UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Universidad Autónoma de Nuevo León

Facultad de Ciencias Físico Matemáticas

Diseño Orientado a Objetos

Aplicaciones Web

Profesor: Miguel Ángel Salazar

Alumno: Jesús Manuel Muñoz Escobedo

Matrícula: 1723308

Aula: 413

Fecha: 18 de agosto del 2017

Introducción

Introduciéndonos al tema de las aplicaciones web, hablaremos principalmente de lo que son estas mismas, entendiendo así su significado dentro de la ingeniería de software siendo así de mucha importancia para nosotros esto, ya que nos ayudara a entender mejor de lo que tratan y el objetivo de las aplicaciones web.

Agregando que hablaremos también de algunos de los tipos de aplicaciones web que existen incluyendo también ciertos ejemplos de las vulnerabilidades que pueden presentarse en dichas páginas afectando así nuestra estadía en las mismas y dificultándonos el trabajar o ingresar a ellas.

Aplicaciones Web

Si bien sabemos que dentro de la ingeniería de software se les denomina a las aplicaciones web a aquellas herramientas que los usuarios pueden llegar a utilizar cuando se accede a un servidor web a través de internet o de una intranet mediante un navegador.

Utilizando otras palabras, es una app de software que se codifica en un lenguaje soportado por los navegadores web en la que se confía la ejecución al navegador.

Las aplicaciones web son populares debido a lo práctico del navegador web como cliente ligero, a la independencia del sistema operativo, así como a la facilidad para actualizar y mantener aplicaciones web sin distribuir e instalar software a miles de usuarios potenciales. Existen aplicaciones como los webmails, wikis, weblogs, tiendas en línea y la propia Wikipedia que son ejemplos bastante conocidos de aplicaciones web.

Es importante mencionar que una página Web puede contener elementos que permiten una comunicación activa entre el usuario y la información. Esto permite que el usuario acceda a los datos de modo interactivo, gracias a que la página responderá a cada una de sus acciones, como por ejemplo rellenar y enviar formularios, participar en juegos diversos y acceder a gestores de base de datos de todo tipo.

Ahora bien, existen distintos tipos de aplicaciones web en las que se puede trabajar, como lo son:

- Aplicación Web Estática
- Aplicación Web Dinámica
- Tienda Virtual o Comercio Electrónico
- Portal Web App
- Aplicación Web Animada
- Aplicación Web con “Gestor de Contenidos”

Existen también diversas vulnerabilidades dentro de las aplicaciones web que pueden hacer que los sitios web sean blancos fáciles para hackearse, extorsionarse, entre otras. Provocando así daños en ellas como robo de información de los usuarios, pérdidas financieras, convertir el sitio web en un punto de descarga de programas maliciosos o dejar incluso al propietario fuera de línea.

Presentando algunos ejemplos de vulnerabilidades más comunes de los sitios web:

- Inyección: Ocurre cuando a nuestro sistema entra información no confiable a través de formularios o comandos que son interpretados por queries en nuestra base de datos. Puede resultar en robo o pérdida de nuestra información. Solución: Validar y limpiar todo lo que el usuario ingrese a nuestro sistema antes de realizar cualquier proceso además de usar Prepared statements y stored procedures.
- Secuencias de Comandos en sitios cruzados: Esta falla permite desplegar en el navegador datos no confiables proporcionados por usuarios, generalmente inyectando código javascript malicioso. Estos datos pueden secuestrar tu sitio web, permitiendo que tus usuarios sean re direccionados a sitios maliciosos o descarguen malware. Solución: Validar y escapar cualquier dato a ser impreso en tu sitio, trata siempre de usar herramientas de

templates los cuales te permitan optimizar este proceso (Freemarker o Smarty).

- Autenticación rota: Se presenta cuando es posible suplantar la identidad del usuario al obtener acceso a datos como contraseñas o identificadores. Un ejemplo es poder modificar el id de la sesión en la cookie y obtener así acceso como un administrador o cambiar el perfil de acceso. Solución: Verificar los procesos de autenticación, usar mecanismos y librerías ya existentes. No guardar información sobre permisos o identidad en cookies.
- Solicitudes falsificadas en sitios cruzados: El atacante engaña a la víctima a enviar solicitudes HTTP que no desea lo que permite al atacante ejecutar operaciones que el usuario no desea. Solución: Controlar el flujo de los procesos usando tokens únicos por sesión y por solicitud.
- Referencias directas e inseguras a objetos: Exponer referencias a objetos de implementación interna como archivos, directorios y base de dato por lo que pueden ser manipulados. Por ejemplo, si usamos un script de descarga que recibe como parámetro el nombre del archivo, puede ser usado para enviar al atacante nuestro documento de configuración con la clave de nuestra Base de Datos. Solución: Usar siempre controles de acceso y no ofrecer datos sobre la implementación interna.

Conclusión

Concluyendo con este trabajo puedo decir que entendí de mejor manera de lo que se tratan y el objetivo que tienen las aplicaciones web, siendo así que nos mejoran en una gran cantidad nuestras experiencias dentro del internet y facilitando también nuestro trabajo en él.

Aprendí además que existen diversos tipos de vulnerabilidades que se encuentran constantemente atacando a las aplicaciones web para causar distintos tipos de problemas, ya sea desde impedirnos el acceso o involuntariamente hacerse la descarga de contenido malicioso que nos puede afectar el rendimiento de nuestro equipo.