UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Materia: Diseño Orientado a Objetos.

Tema: Seguridad en Aplicaciones Web: comunicación cliente/servidor (Ensayo).

Alumno: Arodi Fuentes Montelongo.

Matricula: 1837486.

Carrera: LSTI

Grupo: 006

Profesor(a): Lic. Miguel Angel Salazar Santillán.

San nicolas de los Garza, N.L.

En la actualidad el crecimiento de internet ha impactado directamente en la seguridad de la información manejada cotidianamente. Sitios de comercio electrónico, servicios, bancos e incluso redes sociales contienen información sensible que en la mayoría de los casos resulta ser muy importante.

Se puede decir que uno de los puntos más críticos de la seguridad en Internet son las herramientas que interactúan de forma directa con los usuarios, en este caso los servidores web. Es común escuchar sobre fallas en los sistemas de protección de los servidores más frecuentemente utilizados, por ejemplo Apache, NGINX, IIS, etc. (Build With, 2016) O en los lenguajes de programación en que son escritas las aplicaciones. Sin embargo, la mayoría de los problemas detectados en servicios web no son provocados por fallas de ninguna de estas partes, si no que los problemas se generan por malas prácticas de parte de los programadores.

Aplicaciones cliente/servidor que utilizan el protocolo HTTP para interactuar con los usuarios u otros sistemas. El cliente utilizado por los usuarios es habitualmente un navegador. Los problemas de seguridad pueden provenir de los programas web en los que se apoyan, aunque en su mayor parte son consecuencia de fallos en la lógica y el diseño de la propia aplicación.

Actualmente cada vez es más común que las aplicaciones web interacciones entre sí, pero muchas veces para realizar esa conexión es necesario implementar complejas APIs con sus propias especificaciones y necesidades. Para cubrir esta necesidad de comunicación entre aplicaciones web de forma simple surge Web Intents de la mano de Google y Mozilla.

Uno de los conceptos que más problemas produce cuando comenzamos a trabajar con aplicaciones web en Java es el concepto de java session (HttpSession) que sirve para almacenar información entre diferentes peticiones HTTP ya que este protocolo es stateless (sin estado). Así pues en muchas ocasiones nos encontraremos con el problema de compartir estado (datos usuario) entre un conjunto amplio de páginas de nuestra Aplicación.

Para solventar este problema en la plataforma Java EE se usa de forma muy habitual la clase HttpSession que tiene una estructura de HashMap (Diccionario) y permite almacenar cualquier tipo de objeto en ella de tal forma que pueda ser compartido por las diferentes páginas que como usuarios utilizamos. Cada vez que un usuario crea una session accediendo a una página (que la genere) se crea un objeto a nivel de Servidor con un HashMap vacío que nos permite almacenar la información que necesitamos relativa a este usuario.

El concepto de Session es individual de cada usuario que se conecta a nuestra aplicación y la información no es compartida entre ellos. Así pues cada usuario dispondrá de su propio HashMap en donde almacenar la información que resulte útil entre páginas.

Las cookies son sólo datos que recibe un navegador web junto con una página y que se almacenan en el ordenador del usuario. La información se almacena en el ordenador del usuario a petición del servidor web, directamente desde la propia página web con JavaScript.

Una cookie se compone de los siguientes atributos: una pareja nombre/valor, que es la información de la cookie; un dominio, que indica en qué dominio se puede utilizar la cookie; una ruta, que limita el uso de la cookie a páginas que se encuentren en dicha ruta; una fecha de caducidad o máxima edad, que indica hasta cuándo la cookie es válida; una marca de sólo conexión segura, que obliga a enviar la cookie mediante un protocolo de encriptación; y una marca de sólo HTTP, para limitar el uso de la cookie al protocolo HTTP.

En el navegador Google Chrome, a través del menú "Herramientas para desarrolladores", se visualiza una barra de herramientas en la que seleccionamos el menú "Resources" y a continuación seleccionamos "Cookies" y el dominio del cual queremos ver las cookies. Finalmente, en el navegador Opera, seleccionamos el menú "Herramientas", a continuación "Avanzado" y por último "Cookies". Y se muestra una ventana donde podemos consultar todas las cookies que se almacenan en nuestro ordenador.

Conclusión

Estas vulnerabilidades representan un serio riesgo para las agencias y compañías que han expuesto sus reglas de negocio en Internet. Los problemas de seguridad en aplicaciones Web son tan serios como los problemas de seguridad de red, aunque tradicionalmente han recibido considerablemente menos atención. Los atacantes han comenzado a enfocarse en los problemas de aplicaciones Web y están desarrollando activamente herramientas y técnicas para detectarlas y explotarlas.