validar los campos de los usuarios el no realizar este tipo de practicas conlleva a riesgos del tipo en el cual puedes modificar datos dentro de una pagina web, o puedes ejecutar código de lado de la maquina cliente. |
| Las vulnerabilidades registradas dentro de javascript también se registra código inseguro por parte de las librerias de jquery las cuales permiten junto a xss ejecutar ventanas emergentes las cuales roban datos |

En cuanto a vulnerabilidades dentro de javascript las recomendaciones serian:

* Actualizar constantemente javascript y sus componentes.
* Dejar de utilizar cuentas con permisos de administrador.
* Deshabilitar javascript cuando no sea necesario de utilizar.
* Utilizar complementos de navegador los cuales te permiten escoger si quieres utilizar javascript.

En cuanto a vulnerabilidades dentro de html las recomendaciones serian:

* Tener mucho cuidado con los permisos que otorgas a las paginas en las cuales ingresas
* Evitar utilizar las opciones de autoguardado de los navegadores en general

¿Qué implica para los desarrolladores?

Representa un reto para los desarrolladores ya que es reformular una gran parte del pensamiento integrado para la estructura bajo la cual se maneja HTML5

¿Qué implica para los usuarios?

Puede implicar varias cosas en cuanto a los usuarios puede ser una manera de actualizarse en cuanto a la tecnología y poder complementarlo con extensiones para proteger su información que viaja a través del explorador o puede ser algo abrumador que no comprenda y no le interese.