OWASP Top 10 2021

A01:2021 - Pérdida de Control de Acceso

El control de acceso se establece para garantizar que los usuarios no puedan operar más allá de los permisos asignados. Cuando se presentan fallas en este control, suele haber divulgación de información no autorizada, modificación o destrucción de datos, o incluso la ejecución de funciones comerciales fuera de los límites establecidos para el usuario

A02:2021 – Fallas Criptográficas

Subiendo una posición al número 2, anteriormente conocido como Exposición de datos sensibles, que es más un amplio síntoma que una causa raíz, la atención se centra en las fallas relacionadas con la criptografía (o la falta de ésta). Esto a menudo conduce a la exposición de datos sensibles. Las CWE incluidas son CWE-259: Uso de contraseña en código fuente, CWE-327: Algoritmo criptográfico vulnerado o inseguro y CWE-331: Entropía insuficiente.

A03:2021 - Inyección

Algunas de las inyecciones más comunes son SQL, NoSQL, comandos de sistema operativo, Object-Relational Mapping (ORM), LDAP, expresiones de lenguaje u Object Graph Navigation Library (OGNL). El concepto es idéntico para todos los intérpretes. La revisión del código fuente es el mejor método para detectar si las aplicaciones son vulnerables a inyecciones. Las pruebas automatizadas en todos los parámetros, encabezados, URL, cookies, JSON, SOAP y XML son fuertemente recomendados.

A04:2021 - Diseño Inseguro

El diseño inseguro es una categoría amplia que representa diferentes debilidades, expresadas como "diseño de control faltante o ineficaz". El diseño inseguro no es la fuente de las otras 10 categorías. Existe una diferencia entre un diseño inseguro y una implementación insegura. Distinguimos entre fallas de diseño y defectos de implementación por un motivo, difieren en la causa raíz y remediaciones. Incluso un diseño seguro puede tener defectos de implementación que conduzcan a vulnerabilidades que pueden explotarse.

A05:2021 - Configuración de Seguridad Incorrecta

Una configuración de seguridad incorrecta puede dejar expuesta la aplicación a una variedad de riesgos, incluyendo el acceso no autorizado, la divulgación de información sensible, la ejecución remota de código, entre otros. Es crucial que los desarrolladores y administradores de sistemas revisen y configuren adecuadamente la seguridad de la aplicación y de la infraestructura subyacente para mitigar estos riesgos y proteger los datos y recursos de la aplicación.

A06:2021 - Componentes Vulnerables y Desactualizados

La inclusión de componentes vulnerables y desactualizados en una aplicación aumenta significativamente el riesgo de seguridad, ya que los atacantes pueden explotar las vulnerabilidades conocidas en estos componentes para comprometer la seguridad de la aplicación. Es esencial mantener actualizados todos los componentes utilizados en el desarrollo de una aplicación web, ya sea a través de parches de seguridad, actualizaciones de software o migraciones a versiones más seguras, para reducir el riesgo de exposición a posibles amenazas.

A07:2021 - Fallas de Identificación y Autenticación

Las fallas en la identificación y autenticación pueden permitir a los atacantes acceder de forma no autorizada a cuentas de usuario, comprometer datos sensibles o realizar actividades maliciosas en nombre de usuarios legítimos. Para mitigar estos riesgos, es fundamental implementar medidas de autenticación sólidas, como el uso de contraseñas seguras, la autenticación multifactorial, la gestión adecuada de sesiones y el uso de protocolos seguros de autenticación, como OAuth o OpenID Connect.

A08:2021 - Fallas en el Software y en la Integridad de los Datos

Se refiere a problemas relacionados con la integridad y la seguridad del software en una aplicación web. Esto incluye errores de programación, vulnerabilidades de software, y debilidades en la validación de datos que pueden permitir a los atacantes manipular datos de la aplicación de manera no autorizada.

A09:2021 - Fallas en el Registro y Monitoreo

Se refiere a deficiencias en la capacidad de una aplicación para registrar eventos relevantes y monitorear su funcionamiento en busca de anomalías o actividades sospechosas. Esto implica la ausencia o la implementación inadecuada de mecanismos de registro de eventos y sistemas de monitoreo en la aplicación web.

A10:2021 - Falsificación de Solicitudes del Lado del Servidor

Se refiere a un tipo de ataque en el que un atacante puede falsificar o manipular solicitudes enviadas al servidor desde el lado del cliente. Este tipo de ataque es especialmente peligroso porque puede permitir al atacante realizar acciones no autorizadas en nombre de un usuario legítimo, como cambiar contraseñas, acceder a datos confidenciales o realizar transacciones no deseadas.