📘 Glosario: Herramientas de Auditoría: Burp Suite y OWASP ZAP

---

1. Burp Suite

Conjunto de herramientas para pruebas de penetración en aplicaciones web. Permite interceptar, modificar, repetir y automatizar solicitudes HTTP/S. Cuenta con versiones gratuita y profesional.

---

2. OWASP ZAP (Zed Attack Proxy)

Herramienta gratuita y de código abierto desarrollada por OWASP para encontrar vulnerabilidades de seguridad en aplicaciones web mediante análisis pasivo y activo.

---

3. Proxy

Componente que actúa como intermediario entre el navegador y el servidor. Permite interceptar y analizar tráfico HTTP/S. Tanto Burp Suite como ZAP utilizan proxies locales (por defecto en `127.0.0.1:8080`).

---

4. Repeater

Módulo de Burp Suite que permite repetir y modificar manualmente una solicitud HTTP para analizar cómo responde la aplicación a diferentes entradas.

---

5. Intruder

Herramienta dentro de Burp Suite que permite automatizar ataques como fuerza bruta, fuzzing o inyección, modificando múltiples parámetros en una misma solicitud.

---

6. Fuzzer (Fuzzing)

Técnica de prueba que envía múltiples entradas inesperadas, aleatorias o maliciosas a una aplicación para detectar comportamientos anómalos o vulnerabilidades.

---

7. Scanner (Burp)

Módulo que analiza de forma automática las solicitudes y respuestas HTTP para identificar vulnerabilidades comunes (solo disponible en la versión profesional de Burp Suite).

---

8. Spider

Funcionalidad que permite rastrear automáticamente todas las rutas, enlaces y parámetros de una aplicación web para mapear su estructura y superficie de ataque.

---

9. Escaneo Pasivo

Tipo de análisis que observa el tráfico existente sin enviar solicitudes adicionales. Útil para identificar vulnerabilidades sin generar ruido en la red.

---

10. Escaneo Activo

Método de análisis que envía solicitudes específicamente diseñadas para detectar vulnerabilidades, como inyecciones, XSS, errores de configuración, etc.

---

11. Intercepción (Intercept)

Función que permite detener una solicitud o respuesta HTTP antes de que llegue a su destino, permitiendo al auditor modificarla antes de reenviarla.

---

12. Payload

Conjunto de datos diseñados para probar una vulnerabilidad, como por ejemplo: `'; DROP TABLE users;--` (SQLi) o `<script>alert(1)</script>` (XSS).

---

13. Token de Sesión

Identificador único que gestiona la sesión activa del usuario. Burp y ZAP pueden analizar su entropía (aleatoriedad) y vulnerabilidades asociadas.

---

14. Comparador (Comparer)

Herramienta de Burp Suite que permite comparar dos cadenas de texto (como respuestas HTTP) para identificar diferencias útiles durante pruebas de fuzzing o bypass.

---

15. Sequencer

Módulo de Burp Suite para analizar tokens de sesión, cookies u otros identificadores y evaluar su imprevisibilidad (entropía), ayudando a detectar si pueden ser predecibles.

---

16. Crawling

Proceso automatizado mediante el cual se navega por un sitio web para descubrir páginas, formularios y parámetros ocultos o accesibles mediante enlaces internos.

---

17. Content-Security-Policy (CSP)

Cabecera de seguridad que restringe qué contenido puede cargarse en una aplicación web. Su ausencia puede ser detectada por herramientas como ZAP y Burp.

---

18. X-Frame-Options

Cabecera HTTP que previene ataques de clickjacking evitando que el sitio sea embebido en marcos (`iframes`). Es auditada por herramientas de seguridad.

---

19. Automatización de Pruebas

Uso de herramientas como Intruder o ZAP Fuzzer para realizar pruebas de seguridad a gran escala sin intervención humana continua, acelerando la detección de vulnerabilidades.

---

20. Auditoría Ética

Evaluación controlada y con consentimiento de la seguridad de una aplicación. Su objetivo es descubrir y mitigar vulnerabilidades antes de que sean explotadas de forma maliciosa.
