Vulnerabilidades de control de acceso

Las directivas de control de acceso tienen como objetivo garantizar que los usuarios solo puedan acceder a funcionalidades en las que tengan autorización. Las consecuencia de este tipo de vulnerabilidades son:

- Acceso a cuentas de usuario sin pasar por autenticación
- Acceso a funcionalidades de administrador por parte de usuarios sin permisos
- Acceso a recursos no permitidos.

El control de acceso debe seguir el principio de privilegio menor POLP (Principle Of Least Privilege) que consiste en limitar los permisos de acceso de un usuario a los mínimos imprescindibles para que este pueda realizar su trabajo.

Problemas en el control de acceso

- Modificaciones en las URL cuando referencian las claves primarias de los recursos
- Manipulación de metadatos
- Acceso al sistema de ficheros
- Redirecciones no controladas

Cuando no existe control de acceso o este no es bueno, conociendo la URL, el atacante puede acceder a zonas de la aplicación a las que no debería tener acceso.