**OWASP Top 10**

El OWASP Top 10 es una lista de los diez riesgos de seguridad más críticos para aplicaciones web, creada y mantenida por la Open Web Application Security Project (OWASP). La lista se actualiza periódicamente para reflejar los cambios en el panorama de amenazas de seguridad.

**OWASP Top 10 2021**

1. **A01:2021 - Broken Access Control**: Problemas con la aplicación de políticas de acceso a recursos, permitiendo a usuarios no autorizados acceder a datos o funcionalidades.
2. **A02:2021 - Cryptographic Failures**: Fallos en la protección de datos a través de técnicas criptográficas, como el uso de algoritmos débiles o la falta de cifrado.
3. **A03:2021 - Injection**: Inyección de código malicioso en la aplicación, como SQL, NoSQL, OS y LDAP, debido a la falta de validación de entradas.
4. **A04:2021 - Insecure Design**: Deficiencias en el diseño de la seguridad de la aplicación desde el inicio, incluyendo modelos de amenazas y análisis de riesgo.
5. **A05:2021 - Security Misconfiguration**: Configuraciones de seguridad incorrectas o por defecto que permiten el acceso no autorizado o la exposición de datos.
6. **A06:2021 - Vulnerable and Outdated Components**: Uso de componentes con vulnerabilidades conocidas que pueden ser explotadas por atacantes.
7. **A07:2021 - Identification and Authentication Failures**: Fallos en los mecanismos de autenticación y gestión de sesiones, permitiendo accesos no autorizados.
8. **A08:2021 - Software and Data Integrity Failures**: Compromiso de la integridad del software o datos, como la inserción de actualizaciones maliciosas.
9. **A09:2021 - Security Logging and Monitoring Failures**: Falta de registros de seguridad y monitoreo que dificultan la detección y respuesta a incidentes.
10. **A10:2021 - Server-Side Request Forgery (SSRF)**: Manipulación de la aplicación para que realice solicitudes a servidores no intencionados, exponiendo información interna.

**OWASP Testing Guide**

La OWASP Testing Guide es una guía completa para realizar pruebas de seguridad en aplicaciones web. Proporciona metodologías y técnicas detalladas para identificar y mitigar vulnerabilidades de seguridad.

**Principales Secciones de la OWASP Testing Guide v4**

1. **Introducción**: Contexto y objetivos de la guía, incluyendo el alcance y la importancia de las pruebas de seguridad.
2. **Proceso de Pruebas de Seguridad**: Descripción del ciclo de vida de las pruebas de seguridad, desde la planificación hasta la ejecución y el análisis de resultados.
3. **Técnicas de Prueba**:
   * **Gestión de Configuración**: Verificación de configuraciones seguras en servidores, bases de datos y aplicaciones.
   * **Pruebas de Identificación y Autenticación**: Evaluación de los mecanismos de autenticación y gestión de sesiones.
   * **Pruebas de Autorización**: Comprobación de controles de acceso a recursos y datos.
   * **Pruebas de Gestión de Entrada de Usuario**: Identificación de vulnerabilidades relacionadas con la validación y sanitización de entradas de usuario.
   * **Pruebas de Manejo de Errores**: Verificación de la gestión segura de errores y excepciones.
   * **Pruebas de Criptografía**: Evaluación del uso y la implementación de técnicas criptográficas.
   * **Pruebas de Negocios Lógicas**: Verificación de la lógica de negocio para identificar errores que pueden llevar a vulnerabilidades.
4. **Informes y Mitigación**: Recomendaciones para documentar los resultados de las pruebas y proporcionar soluciones para mitigar las vulnerabilidades encontradas.

**Conclusión**

El OWASP Top 10 y la OWASP Testing Guide son recursos fundamentales para cualquier profesional de seguridad de aplicaciones. Proporcionan un marco claro y comprensible para identificar, evaluar y mitigar las vulnerabilidades más críticas en aplicaciones web. Utilizar estos recursos ayuda a mejorar la seguridad y a proteger los datos y la funcionalidad de las aplicaciones contra amenazas comunes y emergentes.

Si necesitas más detalles o ejemplos específicos sobre cualquiera de los puntos mencionados, estaré encantado de ayudarte.