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

Nombre: Gilberto Beltrán Marfileño

Matrícula: 1627097

Carrera: Lic. Seguridad en Tecnologías de Información

Grupo: 006

Salón: 413

Maestro: Lic. Miguel Ángel Salazar Santillán

Ciudad Universitaria, San Nicolás de los Garza 10 de octubre del 2017

Seguridad en Aplicaciones Web: comunicación entre cliente y servidor

El Cliente-Servidor es un sistema distribuido entre múltiples Procesadores donde hay clientes que solicitan servicios y servidores que los proporcionan. La Tecnología Cliente/Servidor, es un modelo que implica productos y servicios enmarcados en el uso de la Tecnología de punta, y que permite la distribución de la información en forma ágil y eficaz a las diversas áreas de una organización, así como también fuera de ella.

Una de las técnicas para lograr estas conexiones es la utilización de las llamadas cookies. Las cookies son unos archivos de texto que genera el navegador y se almacenan en el disco duro, éstas sirven como una tarjeta de identificación, para reconocerte a ti de entre todos los usuarios que entran a una página, gracias a las cookies basta con que te registres una sola vez en un sitio para que recuerde tu nombre de usuario, contraseña, preferencias de sistema, etc.

Hoy en día se tiene la idea de que las cookies son una especie de malware o virus, pero esto es totalmente falso, ya que las cookies no tienen ningún código ejecutable y por lo tanto es imposible que pueda dañar nuestro equipo o software. Sin embargo, sí tienen la capacidad de realizar seguimientos de los movimientos que realiza el usuario dentro de un sitio, lo cual puede ser recopilado y usado con fines ajenos a su propósito original.

Otro método que se utiliza son las sesiones, las sesiones son una forma más de paso de variables de una página a otra. Una sesión es una variable que se crea en el servidor y esta variable puede ejecutarse sin que el usuario de la Web tenga conocimiento alguno de ello. Las variables de sesión tienen caducidad, que esta predeterminada en el servidor y se auto-elimina pasados unos 20 minutos aproximadamente de inactividad. Inactividad significa no estar navegando en la página, mientras pases de una página a otra, la sesión estará activa. La única forma que tiene la página web de reconocer a un usuario es por medio de su identificador de sesión.

Si un atacante consigue el identificador de sesión de un usuario que ya está autenticado, puede hacerse pasar por él y entrar en su cuenta sólo con hacer que su navegador envíe el identificador a la página web, ya sea a través de la URL o de una cookie.

Algunas técnicas se utilizan a la hora de estar creando una página web, en el código fuente, tal es el caso de las Hidden Inputs. Los elementos de este tipo permiten a los desarrolladores web incluir datos que no pueden ser vistos o modificados por los usuarios cuando se envía un formulario. Las entradas ocultas son completamente invisibles en la página renderizada, y no hay forma de hacerlo visible en el contenido de la página. Las entradas ocultas se pueden utilizar en cualquier lugar que desee

incluir datos que el usuario no puede ver ni editar junto con el formulario cuando se envía al servidor.

Debido a las malas prácticas de codificación, los campos ocultos suelen contener información confidencial (como los precios de los productos en un sitio de comercio electrónico) que deben almacenarse únicamente en una base de datos de fondo. Los usuarios no deben ver campos ocultos pero un hacker o atacante puede descubrirlos y explotarlos.

Referencias

http://www.parentesis.com/tutoriales/Que_son_y_para_que_sirven_las_cookies

https://www.ecured.cu/Cliente-Servidor

http://www.uterra.com/codigo_php/codigo_php.php?ref=las_variables_de_sesion_en_php

https://developer.mozilla.org/en-US/docs/Web/HTML/Element/input/hidden

https://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Cookies-Seguridad-Informatica.php

http://www.arumeinformatica.es/blog/seguridad-de-las-sesiones-en-php-session-hijacking/