



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS



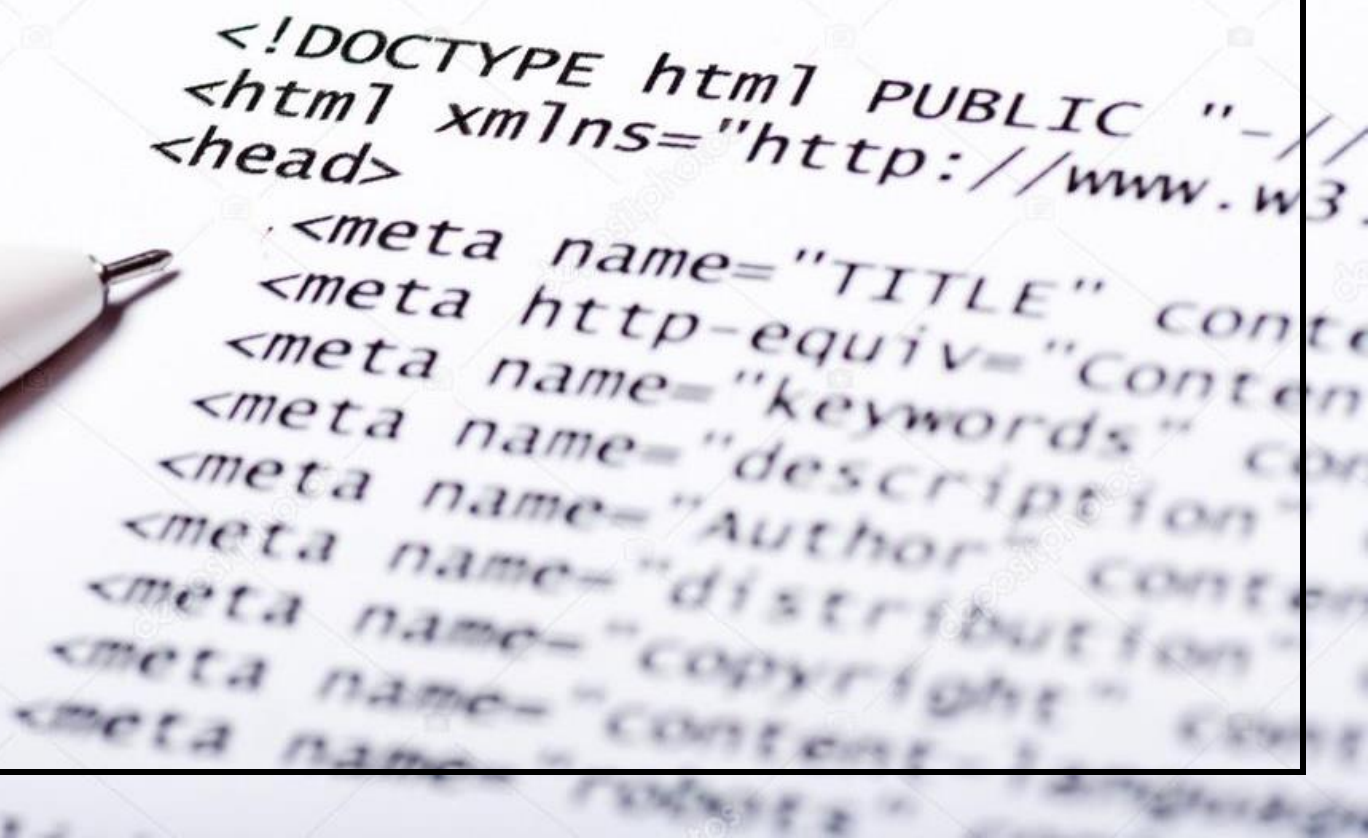
Universidad Autónoma de Nuevo León  
Facultad de Ciencias Físico Matemáticas

## Diseño Orientado a Objetos

Lic. Miguel Angel Salazar S.

### Tarea 1.- Aplicaciones de Software y Vulnerabilidades de Páginas WEB

JOSE ISRAEL RESENDIZ VALENCIA  
MATRICULA: 1757415



```
<!DOCTYPE html PUBLIC "-//  
<html xmlns="http://www.w3.  
<head>  
  <meta name="TITLE" conte  
  <meta http-equiv="Conten  
  <meta name="keywords" cor  
  <meta name="description"  
  <meta name="Author" conte  
  <meta name="distribution"  
  <meta name="copyright" con  
  <meta name="content-lang
```

## Introducción

A continuación, se llevará a cabo una investigación sobre vulnerabilidades más comunes de que pueda tener una página WEB y así también dentro de este documento veremos Aplicaciones de Software que como todos conocemos son los programas diseñados para los usuarios con el fin de facilitar la realización de tareas específicas en la computadora o actualmente por cualquier medio, en esta parte mencionare tres tipos de aplicaciones móviles (Nativa, Híbrida y WEB).

Justifico que utilizare la definición de Aplicaciones WEB de la clase.



## Aplicaciones de Software

Software construido sobre lenguajes soportados por un navegador web (*front-end*) y con soportado por código para el trabajo en el servido (*back-end*).

<i>front-end</i>	<i>back-end</i>
<ul style="list-style-type: none"><li>▪ HTML</li><li>▪ JS</li><li>▪ CSS</li></ul>	<ul style="list-style-type: none"><li>▪ Python</li><li>▪ Java</li><li>▪ .NET</li><li>▪ Ruby</li><li>▪ Node JS</li><li>▪ GO</li><li>▪ Scala</li><li>▪ Etc.</li></ul>

Tal como mencione en la introducción en esta parte trata de lo que son las aplicaciones móviles: nativas, híbridas y WEB. Además de este tipo de aplicaciones también están las de escritorio, console, entre otras.

### ¿Aplicaciones Nativas?

Las aplicaciones nativas son una aplicación que se desarrolla directamente en el lenguaje nativo de cada terminal, en si, si se desea desarrollar una App nativa se tiene que utilizar un lenguaje diferente para cada Sistema Operativo. Por ejemplo, los lenguajes de programación serian:

Android: Java

Windows: C# y Visual Basic .NET.

### ¿Aplicaciones Híbridas?

Las aplicaciones híbridas consisten en que contienen en su interior el navegador web del dispositivo. Y para su desarrollo se utilizan frameworks de desarrollo basados en lenguajes de programación web (HTML, CSS y JS).

### ¿Aplicaciones WEB?

Una aplicación WEB es la que se accede a través de una URL en el navegador del dispositivo (Safari, Chrome o el que sea) además se adapta al formato de la pantalla para que se tenga un mejor aspecto de navegación. Además, los navegadores de los móviles permiten crear accesos directos en nuestro escritorio de tal WEB, y es así la manera en la que se instala y es llamada como aplicación.

## **5 vulnerabilidades de Seguridad que pueda tener una Página WEB**

Por lo visto, no todo el error lo lleva el lenguaje que utilicemos si no, nosotros mismo, es decir que nosotros somos vulnerables ante cualquier ataque de nuestro sitio WEB:

### **1. Falta de actualizaciones de seguridad**

Al igual que con muchos tipos de defectos de seguridad, las vulnerabilidades en sitios web a menudo comienzan con aplicaciones que no están parcheados y se mantiene hasta la fecha. Un estudio reciente encontró que la explotación de software obsoleto era método más común que los hackers utilizan para atacar sitios web.

### **2. Reabren las vulnerabilidades**

Las vulnerabilidades encontradas existen por varias razones, como por ejemplo un mal código o configuraciones incorrectas. Y en algunos casos, cuando esos problemas se solucionan, se repiten de nuevo más tarde. De hecho, el 20% de las vulnerabilidades descubiertas por WhiteHat se solucionaron pero volvieron abrirse más adelante en algún momento. Eso pasó por una variedad de razones, tales como que se corrige el problema del código, pero luego se sobrescriben durante una actualización de software o si hay una actualización restaura una configuración vulnerable que se había reparado previamente.

### **3. La falta de cortafuegos**

Uno de los puntos del informe de WhiteHat señala que muchas de las vulnerabilidades más comunes se pueden mitigar mediante el uso de un firewall de aplicaciones web (WAF). Como un firewall de red, protege el sitio web de los ataques maliciosos y los monitores de entrada y salida de tráfico. El informe estima que esta tecnología podría solucionar el 71% de las vulnerabilidades.

#### 4. Procedimientos de inicio de sesión defectuosos

Algunas de las vulnerabilidades en la lista de los 10 son causados por la inseguridad en los procedimientos de inicio de sesión, incluidos los de inicio de sesión en las sesiones con defecto de expiración, como se muestra por el último elemento de la lista. En otro ejemplo, estuvieron presentes muchas vulnerabilidades de fuerza bruta debido a que el sitio web de registro en la página reveló que el nombre de usuario o contraseña eran correctos o incorrectos. Dado que muchos sitios utilizan direcciones de correo electrónico como nombres de usuario, los spammers pueden utilizar estos sitios para extraer direcciones de correo electrónico válidas.

#### 5. La falta de conocimiento acerca de las vulnerabilidades

Mientras que las organizaciones en el estudio eran los clientes del servicio de monitoreo de WhiteHat y por tanto conocía sus problemas, muchas vulnerabilidades pasan completamente inadvertidos para los propietarios de los sitios web y los administradores. De hecho, más de la mitad de los administradores web no saben cuándo sus sitios son atacados, según una encuesta reciente de la empresa de seguridad Commtouch.

## Conclusión

En conclusión, las vulnerabilidades que en mi opinión son más importantes son las que añadí, pero entre otras cosas, las vulnerabilidades en las páginas WEB son:

- Cross-site scripting
- Filtración de información
- Contenido de suplantación de identidad
- Autorización insuficiente
- Cross-site request forgery
- Ataques de fuerza bruta
- Predecible localización de recursos
- Inyección SQL
- Sesión fijación
- Expiración de sesión insuficiente

Además de lo visto aquí, podemos notar que para la realización de una Aplicación, para que esta funcione adecuadamente debemos saber y aplicar los lenguajes de programación.



## Referencias

Software de Aplicación., de webcindario

Sitio web: [http://proyectoova.webcindario.com/software\\_de\\_aplicacin.html](http://proyectoova.webcindario.com/software_de_aplicacin.html)

Miguel Salazar. Diseño Orientado a Objetos.,

Sitio web: <http://migsalazar.com/DOO201709/slides/#/>

mario\_ba300. Aplicaciones., de emaze

Sitio web: <https://www.emaze.com/@AFFFIRWR>

(27 ago. 2012). 5 de fallas de seguridad de tu sitio WEB., de SEGU INFO

Sitio web: <http://blog.segu-info.com.ar/2012/08/5-de-fallas-de-seguridad-de-tu-sitio.html>