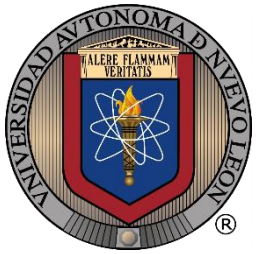



# APLICACIONES WEB

Tarea 1, DOO

Victor Hugo Martinez Garcia

Matricula: 1657393

Grupo: 006

El internet ha revolucionado el mundo informático y con ello también la sociedad, La programación de páginas web también ha evolucionado en estos pocos años pues han pasado de páginas sencillas, con unas cuantas imágenes y contenido estático a páginas con elementos multimedia además que ofrecen contenidos dinámicos adaptados a cada usuario individual.

Se le dice así a todas aquellas aplicaciones que los usuarios pueden utilizar accediendo a un Servidor web a través de Internet mediante un navegador. Es decir, es una aplicación (Software) que se codifica en un lenguaje soportado por los navegadores web en la que se confía la ejecución al navegador con el protocolo mediante el que se comunican (HyperText Transfer Protocol (HTTP)).

El protocolo HTTP forma parte de la familia de protocolos de comunicaciones Transmission Control Protocol/Internet Protocol (TCP/IP), que son los empleados en Internet. Estos protocolos permiten la conexión de sistemas diferentes, lo que facilita el intercambio de información entre distintos ordenadores.

# Tipos de Aplicaciones Web

a) **APLICACION WEB ESTATICA**
   Son aquellos sitios enfocados principalmente a mostrar una información permanente, donde el usuario se limita a obtener dicha información, sin que pueda interactuar con la página Web visitada.
   Pueden estar desarrolladas en HTML y CCS.
   En pocas palabras, solo muestra información y a veces imágenes, gift o videos.

b) **APLICACION WEB DINAMICA**
   Presenta la información a partir de una petición por el usuario de la página pues utilizan bases de datos para cargar información y estos se actualizan cada vez que el usuario accede a la web.

c) **TIENDA VIRTUAL/E-COMMERCE**
   La web desarrolla aplicaciones para permitir pagos electrónicos a través de tarjetas de credito, paypal,etc.
   Se crea una gestión para el administrador, pues el deberá subir los productos, actualizarlos o eliminarlos si es necesario.

d) **PORTAL WEB APP**
   Web donde existen accesos a diversos apartados, categorías o secciones.

# Vulnerabilidades de las Aplicaciones Web:

## XSS (Cross Site Scripting)

Este tipo de vulnerabilidad explota la confianza del cliente pues consiste en inyectar código, HTML o JavaScript en una aplicación web, con el objetivo de que el cliente ejecute el código inyectado al momento de ejecutar la aplicación.
Y esta vulnerabilidad puede ser usada para es redirigir a otro sitio y así robar información mediante phishing, hasta hacer que se descargue alguna amenaza y se ejecute en el sistema.

## INYECCION DE CODIGO

Consiste en insertar código que podría ser ejecutado por una aplicación.

Puede ser inyección de SQL donde se aprovecha de la sintaxis en este lenguaje para introducir comandos de manera ilícita que permitan leer o modificar la base de datos, comprometiendo el contenido de la consulta original.

## Buffer Overflow

Consiste en enviar datos superiores a los que pedía la aplicación, lo que provoca la sobrescrita de espacios unidos en la memoria. En las aplicaciones web, los atacantes explotan vulnerabilidades de este tipo para corromper la pila de ejecución de las aplicaciones web. Al enviar cuidadosamente datos de entrada a una aplicación web, el atacante puede causar que dicha aplicación ejecute código de una manera arbitraria y así hacerse de una manera efectiva del control del sistema.

## Comunicaciones Inseguras

Esto ocurre cuando las aplicaciones fallan al autenticar, cifrar, y proteger la confidencialidad e integridad de tráfico de red sensible.

Y es debido a la utilización de algoritmos débiles, certificados inválidos o no utilizados correctamente.

Para mejorar los tradicionales protocolos de red de forma que admitan cifrados habitualmente se utiliza el protocolo de túnel TLS (Transport Layer Security), también conocido como TLS/SSL (seguridad en capa de transporte, basado en el cifrado). Proporciona una seguridad ubicua, dando lugar a HTTPS, SMTPS o FTPS, entre otros.

## Ataques de fuerza bruta

El método de prueba y error es utilizado para obtener información de una contraseña, clave o número de identificación personal, entre otros. Funciona mediante la generación de un gran número de intentos consecutivos para el valor de los datos deseados. Un ataque de este tipo agota todas las posibilidades sin preocuparse por cuales opciones tienen mayor probabilidad de funcionar

# Conclusión

En conclusión, tenemos que estas son fallas del programador pues no es fácil hacer estas aplicaciones, ya que requiere por parte del programador, no sólo cumplir con el objetivo funcional básico de la aplicación, sino una concepción general de los riesgos que puede correr la información procesada por el sistema ya que no solo se pierde dinero, si no el prestigio de la aplicación.

## Bibliografía


Aguilar, A. (21 de Agosto de 2015). Obtenido de http://www.seguridad.unam.mx/documento-id=35

Luján, S. (2002). *Progamación de aplicaciones web:historia,principios básicos y clientes web.* San Vicente,España: Editorial Club Universitario.

OWASP. (3 de Febrero de 2014). Obtenido de https://www.owasp.org/index.php/Top_10_2013-A3-Cross-Site_Scripting_(XSS)