📘 Glosario: Explotación de Vulnerabilidades Web

---

1. Vulnerabilidad

Debilidad en el diseño, implementación o configuración de un sistema que puede ser aprovechada por un atacante para comprometer la seguridad.

---

2. Explotación

Proceso mediante el cual un actor malicioso o un auditor ético utiliza una vulnerabilidad para obtener acceso, modificar datos o alterar el funcionamiento de un sistema.

---

3. Inyección SQL (SQLi)

Tipo de ataque que consiste en insertar código SQL malicioso en una entrada de usuario para manipular la base de datos subyacente.

---

4. Cross-Site Scripting (XSS)

Vulnerabilidad que permite inyectar y ejecutar scripts maliciosos en el navegador de otro usuario, afectando su sesión o datos.

---

5. Cross-Site Request Forgery (CSRF)

Ataque que obliga a un usuario autenticado a ejecutar acciones no autorizadas en una aplicación en la que ha iniciado sesión.

---

6. Ejecución de Código Remoto (RCE)

Explotación que permite ejecutar comandos arbitrarios en el servidor de destino, generalmente mediante la carga de archivos maliciosos.

7. Payload

Fragmento de código o instrucción especialmente diseñado para explotar una vulnerabilidad específica.

---

8. Burp Suite

Suite de herramientas profesionales para pruebas de seguridad en aplicaciones web. Permite interceptar, modificar y automatizar análisis de tráfico web.

---

9. OWASP ZAP (Zed Attack Proxy)

Herramienta gratuita y de código abierto para pruebas de penetración en aplicaciones web, mantenida por el proyecto OWASP.

---

10. Fuzzing

Técnica automatizada que envía grandes volúmenes de entradas aleatorias o maliciosas a una aplicación para descubrir errores o vulnerabilidades.

---

11. Spidering

Proceso de navegación automática por una aplicación web para identificar todos los recursos y rutas disponibles.

---

12. DVWA (Damn Vulnerable Web Application)

Aplicación web intencionalmente vulnerable diseñada para fines educativos y de práctica en seguridad ofensiva.

---

13. Intercepción

Captura y manipulación del tráfico HTTP/S entre el navegador del usuario y el servidor web, generalmente mediante un proxy.

---

14. Auditoría Ética

Proceso estructurado de análisis de seguridad realizado con consentimiento, con el fin de identificar y mitigar vulnerabilidades antes de que sean explotadas maliciosamente.

---

15. Seguridad Ofensiva

Rama de la ciberseguridad centrada en simular ataques controlados para detectar debilidades y fortalecer la defensa de los sistemas.
