



UANL



FCFM

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

# UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

## Facultad de Ciencias Físico Matemáticas

### **Diseño Orientado a Objetos**

SEMESTRE: Agosto-Diciembre 2017

MTRO: Miguel Salazar

ACTIVIDAD: Ensayo Semana 3

Grupo: 006

ALUMNO: José Santiago Vazquez García

SAN NICOLÁS DE LOS GARZA, NUEVO LEÓN A 3 de septiembre de 2017

## Tipos de amenazas a la seguridad

Las amenazas a la seguridad evolucionan tan rápido como la tecnología que intentan comprometer. La base de datos CVE (Vulnerabilidades y Exposiciones Comunes) incluye de por sí más de 59.000 amenazas conocidas contra la seguridad de la información, y una búsqueda en la base de datos de apache devuelve una lista de más de 500 vulnerabilidades conocidas.

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

## Sobre la Encriptacion de Códigos JS y HTML

La encriptación de código HTML y JavaScript consiste en convertir todos los caracteres a una tabla de equivalencias no legible para humanos, y utilizar una pequeña función para su visualización en los navegadores Web.

De esta manera el código original queda oculto para cualquiera que observe la fuente HTML de la página, y por la complejidad (menor, pero existente) de su implementación previene copias y ofrece cierta privacidad y protección de autoría.

La protección ofrecida por este tipo de implementaciones no evita su decodificación (recuperación del código original) por parte de programadores con conocimientos en el tema.

Al pasar los datos a través de jQuery o de la API DOM del navegador, aseguramos que los valores están debidamente desinfectados y eliminamos la necesidad de inyectar snippets HTML inseguros en la página.



Para garantizar la seguridad de la aplicación, es recomendable usar la API DOM proporcionada por el navegador (o jQuery) para toda la manipulación DOM.

Aplicando esto el formulario web será mas seguro.

Con Post

<http://www.igdonline.com/blog/6-tips-para-mejorar-la-seguridad-de-tus-formularios-web/>

<http://www.igdonline.com/blog/6-tips-para-mejorar-la-seguridad-de-tus-formularios-web/>

