Universidad Autónoma de Nuevo León

Facultad de Ciencias Físico Matemáticas

Lic. En Seguridad de Tecnologías de la Información

Tarea 5

Alumno: Roberto Iván Hernández Chavarría

Matricula: 1452359

Materia: Diseño Orientado a Objetos

Profesor: Lic. Miguel Ángel Salazar Santillán

Cookies

Una cookie es un fichero que se descarga en el dispositivo del usuario al acceder a determinadas páginas web para almacenar y recuperar información sobre la navegación que se efectúa desde dicho equipo.

Sus principales funciones son:

- Llevar el control de usuarios: cuando un usuario introduce su nombre de usuario y contraseña, se almacena una galleta para que no tenga que estar introduciéndolas para cada página del servidor. Sin embargo, una galleta no identifica a una persona, sino a una combinación de computadora de la clase de computación-navegador-usuario.
- Conseguir información sobre los hábitos de navegación del usuario, e intentos de *spyware*, por parte de agencias de publicidad y otros.

Tipos de *cookies*

- **De sesión (*session cookies*)**.– Son *cookies* que usualmente es eliminada cuando el navegador se cierra.
- **Persistentes (*persistent cookies*)**.– Estas son cookies que se mantienen a pesar de que el navegador sea cerrado. Se mantienen por un tiempo específico (tienen fecha de expiración), durante el cual una página puede conocer lo último que hiciste o algunas de tus preferencias. A este tipo de cookies también se les conoce como ***tracking cookies***, porque pueden ser usadas por compañías de publicidad para conocer tus hábitos de navegación.
- **Segura (*secure cookies*)**.– Estas son *cookies* que se usan únicamente con HTTPS(conexión cifrada).
- **De terceros (*third-party cookie*)**.– Las cookies que reciben este nombre se usan principalmente para páginas publicitadas, esto es: la página visitada crea una *cookie* a nombre de una página publicitada o, en otras palabras, el URL de la cookie es diferente al URL que ves en la barra de direcciones de tu navegador

Otros sitios web utilizan las *cookies* para personalizar su aspecto según las preferencias del usuario. Los sitios que requieren identificación a menudo ofrecen esta característica, aunque también está presente en otros que no la requieren. La personalización incluye tanto presentación como funcionalidad. Las *cookies* se utilizan también para realizar seguimientos de usuarios a lo largo de un sitio web.

Las compañías publicitarias utilizan *cookies* de terceros para realizar un seguimiento de los usuarios a través de múltiples sitios. En concreto, una compañía publicitaria puede seguir a un usuario a través de todas las páginas donde ha colocado imágenes publicitarias o *web bugs*. El conocimiento de las páginas visitadas por un usuario permite a estas compañías dirigir su publicidad según las supuestas preferencias del usuario

Inconvenientes de las *cookies:*

Identificación inexacta

Robo de *cookies*

Falsificación de *cookies*

Cookies entre sitios (*cross-site cooking*)

Sesiones

Una sesión es la duración de una conexión empleando una capa de sesión de un protocolo de red, o la duración de una conexión entre un usuario (el agente) y un servidor, generalmente involucrando el intercambio de múltiples paquetes de datos entre la computadora del usuario y el servidor. Una sesión es típicamente implementada como una capa en un protocolo de red (por ejemplo, telnet y FTP).

En los casos de los protocolos de transporte en donde no se implementa una capa de sesión formal (por ejemplo, UDP), o en donde las sesiones en la capa de sesión son generalmente de una vida corta (por ejemplo, HTTP), las sesiones pueden ser mantenidas por un programa de más alto nivel, usando algún método. Por ejemplo, un intercambio HTTP entre un navegador y un servidor remoto, puede incluir una cookie, que permite mantener una "sesión", con su identificador propio, datos del usuario, sus preferencias, etc.

El login es la opción y acción (logging in) de iniciar una sesión, generalmente empleando un nombre de usuario y contraseña.

El Transporte de comunicación puede ser implementado como parte de protocolos y servicios en la capa de aplicación, en la capa de sesión o en la capa de transporte en el modelo OSI.

- Ejemplos de capa de la aplicación:
  - Sesiones HTTP, los cuales dejan asociar información con visitantes individuales
  - Una sesión de login remoto mediante telnet
- Ejemplo de capa de sesión:
  - Un Protocolo de Iniciación de la Sesión (VOIP) en el que se basa una llamada de teléfono de Internet
- Ejemplo de capa de transporte:
  - Una sesión TCP, la cual es sinónimo a un circuito virtual TCP, una conexión TCP, o un socket TCP establecido.

En el caso de protocolos de transporte que no implementan una capa de sesión formal (p. ej., UDP) o donde las sesiones en la capa de aplicación son generalmente de un tiempo de vida muy corto (p. ej., HTTP), las sesiones se mantienen mediante un programa de más alto nivel que utiliza un método de intercambio de información definido. Por ejemplo, un intercambio de HTTP entre un navegador y un anfitrión remoto pueden incluir una cookie HTTP que identifica el estado, como una única sesión ID, información sobre las preferencias o nivel de autorización del usuario.

En la interacción de ordenador-humano, la **administración de sesión** es el proceso de mantener la pista de la actividad de un usuario a través de sesiones de interacción con el sistema de ordenador.

Hidden inputs

El atributo global **hidden** es un atributo Booleano que indica que el elemento todavía no está, o ya no es relevante. Por ejemplo, puede ser usado para ocultar elementos de la página que no pueden ser usados hasta que el proceso de login se haya completado. El explorador no dibujará dichos elementos.

Esta atributo no debe de usarse para ocultar contenido que pudiera ser legítimamente mostrado. Por ejemplo, no debe de ser usado para ocultar paneles de pestañas o una interfaz con pestañas, ya que esta es una decisión de estilo y otro estilo mostrándolos lo llevaría a una página perfectamente mostrada.

Los elementos ocultos no deben de ser vinculados desde elementos no ocultos y elementos que son descendientes de un elemento oculto todavía activo; lo que significa que los elementos del script pueden todavía ejecutarse y los elementos de formulario pueden todavía enviarse.

Estos datos pueden ser útiles para ayudar al programa en su gestión de los datos del formulario. Lo que hacen es comunicar cierta información al servidor sobre cómo tratar los datos manteniéndose ocultos a la vista de los usuarios.

Este tipo de datos ocultos no se muestran en la página, aunque sí pueden ser detectados solicitando el código fuente. El atributo hidden no se llega a usar en páginas escritas en html, sólo en las que empleen también otro tipo de lenguajes.

Parámetros en la URL

Los parámetros en la URL, son acciones o indicaciones en las cuales, por medio de un comando agregado en la barra de dirección, se puede acceder a lugares en los cuales no se podría o debería acceder normalmente.

Algunos tipos de parámetros en le URL son los siguientes:

- Los **parámetros de URL generales** transfieren información a su sitio web.
    - Por ejemplo, http://example.com?productid=1234 enviaría a alguien directamente a la página 1234 del producto en su sitio web.
- Los **parámetros de seguimiento de URL generales** registran la información de seguimiento sobre el anuncio, pero no los crea Google.
    - Por ejemplo, http://example.com?utm_source=google usa un parámetro común ("utm_source=xyz") que registra el sitio del que procede un usuario.
- Los **parámetros de ValueTrack** registran información sobre su anuncio que se basa en el parámetro que utiliza.
    - Representan el valor en un parámetro de URL (por ejemplo, "{network}" en el parámetro de URL "network= {network}"). El parámetro {network} registrará la red de la que procede el clic (Red de Búsqueda o Red de Display) en la URL de la página de destino del anuncio.

Una vulnerabilidad de este tipo, es que en alguna página web que esté mal programada, al analizar la dirección, se puedan descubrir elementos los cuales no deberían estar ahí, como por ejemplo usuarios o contraseñas, o redirecciones que deberían de estar ocultas, por lo que sería fácil acceder a estos elementos, o modificar la página en su estructura en general, para poder realizar acciones que no deberían hacer estar permitidas.