UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Universidad Autónoma de Nuevo León

Facultad de Ciencias Físico Matemáticas

Licenciatura en Seguridad en Tecnologías de Información

Diseño Orientado a Objetos

Maestro: Miguel Salazar

Ensayo

Nombre: Daniel de la Rosa Rodríguez

Matrícula: 1666385

9 de octubre de 2017, Cd. Universitaria, San Nicolás de los Garza, Nuevo León

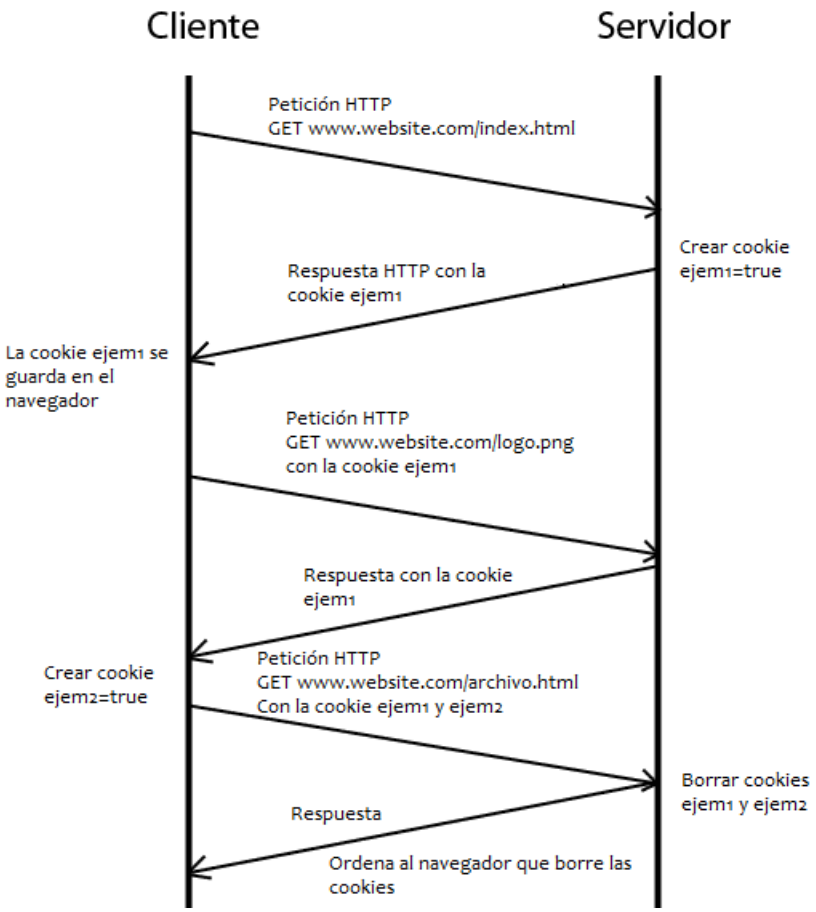
Una ***cookie*** es un pequeño archivo con información que se almacena en el navegador del usuario cuando visita un sitio web y suele guardar configuraciones y preferencias del usuario o el estado de sesión de navegación. Los archivos que forman webs viajan a través de redes encapsulados dentro de paquetes de información que usan el protocolo **HTTP**. Una de las formas de mantener el estado y permitir que el contenido de una misma **URL** cambie según las acciones del usuario son las cookies.

Una cookie está formada por una clave que le da un nombre y un valor, que se crea, modifica o borra tanto el cliente como el servidor. Una vez creada, se envía en cada petición HTTP como parámetro de este protocolo.

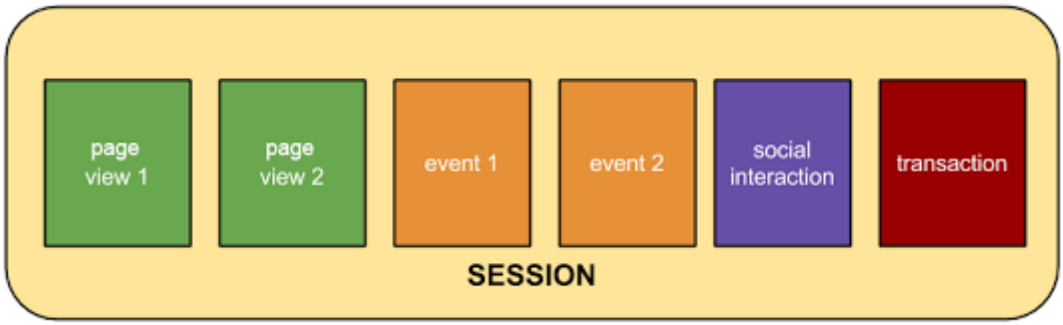
Una cookie puede ser persistente o no persistente. Si son persistentes tienen un tiempo de expiración, si no, no lo tienen, se borran al momento en que el navegador se cierra. Las cookies no persistentes son las que se usan para mantener abierta la sesión del usuario.

Las cookies van siempre asociadas de un dominio y solo pueden crearse, modificarse o borrarse si pertenecen al mismo dominio o subdominio del nivel superior.

Ejemplo gráfico cuando se crea una cookie en el cliente y servidor:



Una **sesión** es un conjunto de interacciones que tienen lugar en el sitio web en un periodo determinado. Una única sesión puede contener varias páginas visitadas, eventos, etc. Es el elemento que engloba las acciones del usuario en un sitio web. Es el intercambio de información, también conocido como dialogo entre dos o más dispositivos de comunicación. Es un requisito básico para realizar una comunicación orientada a conexión.



Un único usuario puede abrir varias sesiones, que pueden ocurrir el mismo día o en varios, días, semanas o meses. En cuanto finaliza una sesión, es posible empezar otra nueva.

Cuando un usuario permanece en el estado de registrado después de un tiempo no razonable (por ejemplo, cuando no expira la sesión), tenemos un problema de registros persistentes.

Este tipo de problemas disminuyen la seguridad de nuestro mecanismo de autenticación. Generalmente son causados por una cookie persistente, un ticket enviado al usuario o alguna variable de sesión establecida que no se considera como expirado jamás o que no cambia en cada nuevo registro establecido por el usuario.

Las cookies permanentes y variables de sesión ayudan a los sitios web a recordar tu información y ajustes cuando los visitas más adelante. Esto conlleva un acceso más rápido y sencillo ya que, por ejemplo, no tienes que iniciar sesión de nuevo.

La implementación de sesiones permite dar seguimiento al usuario, permite mantener valores de variables a través del sitio (sin tener que emplear campos ocultos en formularios), así como restringir el acceso a determinados elementos.

Es muy importante dar seguimiento a la sesión, así como iniciarla y terminarla de forma correcta, para evitar su posible secuestro.

El elemento ***input*** teniendo el valor "*hidden*" en su atributo *type* representa cualquier cadena de texto arbitraria que no está pensada para ser vista o editada por el usuario. Los controles ocultos son especialmente útiles para enviar datos al servidor definidos por el autor, basados o no en la interacción con el usuario

A menudo, los anunciantes añaden parámetros a sus URL para enviar datos a la página de destino. Los **parámetros de URL** constan de una clave y un valor separados por un signo igual (=) y unidos por el signo (&). El primer parámetro siempre aparece después de un signo de interrogación en una URL. Por ejemplo, la siguiente URL incluye un código de producto:
`http://example.com?sid=1234567`

En este ejemplo, la página de destino puede tener un script que hace que muestre información sobre el producto identificado mediante el parámetro de URL `sid.`

- Parámetros dinámicos específicos del motor.
- Parámetros estáticos que hagan referencia a sus propias campañas de marketing, códigos de productos u otro tipo de información de seguimiento interno que quiera añadir a la página de destino.

En conclusión, la seguridad en aplicaciones Web involucra principalmente al desarrollador, aunque con gran frecuencia se encuentran defectos que pueden ser aprovechados por atacantes en las tecnologías en que se basan los sistemas web (Sistemas Operativos, Servidores Web, Servidor de Base de Datos, etc.) la atención principal debe dirigirse a los defectos propios al desarrollo nuestras aplicaciones.

Todo programador debe estar consciente que el manejo de las peticiones, para aceptarlas o rechazarlas, deben estar los datos o variables recibidas no cumplan con las características esperadas o predefinidas. Todas las entradas del sistema deben pasar por el filtrado de los datos contenidos para confirmar su usabilidad. Además, para el programador debe ser claro y fácil de identificar cuando una variable ya ha sido sometida al proceso de limpieza, de esta forma evitaremos tener que confiar en la memorización o tener que hacer un mapa de los procesos ejecutados por cada línea de código ejecutada de manera previa.

Otro aspecto importante por considerar son los procesos de salida de la información del sistema. Es importante siempre considerar el significado que pueda tener la información enviada en su nuevo contexto, y en el caso de poder crear problemas de interpretación de las salidas, escaparlas para preservarlas. Al igual que en el proceso de filtrado, es importante mantener un control sobre la codificación que tienen los datos antes de enviarlos a su nuevo contexto.

Referencias

- Navegación Segura: entendiendo las Cookies, Rosendo Méndez López, UNAM-CERT, noviembre 2004
- Sugerencia de Seguridad para Sitios Web, Andrés Hernández, UNAM-CERT, junio 2013