Universidad Mariano Galvez de Guatemala
Ingeniería En Sistemas de Información
Sede Chiquimulilla
Curso: Aseguramiento de Calidad de Software
Docente: Carmelo Mayen

Guía OWASP, Investigación Planes y Casos de prueba

Estudiante:
Armando Sierra González
Carné: 1790-21-18438

Chiquimulilla Agosto 2025

Guía para usuarios no técnicos sobre cómo mitigar las vulnerabilidades del OWASP Top 10 – 2021

1. Control de Acceso Roto (Broken Access Control)

¿Qué es?
Ocurre cuando las personas pueden acceder a información o funciones que no deberían, como ver datos de otros usuarios o cambiar configuraciones sin permiso.

¿Cómo prevenirlo?

- Asegurarse de que cada usuario solo vea lo que le corresponde.
- No mostrar botones o enlaces a funciones que no debe usar.
- Pedir una nueva verificación antes de hacer cambios importantes.

2. Fallas Críticas de Seguridad (Cryptographic Failures)

¿Qué es?
Son errores al proteger datos importantes como contraseñas o información personal.

¿Cómo prevenirlo?

- Usar contraseñas seguras.
- Activar el "candado" en la dirección web (HTTPS).
- Evitar compartir datos personales sin necesidad.

3. Inyección (Injection)

¿Qué es?
Es cuando alguien malintencionado introduce comandos peligrosos en formularios o direcciones web para robar información o dañar el sistema.

¿Cómo prevenirlo?

- Revisar que lo que se escribe en formularios sea válido.
- No permitir símbolos extraños o comandos.
- Usar filtros automáticos para proteger la información.

4. Diseño Inseguro (Insecure Design)

¿Qué es?
Es cuando el sistema se crea sin pensar en la seguridad desde el inicio.

¿Cómo prevenirlo?

- Planificar bien qué puede y no puede hacer cada usuario.
- Incluir medidas de seguridad en cada parte del sistema.

5. Fallos de Seguridad en Configuración (Security Misconfiguration)

¿Qué es?
Pasa cuando el sistema se deja con configuraciones por defecto o mal configurado, facilitando el acceso no autorizado.

¿Cómo prevenirlo?

- Cambiar contraseñas predeterminadas.
- Desactivar funciones que no se utilizan.
- Mantener el sistema actualizado.

6. Componentes Vulnerables y Desactualizados

¿Qué es?
Es cuando se usan partes del sistema (como bibliotecas o plugins) que tienen errores conocidos y no se han actualizado.

¿Cómo prevenirlo?

- Revisar y actualizar las herramientas del sistema con frecuencia.
- Evitar instalar software no confiable.

7. Fallas de Identificación y Autenticación

¿Qué es?
Ocurre cuando no se protege bien el inicio de sesión, permitiendo accesos no autorizados.

¿Cómo prevenirlo?

- Usar contraseñas fuertes.
- Activar la verificación en dos pasos.
- Bloquear cuentas después de varios intentos fallidos.

8. Fallos en la Integridad de Software y Datos

¿Qué es?
Es cuando no se verifica que el software o los datos no hayan sido modificados por alguien externo.

¿Cómo prevenirlo?

- Descargar actualizaciones desde sitios oficiales.
- Usar herramientas que detecten cambios sospechosos.

9. Fallos en Registro y Monitoreo de Seguridad

¿Qué es?
Pasa cuando no se detectan ataques o accesos indebidos porque no se registran correctamente los eventos del sistema.

¿Cómo prevenirlo?

- Activar alertas cuando haya intentos extraños.
- Revisar los registros de actividad con regularidad.

10. Falsificación de Solicitudes del Lado del Servidor (SSRF)

¿Qué es?
Es cuando alguien engaña al sistema para que acceda a direcciones internas que deberían estar protegidas.

¿Cómo prevenirlo?

- Limitar las direcciones a las que puede acceder el sistema.

- Revisar las solicitudes que hacen los usuarios.

Glosario

- **HTTPS:** Protocolo seguro que protege la información mientras se transmite por internet.
- **Formulario:** Espacio donde los usuarios escriben datos (por ejemplo, nombre o contraseña).
- **Contraseña fuerte:** Clave difícil de adivinar (mezcla de letras, números y símbolos).
- **Verificación en dos pasos:** Método que pide un segundo código (como el de un mensaje SMS) además de la contraseña.
- **Actualización:** Nueva versión de un programa que corrige errores y mejora la seguridad.
- **Plugins:** Pequeños programas que se agregan a un sistema para añadir funciones nuevas.
- **Registro de actividad:** Lista de acciones que se han realizado en el sistema.

Investigación sobre Planes de Prueba y Casos de Prueba

¿Qué son los Planes de Prueba?

Es un documento que describe qué se va a probar, cómo se va a probar, quién lo hará y con qué recursos. Ayuda a asegurarse de que todo funcione correctamente antes de que el sistema sea usado.

¿Qué son los Casos de Prueba?

Son las acciones específicas que se realizan para comprobar que una parte del sistema funciona bien. Cada caso de prueba incluye qué se hará, qué se espera que pase y qué resultado se obtuvo.

Ejemplo de Plan de Pruebas

Nombre del sistema: Catálogo de productos
Objetivo: Validar la creación, edición y eliminación de registros
Responsable: Equipo de pruebas
Fecha de ejecución: 1 al 5 de agosto de 2025
Entorno de prueba: Sistema web local

Módulos a evaluar:

- Crear nuevo producto
- Editar producto existente
- Eliminar producto

Criterios de éxito: Todos los casos deben funcionar sin errores y mostrar los mensajes correctos.

ID	Caso de prueba	Paso a paso	Resultado esperado
CP01	Crear producto válido	Ingresar nombre, precio y categoría → Guardar	Se crea el producto y aparece en la lista
CP02	Crear producto sin nombre	Dejar campo vacío y guardar	Se muestra mensaje de error: "Nombre requerido"
CP03	Editar producto existente	Cambiar nombre y guardar	Se actualiza el producto en la lista
CP04	Eliminar producto	Seleccionar producto → Eliminar → Confirmar	El producto ya no aparece en la lista