📘 Glosario: Vulnerabilidades Comunes en Aplicaciones Web

---

1. Aplicación Web

Programa que se ejecuta en un servidor y es accesible desde un navegador, permitiendo la interacción entre usuarios y datos a través de Internet.

---

2. Vulnerabilidad

Debilidad en un sistema que puede ser explotada por un atacante para comprometer su seguridad, como acceso no autorizado, pérdida de datos o daño a la integridad del sistema.

---

3. Inyección SQL (SQLi)

Técnica que permite insertar código SQL malicioso en una consulta de base de datos, lo que puede generar acceso no autorizado, manipulación de datos o control total del sistema.

---

4. Prepared Statement

Consulta SQL preparada que separa los datos del código, lo cual evita que los datos del usuario se interpreten como comandos maliciosos. Previene eficazmente la inyección SQL.

---

5. Sanitización

Proceso de limpiar y filtrar entradas de usuario para eliminar caracteres potencialmente peligrosos que puedan alterar la lógica del sistema o ser interpretados como código.

---

6. Validación de Entradas

Verificación sistemática de que los datos ingresados por el usuario cumplen con el tipo, formato y restricciones esperadas antes de ser procesados.

---

7. Cross-Site Scripting (XSS)

Vulnerabilidad que permite a un atacante insertar y ejecutar scripts maliciosos en una página web, afectando a los usuarios que la visitan. Puede ser reflejado, almacenado o basado en DOM.

---

8. Reflejado (XSS Reflected)

Tipo de ataque XSS en el que el script malicioso se incluye en una URL y se ejecuta inmediatamente en la respuesta del servidor sin ser almacenado.

---

9. Almacenado (XSS Stored)

Tipo de XSS donde el script malicioso se guarda en una base de datos o sistema y se ejecuta cada vez que otro usuario accede al contenido infectado.

---

10. DOM-based XSS

Tipo de XSS que se ejecuta en el navegador del usuario a través de la manipulación del DOM (Document Object Model), sin intervención del servidor.

---

11. Escape de Caracteres

Técnica que convierte caracteres especiales (como `<`, `>`, `&quot;`) en entidades HTML seguras para evitar que se interpreten como código ejecutable.

---

12. htmlspecialchars()

Función de PHP que transforma caracteres especiales en entidades HTML para prevenir ataques XSS.

---

13. Cross-Site Request Forgery (CSRF)

Ataque que consiste en forzar a un usuario autenticado a ejecutar acciones no deseadas sin su consentimiento, generalmente mediante la carga de solicitudes desde sitios externos.

---

14. Token CSRF

Valor único generado por el servidor e incluido en formularios críticos para verificar que las solicitudes provienen de una fuente legítima y evitar ataques CSRF.

---

15. SameSite (Cookie)

Atributo de seguridad que restringe el envío de cookies en solicitudes entre sitios, previniendo ataques CSRF.

---

16. Referer / Origin (Cabeceras HTTP)

Cabeceras utilizadas por el servidor para verificar el origen de una solicitud HTTP, permitiendo detectar solicitudes maliciosas desde otros dominios.

---

17. OWASP ZAP

Herramienta gratuita y de código abierto para realizar pruebas de seguridad en aplicaciones web, desarrollada por la comunidad OWASP.

---

18. Burp Suite

Suite de herramientas profesional utilizada para realizar pruebas de penetración y analizar la seguridad de aplicaciones web.

---

19. Pentesting

Proceso de pruebas de penetración en sistemas informáticos para identificar, explotar y documentar vulnerabilidades, de forma controlada y ética.

---

20. Exploit

Código o técnica que aprovecha una vulnerabilidad para comprometer un sistema, ejecutar código arbitrario o ganar acceso no autorizado.

---

21. Mitigación

Conjunto de acciones o mecanismos implementados para reducir o eliminar el impacto de una vulnerabilidad conocida en un sistema o aplicación.
