## AUTENTICACION DE WEB

Consideraciones generales:

* La autenticación es solo tan fuerte como sus procesos de administración de usuarios
* Use la forma más apropiada de autenticación adecuada para su clasificación de bienes
* Re-autenticar al usuario para transacciones de alto valor y acceso a áreas protegidas
* Autenticar la transacción, no el usuario
* Las contraseñas son trivialmente rotas y no son adecuadas para sistemas de alto valor

Buenas practicas:

1. User IDs
2. Fortalezas de seguridad
3. Implementar métodos seguros de recuperación
4. Almacenar contraseñas de forma segura
5. Transmitir contraseñas solo sobre TLS
6. Solicitar re-autenticacion
7. Utilizar sistemas de autenticación de factores multiple
8. Manejo de mensajes de error
9. Prevenir ataques por fuerza bruta

## TECNICAS DE AUTENTICACION DE USUARIOS

1. BASICA Y SEGURA (HTTP-Digest)
2. BASADA EN FORMAS
3. INTEGRADA (ISS-ASP.NET-AD)
4. BASADA EN CERTIFICADO
5. FUERTE (Algo que sabes, tienes/eres)

## AUTORIZACION EN LA WEB

Objetivos:

* Asegurar que únicamente usuarios autorizados puedan realizar acciones permitidas con su correspondiente nivel de privilegio.
* Controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
* Prevenir ataques de escalada de privilegios.

Buenas practicas:

* Codificar el control en la actividad del objeto.
* Disponer de un Controlador Centralizado (ACL)
* Utilizar un Control Central de Acceso, en las diferentes capas
* Verificar la política del lado del servidor (server-side)

## METODOS DE CONTROL DE ACCESO

1. Role Based Access Control (RBAC): Basada en ROLES. DIferentes accesos por individuos. Ej: Hospital.
2. Discretionary Access Control (DAC): Es un medio para restringir el acceso a la informacion sobre la base de la identidad de los usuarios y/o pertenencia a ciertos grupos. Ej: Sistema de archivos de un Sistema Unix(rwx).
3. Mandatory Access Control (MAC): Asegura la informacion mediante la asignacion de etiquetas de sensivilidad y la compara con la sensivilidad del usuario que está operando.

## Ataques de Control de Acceso

* Vertical Access Control Attacks - Un usuario convencional obtiene accesos superiores o de administrador.
* Horizontal Access Control Attacks - Con el mismo rol o nivel el usuario puede acceder a información de otros usuarios.
* Business Logic Access Control Attacks - Abusar de una o más actividades para realizar una operación con un resultado no autorizado para ese usuario.

## ADMINISTRACION DE USUARIOS Y PRIVILEGIOS

Objetivos:

* Las funciones de nivel de administrador están segregadas apropiadamente de la actividad del usuario.
* Los usuarios no pueden acceder o utilizar funcionalidades administrativas.
* Proveer la necesaria auditoria y trazabilidad de funcionalidad administrativa.

Mejores Prácticas:

* Cuando se está diseñando aplicaciones, trazar la funcionalidad administrativa fuera y asegurarse que los controles apropiados de acceso y auditoria están en su lugar.
* Considerar procesos – en algunas ocasiones todo lo que se requiere es entender como los usuarios pueden ser prevenidos de utilizar una característica con la simple falta de acceso.
* Acceso de servicio de asistencia es siempre un término medio –ellos necesitan acceso para ayudar a los clientes, pero no son administradores.
* Diseñar cuidadosamente la funcionalidad de servicio de asistencia /moderador/ soporte al cliente alrededor de una capacidad administrativa limitada y aplicación segregada o acceso.
* Todos los sistemas deberían tener aplicaciones separadas del acceso de los usuarios para los administradores.
* Sistemas de alto valor deberían separar estos sistemas en un servidor separado, que tal vez no sea accesible desde el amplio Internet sin acceso para la administración de redes, como a través del uso de una VPN fuertemente autenticada o desde la red de un centro de operaciones de confianza.

**MANEJO DE SESIONES DE USUARIOS**



Objetivos, asegurar que:

* Los usuarios atenticados tengan una robusta y criptograficamente segura asociacion de sus sesiones.
* Se hagan cumplir los controles de autorizacion
* Se prevengan los tipicos ataques web, tales como la reutilizacion, falsificacion e intercepcion de sesiones.

Propiedades del ID de sesión:

* Nombre
* Longitud
* Entropía
* Contenido o valor

Ciclo de vida del ID de sesión:

* Generacion y verificación
* Confiabilidad
* Cambios en el nivel de privilegios
* Uso de multiples cookies
* Expiracion de sesión
* Expiracion automática
* Expiracion manual

## WEB SERVICES

Basados en XML/SOAP.