A01-2021 Broken Access Control

Este fallo se centra en la incapacidad de restringir adecuadamente las acciones de usuarios autenticados. Lo que permite a los usuarios realizar acciones o acceder a recursos para los cuales no están autorizados. Dentro de lo que incluye:

- Escalada de privilegios.
- Acceso no autorizado a datos sensibles.
- Modificación o eliminación de datos sin permisos adecuados.

Ejemplo: Un atacante podría modificar cookies o tokens de sesión para asumir la identidad de otro usuario.

Gravedad

El impacto puede variar desde datos expuestos hasta comprometer todo el sistema, dependiente del contexto en el que se vea explotada.

- Puede comprometer datos sensibles de usuario y sistemas.
- Impactos severos como pérdida de información, violación de privacidad y manipulación de recursos del sistema.
- Se puede explotar con herramientas simples o cambios manuales en solicitudes.

Mitigación

Para que esta vulnerabilidad sea mitigada, se requiere un enfoque continuo y actualizado, especialmente para sistemas que manejan información sensible o tienen múltiples niveles de usuarios, entre las medidas que se pueden tomar están:

- Principio de mínimo privilegio (PoLP): Este principio es fundamental. Cada usuario o proceso debe tener solo los permisos necesarios para realizar sus tareas.
- Controles de acceso basados en roles (RBAC): Implementar RBAC para gestionar permisos de forma centralizada y eficiente.
- Validación de entradas: Validar todas las entradas del usuario en el lado del servidor para evitar la manipulación de datos.
- Implementación de políticas de control de acceso: Es necesario implementar políticas de control de acceso que sean claras, y que estén debidamente documentadas.