Apuntes 12 de mayo del 2023
Erick Madrigal

Sobre el proyecto

Al dejar variables “quemadas” en el código se pone en peligro la información guardada en estas variables ya que se dejan al alcance de todas las personas que puedan acceder al código
Para no dejar los valores “quemados” se pueden utilizar:

- parámetros en la aplicación
- variables de entorno
- archivos de configuración
- Vaults (Secrets Manager/ Config Manager)
- BLOB

Para saber si se debe de aplicar uno de estos métodos para almacenar los valores o si se deben de dejar las variables “quemadas” se debe hacer la pregunta “¿Si ejecuto esta aplicación en otro entorno va a funcionar?”

Es importante que si un valor se utiliza en distintos lugares es mejor almacenarlo en una variable y utilizarla en lugar del valor en sí, de esta manera si se tiene que hacer un cambio en el valor solo se debe cambiar el dato en la variable y no en cada lugar en donde se utilizó.

Un archivo de constantes se es compilado junto con la aplicación y contiene archivos específicos para que la aplicación funcione.

Un archivo de configuración se carga a la aplicación, usualmente se utiliza para configurar el ambiente

Principals and Database Objects Security

Principals

- Individuals: personas.
- Procesos: aplicaciones o tareas programadas que se están ejecutando.
- Grupos: agrupamientos de individuos utilizados para asignar políticas.
- Roles: trabajos predefinidos que tiene una persona (esto en algunos motores de bases de datos), en algunas bases de datos un rol es un grupo de permisos a un individuo, grupo o proceso.
- Políticas: se usan para definir roles o permisos granulares dentro de la base de datos.
- federación de usuarios: es utilizar sistemas manejadores de bases de datos como LDAP o Active Directory (de Microsoft).
- SSO (Single Sign-On): es lo que se utiliza para poder manejar una única sesión para varias aplicaciones.
- Server Auth(local): es cuando la misma base de datos se encarga de manejar: usuario, passwords, roles y políticas.

Si se instala un servidor SQL dentro de un servidor Windows se pueden usar los “Windows Users” para ingresar a la base de datos

Microsoft tiene un mecanismo llamado Trust Relationship el cual permite que una maquina confíe en otra siempre que ambas tengan el mismo usuario y contraseña. Como regla de oro se debe deshabilitar el usuario admin y crear otro usuario con los permisos de administrador en caso de necesitarlo para que un atacante no pueda iniciar sesión como el admin default.

Asegurables

- Servidor
- Base de datos
- Objetos: índices, tablas, colecciones, catálogos, vistas, etc.

Security Token Service

Cuando un usuario solicita entrar a un sistema se le otorga un token el cual es una credencial temporal que se puede utilizar para entrar a la base de datos. Esto permite que se genere información de uso de la base de datos.

Identity provider

Es el encargado de dar información de usuarios.

Security Assertion Markup Languaje

Primer protocolo utilizado para hacer autenticación de sistemas federados en web.

Document Level Security

Término utilizado en bases de datos no SQL. Cuando se generan documentos en una colección se le da acceso a esos documentos solo a los usuarios indicados.

Guest Users

Usuarios de prueba que se utilizan para poder ingresar y hacer cambios en la base de datos. La regla de oro es que estos usuarios siempre deben ser borrados o deshabilitados cuando ya no se estén utilizando.

Cloud Role Auth

Administración o autorización de bases de datos por medio de roles.

Encryption and Certificates

Transport Level Security

Es el que permite encriptar los datos que se van a enviar por la red

handshake

Cuando una aplicación y un servidor se van a comunicar la aplicación le envía su public key al servidor, este encripta la key de la aplicación con la public key del servir y se la envía a la

aplicación para que esta la desencripte con su llave privada y así establecer un medio seguro de comunicación y de esta manera el servidor y la aplicación intercambian sus public keys.

Al hacer esto el servidor puede encriptar la información que le va a enviar a la aplicación son el public key de la aplicación haciendo que solo la aplicación (la cual tiene la private key) pueda desencriptarla. Esto funciona de la misma manera en ambos sentidos. Esto es conocido como inscripción de tránsito “on the fly”.

Server-Side Encryption

Debido a que la información del servidor puede ser robada, se debe asegurar que está no pueda ser legible para el atacante, para lograr esto lo que se hace es encriptar la información una vez que esta llega al servidor por medio de un certificado. En la nube se hace por medio de un key management service.

Client Ecription

Además de encriptar los datos al momento en que llegan al servidor se aplica una capa de seguridad extra en la cual lo que se hace es encriptar los datos desde que el usuario los envía a la aplicación.

Field Encryption

Son espacios de las bases de datos las cuales el usuario es el encargado de realizar la encriptación de estos datos.

Cuando una aplicación tiene muchas capas se van realizando cada vez mas encriptaciones lo que hace que la aplicación se vuelva mas lenta, para corregir esto se pueden ir eliminando pasos de encriptación sin embargo siempre se debe de dejar la encriptación HTTPS entre el cliente y la aplicación ya que esta es la mas peligrosa de no usar, no usar encriptación en todos los componentes es llamado SSL termination.