# 📘 Glosario: Mitigación de Vulnerabilidades en Aplicaciones Web

---

## 🔒 1. Mitigación

Conjunto de medidas que se aplican para **reducir el impacto de una vulnerabilidad** una vez detectada, sin necesariamente eliminar su causa raíz.

---

## 🛡️ 2. Prevención

Acciones **proactivas y planificadas** para evitar que se generen vulnerabilidades o sean explotadas, usualmente integradas desde las etapas iniciales del desarrollo.

---

## 🧱 3. Inyección SQL (SQLi)

Tipo de vulnerabilidad que permite a un atacante **insertar o manipular sentencias SQL**, comprometiendo bases de datos al pasar código malicioso a través de entradas del usuario.

---

## 🦠 4. Cross-Site Scripting (XSS)

Vulnerabilidad que permite inyectar scripts maliciosos en una página web, **ejecutándose en el navegador de otros usuarios**, lo que puede derivar en robo de cookies o secuestro de sesiones.

---

## 🎭 5. Cross-Site Request Forgery (CSRF)

Ataque que engaña al navegador del usuario para que realice **acciones no autorizadas** en una aplicación web en la que el usuario está autenticado.

---

## 🔧 6. Prepared Statement

Técnica que separa el código SQL de los datos ingresados por el usuario, **previniendo la inyección SQL** al utilizar parámetros en lugar de concatenación directa.

---

## ⚙️ 7. Validación de entradas

Proceso mediante el cual se **verifica y filtra la información ingresada** por el usuario, impidiendo que datos maliciosos lleguen al backend.

---

## 🔄 8. Escape de caracteres / Codificación de salida

Técnica que reemplaza caracteres especiales por entidades seguras, evitando que el contenido del usuario **sea interpretado como código ejecutable** (clave para mitigar XSS).

---

## 🧪 9. Content Security Policy (CSP)

Cabecera de seguridad que permite definir las fuentes de contenido autorizadas por una aplicación, limitando la ejecución de scripts externos y reduciendo la superficie de ataque XSS.

---

## 🔐 10. Token CSRF

Valor secreto generado por el servidor e incluido en formularios, que debe ser enviado con cada solicitud para verificar su legitimidad y evitar ataques CSRF.

---

## 🧰 11. Web Application Firewall (WAF)

Dispositivo o software que **analiza el tráfico HTTP** hacia una aplicación web, bloqueando automáticamente patrones maliciosos comunes como SQLi y XSS.

---

## 🧬 12. OWASP ZAP (Zed Attack Proxy)

Herramienta gratuita y de código abierto para pruebas de seguridad en aplicaciones web, que permite detectar vulnerabilidades mediante análisis activo y pasivo.

---

## 🕷️ 13. Burp Suite

Conjunto de herramientas para **auditoría de seguridad web profesional**, que permite interceptar, modificar y automatizar pruebas sobre aplicaciones en tiempo real.

---

## 🧩 14. Framework de Seguridad

Conjunto de librerías o configuraciones integradas que facilitan la **implementación de controles defensivos**, como autenticación, autorización y codificación segura.

---

## 🧪 15. Entorno controlado (Laboratorio de seguridad)

Espacio virtualizado o aislado donde se pueden **simular ataques y aplicar defensas** sin comprometer sistemas reales, usado para formación o pruebas de seguridad.

---

## 🧰 16. ModSecurity

WAF de código abierto que permite establecer reglas personalizadas para proteger aplicaciones web contra ataques como XSS, CSRF o SQLi.

---

## 📦 17. Dependencia vulnerable

Biblioteca externa que contiene una **falla de seguridad conocida**, y que al no ser actualizada, representa un riesgo para la aplicación que la utiliza.

---

## 🧠 18. Hardening

Proceso de **fortalecimiento de un sistema**, eliminando configuraciones inseguras y deshabilitando servicios innecesarios para reducir la superficie de ataque.

---

## 📋 19. Análisis estático de código (SAST)

Técnica que analiza el código fuente sin ejecutarlo, detectando patrones peligrosos y malas prácticas que pueden convertirse en vulnerabilidades.

---

## 📊 20. Análisis dinámico (DAST)

Evaluación de una aplicación **en tiempo de ejecución**, simulando ataques para identificar fallos que solo aparecen cuando la app está activa.

---