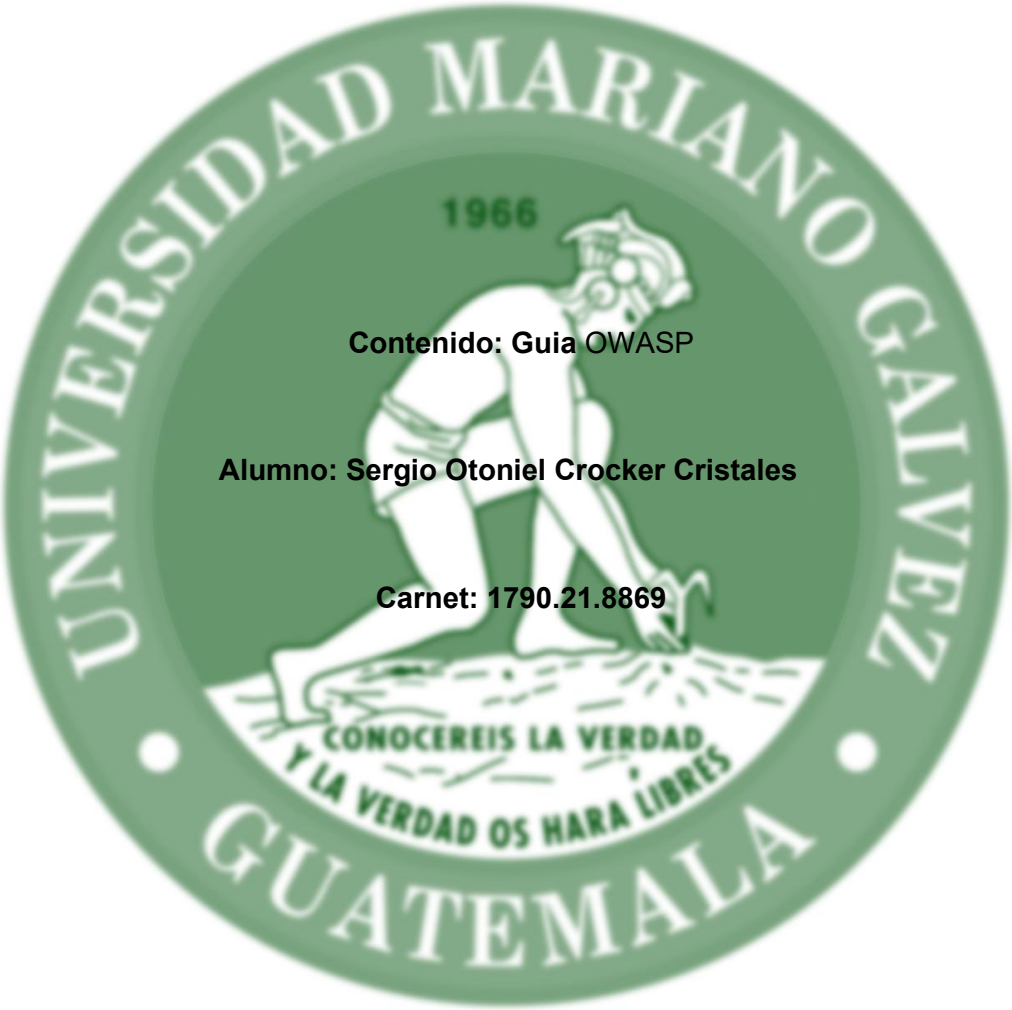
Universidad Mariano Gálvez de Guatemala

Facultad de Ingeniería en Sistemas

Curso: Aseguramiento de Calidad de Software

Catedrático: Ing. Carmelo Estuardo Mayen Monterroso

Semestre: Decimo



Contenido: Guia OWASP

Alumno: Sergio Otoniel Crocker Cristales

Carnet: 1790.21.8869

Chiquimulilla Santa Rosa 2025

Guía Práctica Para Prevenir Vulnerabilidades web y pruebas de catalogo CRUD

Parte 1: Guía para Usuarios no Técnicos sobre el OWASP Top 10 – 2021

Esta guía está diseñada para ayudar a cualquier persona —sin conocimientos técnicos— a entender los riesgos más comunes en aplicaciones web y cómo prevenirlos de forma sencilla.

1. Control de Acceso Roto

Se produce cuando un usuario accede a datos o funciones que no le corresponden. Por ejemplo, un cliente que logra ver la información privada de otro usuario.

Para prevenir este problema, es necesario validar los permisos de cada usuario en todas las acciones importantes. No basta con ocultar botones o menús: el servidor debe confirmar que el usuario tiene autorización antes de ejecutar una operación. También se recomienda revisar los roles de usuario y probar rutas restringidas.

2. Fallos Criptográficos

Aparecen cuando no se protegen correctamente los datos sensibles como contraseñas, números de tarjeta u otra información personal.

Para mitigarlos, siempre debe usarse HTTPS (navegación segura) y cifrado para guardar contraseñas (usando algoritmos como bcrypt). Nunca se deben guardar datos sensibles en texto claro. Además, se deben usar claves secretas fuertes y rotarlas periódicamente.

3. Inyecciones

Suceden cuando un atacante inserta comandos maliciosos en campos como formularios de búsqueda o inicio de sesión. Estos comandos pueden engañar al sistema para ejecutar acciones no deseadas.

Para prevenirlas, se deben validar y filtrar todos los datos que ingresan los usuarios. No debe usarse concatenación directa de texto para construir comandos o consultas a la base de datos.

4. Diseño Inseguro

Se refiere a sistemas que fueron construidos sin considerar la seguridad desde la etapa de diseño.

Para evitarlo, se debe integrar la seguridad desde el inicio del proyecto: identificar posibles riesgos y definir estrategias para mitigarlos. Revisar el diseño y aplicar principios como el mínimo privilegio y separación de funciones.

5. Configuración Incorrecta de Seguridad

Se da cuando el sistema tiene errores en su configuración, como contraseñas por defecto o errores expuestos.

Es importante revisar las configuraciones del servidor y las aplicaciones, cambiar contraseñas por defecto, desactivar funciones no necesarias y limitar los mensajes de error para no revelar información sensible.

6. Componentes Vulnerables y Obsoletos

Ocurre cuando se usan bibliotecas, plugins o frameworks desactualizados o sin soporte, que tienen fallas conocidas.

La solución es mantener actualizado todo el software, revisar periódicamente los componentes en uso, y eliminar aquellos que no se necesiten.

7. Fallos de Identificación y Autenticación

Son fallas que permiten que alguien se haga pasar por otro usuario o acceda sin autenticarse adecuadamente.

Se deben implementar contraseñas robustas, sistemas de bloqueo tras múltiples intentos fallidos y autenticación de múltiples factores (2FA). Además, evitar mantener sesiones activas indefinidamente.

8. Fallos de Integridad de Datos y Software

Suceden cuando no se verifica que los archivos o actualizaciones del sistema no hayan sido modificados maliciosamente.

Es recomendable usar firmas digitales, verificar el origen de los archivos y limitar las actualizaciones automáticas desde fuentes no confiables.

9. Fallos de Registro y Monitoreo de Seguridad

Pasan cuando no se registran o no se revisan eventos importantes como errores, accesos o fallos.

Es fundamental registrar todos los eventos relevantes de seguridad, monitorear esos registros y establecer alertas ante comportamientos sospechosos.

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

Es un tipo de ataque en el que el servidor es engañado para acceder a recursos internos a través de una solicitud externa.

Para prevenirlo, se deben validar cuidadosamente las URLs que los usuarios proporcionan y restringir las direcciones a las que el servidor puede hacer solicitudes.

Glosario de Términos

Servidor: Computadora que almacena y ejecuta aplicaciones o sitios web.

Formulario: Elemento de la página web donde el usuario puede escribir datos.

HTTPS: Protocolo seguro que cifra la información entre el usuario y el sitio web.

Contraseña fuerte: Clave segura que incluye letras, números y símbolos.

Autenticación: Proceso para comprobar que un usuario es quien dice ser.

Actualización: Versión nueva de un software con mejoras y correcciones.

Validación: Proceso para asegurarse de que los datos ingresados son correctos y seguros.

Parte 2: Investigación sobre Planes y Casos de Prueba

¿Qué es un Plan de Pruebas?

Un plan de pruebas es un documento que describe el enfoque, los recursos y las actividades necesarios para garantizar que una aplicación funcione correctamente. Este plan indica qué se va a probar, cómo se va a hacer, qué herramientas se usarán, quién realizará las pruebas y qué resultados se esperan.

¿Qué son los Casos de Prueba?

Los casos de prueba son instrucciones específicas que permiten evaluar si una funcionalidad del sistema se comporta como se espera. Incluyen una descripción de lo que se va a probar, los pasos a seguir y el resultado esperado.

Ejemplo de Plan de Pruebas para Catálogo CRUD

A continuación se presenta un ejemplo de plan de pruebas para validar una aplicación que permite crear, editar y eliminar registros de productos en un catálogo.

Caso #	Funcionalidad	Descripción	Pasos para probar	Resultado esperado	Estado
1	Crear producto	Verificar que se pueda crear un producto con datos válidos	1. Ir a 'Nuevo producto' 2. Ingresar datos válidos 3. Presionar 'Guardar'	El producto aparece en la lista	Alto
2	Crear producto vacío	Verificar que no se permita crear un producto sin nombre	1. Ir a 'Nuevo producto' 2. Dejar nombre vacío 3. Presionar 'Guardar'	Mensaje de error indicando que el nombre es obligatorio	Alto
3	Editar producto	Verificar que se pueda modificar un producto existente	1. Seleccionar producto 2. Cambiar precio 3. Guardar cambios	El producto se actualiza	Alto
4	Eliminar producto	Verificar que se pueda eliminar un producto	1. Seleccionar producto 2. Clic en 'Eliminar' 3. Confirmar	El producto desaparece	Alto
5	Validación duplicado	Intentar crear un producto con nombre repetido	1. Ingresar un nombre ya existente 2. Guardar	Mensaje indicando nombre en uso	Alto