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


Nombre: Gilberto Beltrán Marfileño

Matrícula: 1627097

Carrera: Lic. Seguridad en Tecnologías de Información

Grupo: 006

Salón: 413

Maestro: Lic. Miguel Ángel Salazar Santillán


Ciudad Universitaria, San Nicolás de los Garza 08 de septiembre del 2017

# Riesgos y Vulnerabilidades en HTML y JavaScript

## Ejecución remota del código

Como el nombre sugiere, esta vulnerabilidad permite que un usuario malévolo ejecute código arbitrario a nivel servidor y recupere cualquier información deseada que este contiene.
Ocasionalmente, es difícil descubrir esta vulnerabilidad durante el periodo de testeo de la aplicación web, estos problemas se descubren a menudo mientras que se hace una revisión del código de fuente.
Sin embargo, cuando testeamos nuestra aplicación Web debemos tener en cuenta y recordar esta vulnerabilidad.

## Plagio

Usuarios pueden acceder a su código fuente de la mayoría de navegadores web comunes, simplemente haciendo clic en el botón " Ver Código Fuente" . Los visitantes del sitio pueden, sin su conocimiento, copiar su código y hacerlo pasar como propio. Es poco lo que se puede hacer para combatir esto con excepción de ofuscar el código, o intencionalmente escribir el código de una manera que es difícil de leer y entender. Por supuesto, eso no impide que cualquier persona de mayor robo de su código, pero puede disuadir a alguien que quiera modificar su código. Debe tenerse en cuenta que este problema no existe cuando se trabaja con JavaScript embebido en dispositivos móviles.

## Cross-site scripting

XSS es un ataque de inyección de código malicioso para su posterior ejecución que puede realizarse a sitios web, aplicaciones locales e incluso al propio navegador. Sucede cuando un usuario mal intencionado envía código malicioso a la aplicación web y se coloca en forma de un hipervínculo para conducir al usuario a otro sitio web, mensajería instantánea o un correo electrónico. Así mismo, puede provocar una negación de servicio (DDos).

Las diversas variantes de esta vulnerabilidad pueden dividirse en dos grandes grupos: el primero se conoce como XSS persistente o directo y el segundo como XSS reflejado o indirecto.

**Directo o persistente.** Consiste en invadir código HTML mediante la inclusión de etiquetas <script> y <frame> en sitios que lo permiten.

**Indirecto o reflejado.** Funciona modificando valores que la aplicación web pasa de una página a otra, sin emplear sesiones. Sucede cuando se envía un mensaje o ruta en una URL, una cookie o en la cabecera HTTP.

**Consideraciones como desarrollador**

La aplicación web que se desee implementar debe contar con un buen diseño. Posteriormente, se deben realizar diversos tipos de pruebas antes de su liberación, para detectar posibles fallos y huecos de seguridad, mediante el empleo de alguna herramienta automatizada. También, es conveniente proporcionar mantenimiento a la aplicación y estar actualizado en las versiones de las herramientas que se emplean para su puesta en marcha.

**Algunas recomendaciones para mitigar el problema, son:**

Emplear librerías verificadas o algún framework que ayude a disminuir el inconveniente. Por ejemplo: la librería anti-XSS de Microsoft, el módulo ESAPI de codificación de OWASP, Apache Wicket, entre otros.

Entender el contexto en el cual los datos serán usados y la codificación de los mismos, este aspecto es importante cuando se envían datos de un componente a otro de la aplicación o cuando se deben enviar a otra aplicación.

Conocer todas las áreas potenciales donde las entradas no verificadas pueden acceder al software: parámetros o argumentos, cookies, información de la red, variables de entorno, resultados de consultas, búsqueda de DNS reversible, peticiones enviadas en las cabeceras, componentes de la URL, correos electrónicos, archivos, nombres de archivo, bases de datos o algún sistema externo que proporcione información a la aplicación.