Facultad de Ciencias Físico Matemáticas

Nombre: Gabriel Omar Sanchez Reyes

Matricula: 1664322

Materia: Diseño orientado a objetos

Tarea 1

Introducción : En este ensayo se hablara de cada tipo de aplicación y sus características, además de algunas vulnerabilidades de una de estas aplicaciones.

Desarrollo:

Tipos de aplicaciones

Console App: Realizamos nuestros primeros programas en .NET, utilizando la consola, que utiliza un formato de salida y entrada de datos en modo texto.

Se puede definir una aplicación de consola como aquella que se ejecuta en una ventana de MS-DOS, es decir, en línea de comandos.

Lo más común dentro del desarrollo bajo la plataforma .Net es la creación de aplicaciones Web o aplicaciones Windows sin embargo la mejor forma de sentar unas bases firmes acerca de la programación orientada a objetos es comenzar construyendo aplicaciones sencillas de consola.

Web:

Las aplicaciones web reciben este nombre porque se ejecutan en la internet. Es decir que los datos o los archivos en los que trabajas son procesados y almacenados dentro de la web. Estas aplicaciones, por lo general, no necesitan ser instaladas en tu computador.

El concepto de aplicaciones web está relacionado con el almacenamiento en la nube. Toda la información se guarda de forma permanente en grandes servidores de internet y nos envían a nuestros

dispositivos o equipos los datos que requerimos en ese momento, quedando una copia temporal dentro de nuestro equipo.

Móvil: Una aplicación móvil, apli o app (en inglés) es una aplicación informática diseñada para ser ejecutada en teléfonos inteligentes, tabletas y otros dispositivos móviles y que permite al usuario efectuar una tarea concreta de cualquier tipo —profesional, de ocio, educativas, de acceso a servicios, etc, facilitando las gestiones o actividades a desarrollar.

Por lo general, se encuentran disponibles a través de plataformas de distribución, operadas por las compañías propietarias.

Algunas vulnerabilidades de apps 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.

Secuencias de comandos en sitios cruzados (Cross-site scripting, XSS): 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 redireccionados a sitios maliciosos o descarguen malware

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.

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.

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.