



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS



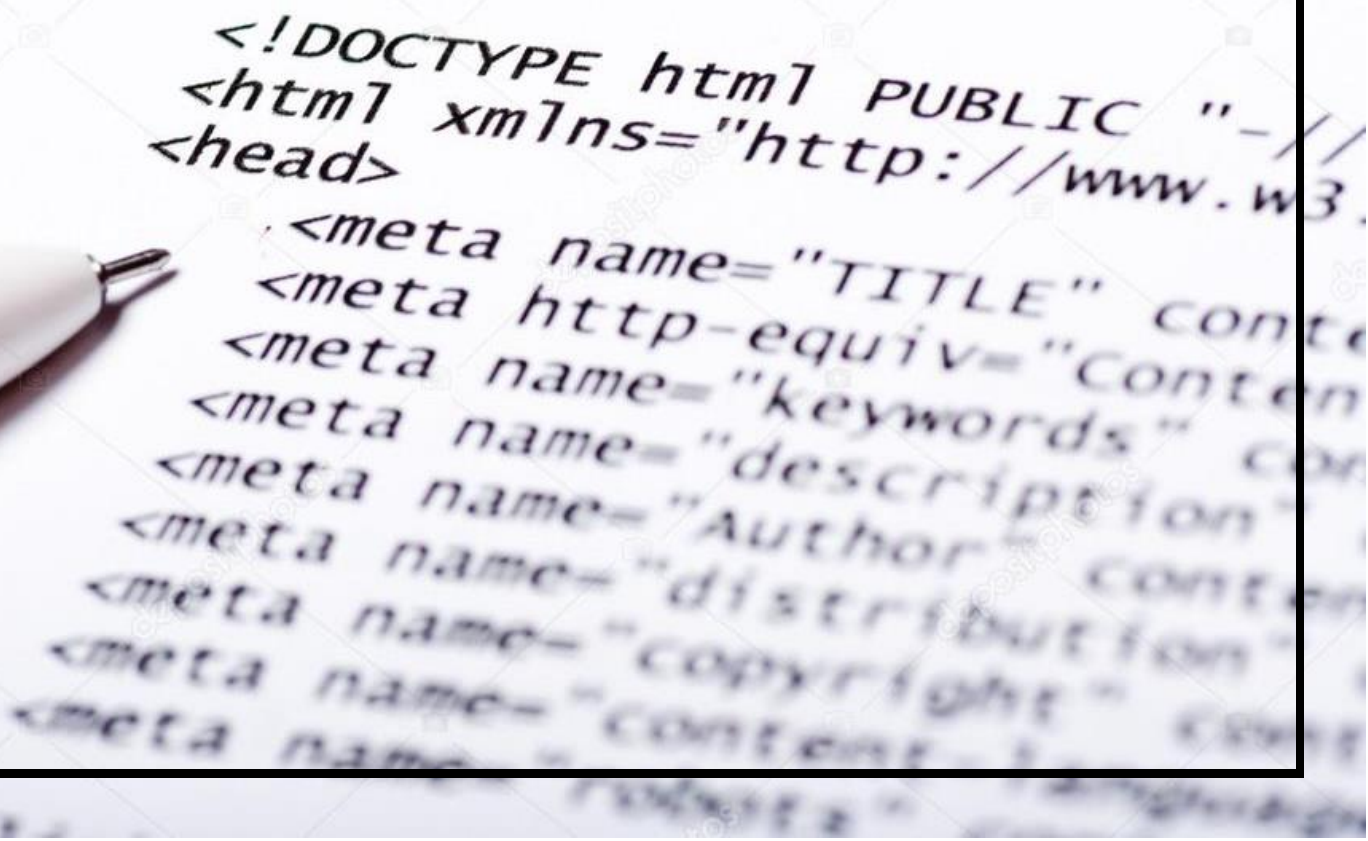
Universidad Autónoma de Nuevo León
Facultad de Ciencias Físico Matemáticas

Diseño Orientado a Objetos

Lic. Miguel Angel Salazar S.

Tarea 3.- Riesgos/Aspectos de Seguridad con HTML y JavaScript

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-type" type="text/html">
```

Introducción

El siguiente ensayo forma parte de la tercer tarea, donde se hizo una pequeña investigación sobre los riesgos y aspectos de seguridad que se podrían encontrar o aplicar, ya sea el caso, en el lenguajes HTML o JavaScript, como bien sabemos estos son muy aplicados en las aplicaciones o páginas web, por lo que hay que tener muy en cuenta aplicar la seguridad y los riesgos que podría conllevar al realizar cierta aplicación en caso de estar programando.



Riesgos/Aspectos de Seguridad con HTML y JavaScript

- ¿Cuáles son?:
 - Riesgos de Seguridad con:

HTML	JavaScript
<ul style="list-style-type: none">• Acceso a la información confidencial. (Sin protección)• Botones: es complicado distinguir entre un botón malicioso y otro real.• Problemas con la especificación y la aplicación de las políticas de seguridad.• Gestión de los permisos del sistema operativo.• Características que aún no son muy específicas, por lo que se puede conducir a errores.	<ul style="list-style-type: none">• El código JavaScript se ejecuta dentro del navegador, es decir, dentro del ordenador con el que se accede a la página.• La mayoría de las paginas utilizan JavaScript.• Cross scripting (XSS): se basa a explotar un mecanismo de seguridad habitual en la web. Se le concede determinados privilegios al contenido de cierto servidor web.• Los usuarios pueden acceder al código fuente en la mayoría de los navegadores.

- ¿Hay modo de evitarlo?

En mi opinión, no se mucho, pero, siempre hay que estar atentos de lo que realizamos en una página web, si es que vamos a descargar algo o hasta cuando buscamos información, ya que al estar navegado, accidentalmente podemos dar click en cualquier cosa, y sin saber es como darle permiso de que se descargue o de que este ejecutándose un malware sin que nos demos cuenta. Además, creo que si es muy necesario utilizar un antivirus hoy en día.

- Aspectos de:

HTML	JavaScript
Hace referencia al lenguaje de marcado predominante para la elaboración de páginas web que se utiliza para describir y traducir la estructura y la información en forma de texto, así como para complementar el texto con objetos tales como imágenes.	En el contexto de un sitio web, con JavaScript se puede hacer todo tipo de acciones e interacción. En sí, permite a las aplicaciones realizar todo tipo de efectos, interfaces de usuario y comunicación.

- ¿Qué implica para los desarrolladores?

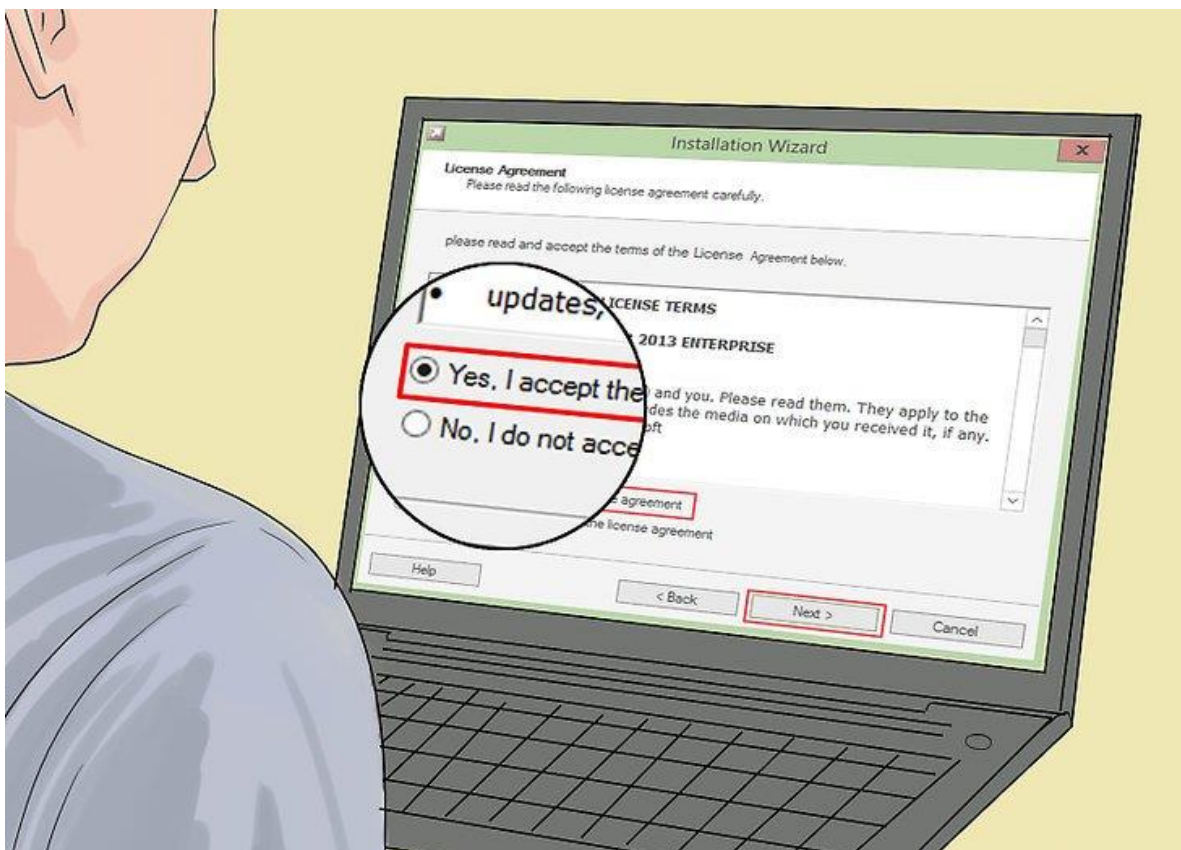
Que por pequeños detalles, podemos poner en peligro la seguridad de nuestra página web, aplicación u otro medio programable con lenguajes, así que es necesario crear y estar observando detalladamente lo que hacemos.

- ¿Qué implica para los usuarios?

La seguridad más que nada es importante, hoy en día vemos mucho el robo de identidad, por lo que a muchas personas les cuesta estar confiando en plataformas, ya sea de bancos, o de otras que traten con datos personales, creo que ese tema es de mucha importancia, ya que hay que generar confianza a los usuarios y mantener su confidencialidad.

Conclusión

En conclusión, tenemos que hoy en día la navegación por internet puede ser muy peligroso, y actualmente se han visto grandes riesgos tales como el robo de datos y hasta completamente el robo de identidad, debemos tener en cuenta que no siempre puede ser la mala programación en el lenguaje, y que puede ser desde pequeños detalles las vulnerabilidades. Simplemente para poder evitarlo es estar atento de lo que hacemos, descargamos y pues investigar de qué forma es más seguro navegar por internet.



Referencias

La ficha bibliográfica es:

jjvelasco (2011). El ENISA preocupado por la seguridad del HTML5., de hipertextual

Sitio web: <https://hipertextual.com/archivo/2011/08/el-enisa-preocupado-por-la-seguridad-del-html5/>

La ficha bibliográfica es:

XABIER GANZÁBAL GARCÍA. (2014). Desarrollo y reutilización de componentes software y multimedia mediante lenguajes de guion., de Google Books

Sitio web: [https://books.google.com.mx/books?id=o73-](https://books.google.com.mx/books?id=o73-CAAAQBAJ&pg=PA12&lpg=PA12&dq=riesgos+de+seguridad+con+javascript&source=bl&ots=hbfcTQYWb5&sig=krAABPLQv40Eoj2nQWb_Vbqb7DM&hl=es-419&sa=X&ved=0ahUKEwj7iPG_piTWAhURxWMKHTb6D4l4ChDoAQgmMAA#v=onepage&q=riesgos%20de%20seguridad%20con%20javascript&f=false)

[CAAAQBAJ&pg=PA12&lpg=PA12&dq=riesgos+de+seguridad+con+javascript&source=bl&ots=hbfcTQYWb5&sig=krAABPLQv40Eoj2nQWb_Vbqb7DM&hl=es-419&sa=X&ved=0ahUKEwj7iPG_piTWAhURxWMKHTb6D4l4ChDoAQgmMAA#v=onepage&q=riesgos%20de%20seguridad%20con%20javascript&f=false](https://books.google.com.mx/books?id=o73-CAAAQBAJ&pg=PA12&lpg=PA12&dq=riesgos+de+seguridad+con+javascript&source=bl&ots=hbfcTQYWb5&sig=krAABPLQv40Eoj2nQWb_Vbqb7DM&hl=es-419&sa=X&ved=0ahUKEwj7iPG_piTWAhURxWMKHTb6D4l4ChDoAQgmMAA#v=onepage&q=riesgos%20de%20seguridad%20con%20javascript&f=false)