Actividad 1.1: Análisis del OWASP Top Ten

A01:2021 - Broken Access Control (Control de Acceso Vulnerable)

Descripción:

Ocurre cuando las restricciones de acceso no están correctamente implementadas, permitiendo a usuarios no autorizados realizar acciones o acceder a datos restringidos.

Ejemplos de ataque:

- Modificación de un parámetro en la URL para acceder a recursos de otro usuario.
- Uso de cuentas con privilegios elevados sin autenticación adecuada.

Consecuencias:

- Filtración de datos sensibles.
- Modificación no autorizada de información.

Mitigación:

- Implementar controles de acceso a nivel de servidor.
- Aplicar el principio de **menor privilegio** en los permisos.
- Validar el acceso a cada recurso mediante autenticación y autorización estricta.

A02:2021 - Cryptographic Failures (Fallos Criptográficos)

Descripción:

Se produce cuando los datos sensibles no se protegen correctamente con cifrado fuerte o protocolos adecuados.

Ejemplos de ataque:

- Almacenamiento de contraseñas en texto plano.
- Uso de cifrados obsoletos como MD5 o SHA-1.
- Transmisión de datos sin cifrado (HTTP en lugar de HTTPS).

Consecuencias:

- Robo de credenciales o datos personales.
- Ataques de intercepción (Man-in-the-Middle).

Mitigación:

- Implementar TLS 1.2 o 1.3 en todas las conexiones.
- Usar algoritmos seguros: AES-256 para cifrado, Argon2 para contraseñas.
- Nunca almacenar datos sensibles sin cifrado.

A03:2021 - Injection (Inyección de Código: SQL, XSS, LDAP, etc.)

Descripción:

Ocurre cuando un atacante logra inyectar código malicioso en una aplicación, manipulando consultas o comandos.

Ejemplos de ataque:

- **SQL Injection:** Modificación de consultas SQL para acceder o manipular bases de datos.
- **Cross-Site Scripting (XSS):** Inyección de scripts en páginas web para robar información o manipular la interfaz.
- **Command Injection:** Ejecución de comandos en el sistema operativo.

Consecuencias:

- Robo de información confidencial.
- Ejecución remota de código en el servidor.

Mitigación:

- Usar **consultas parametrizadas** y ORM en bases de datos.
- Sanitizar entradas de usuario para evitar scripts maliciosos.
- Aplicar **Content Security Policy (CSP)** para prevenir XSS.

A04:2021 - Insecure Design (Diseño Inseguro)

Descripción:

Se refiere a sistemas que no fueron diseñados con medidas de seguridad adecuadas.

Ejemplos de ataque:

- Falta de controles de acceso en APIs.
- Autenticación débil sin doble factor (2FA).
- Sin análisis de amenazas en la fase de diseño.

Consecuencias:

- Aplicaciones vulnerables desde su desarrollo.
- Explotación de errores de lógica de negocio.

Mitigación:

- Aplicar el principio de **seguridad por diseño**.
- Implementar modelos de amenazas desde el inicio del desarrollo.
- Realizar auditorías de código y pruebas de seguridad.

A05:2021 - Security Misconfiguration (Mala Configuración de Seguridad)

Descripción:

Errores en la configuración de servidores, aplicaciones y bases de datos que exponen vulnerabilidades.

Ejemplos de ataque:

- Consolas de administración accesibles sin autenticación.
- Permisos excesivos en archivos o bases de datos.
- Uso de contraseñas por defecto en sistemas en producción.

Consecuencias:

- Acceso no autorizado a sistemas internos.
- Exposición de datos sensibles.

Mitigación:

- Aplicar el **principio de menor privilegio** en configuraciones.
- Realizar revisiones y auditorías de seguridad periódicas.
- Deshabilitar características innecesarias en servidores.

A06:2021 - Vulnerable and Outdated Components

Descripción:

Uso de librerías, frameworks o software con vulnerabilidades conocidas.

Ejemplos de ataque:

- Explotación de fallos en versiones obsoletas de Apache, PHP o WordPress.
- Uso de librerías desactualizadas con fallas conocidas.

Consecuencias:

- Ataques de ejecución remota de código (RCE).
- Compromiso total de la aplicación.

Mitigación:

- Actualizar regularmente los componentes utilizados.
- Aplicar parches de seguridad de forma constante.
- Utilizar herramientas de análisis de dependencias como **OWASP Dependency-Check**.

A07:2021 - Identification and Authentication Failures

Descripción:

Problemas en la autenticación de usuarios, permitiendo accesos indebidos.

Ejemplos de ataque:

- Uso de contraseñas débiles sin restricciones.
- Falta de 2FA en accesos críticos.
- Almacenamiento inseguro de credenciales.

Consecuencias:

- Robo de credenciales y acceso a cuentas.
- Suplantación de identidad (phishing).

Mitigación:

- Implementar autenticación fuerte con **2FA**.
- Almacenar contraseñas con hashing seguro (**Argon2, bcrypt**).
- Bloquear cuentas después de múltiples intentos fallidos.

A08:2021 - Software and Data Integrity Failures

Descripción:

Uso de software manipulado o alteraciones no controladas en datos.

Ejemplos de ataque:

- Actualizaciones de software sin firma digital.
- Manipulación de datos por falta de integridad.

Consecuencias:

- Ejecución de código malicioso en actualizaciones.
- Alteración de registros críticos.

Mitigación:

- Usar **firmas digitales en software**.
- Implementar controles de integridad en bases de datos.

A09:2021 - Security Logging and Monitoring Failures

Descripción:

Falta de registros y monitoreo adecuados para detectar ataques.

Ejemplos de ataque:

- No registrar intentos de acceso fallidos.
- Falta de monitoreo en cambios de configuración.

Consecuencias:

- Detección tardía de ataques.
- Incapacidad de realizar auditorías forenses.

Mitigación:

- Implementar **SIEM** y herramientas de monitoreo.
- Registrar eventos críticos y alertas en tiempo real.

A10:2021 - Server-Side Request Forgery (SSRF)

Descripción:

El atacante engaña al servidor para hacer peticiones a recursos internos.

Ejemplos de ataque:

- Acceso a servicios internos a través de URLs manipuladas.

Consecuencias:

- Acceso no autorizado a sistemas internos.
- Exposición de datos sensibles.

Mitigación:

- Validar y restringir URLs externas en peticiones del servidor.