



Pruebas de Penetración: Metodologías, Técnicas y Herramientas Especializadas



Introducción + Definición



Introducción + Definición

- Las pruebas de penetración (Pentesting) permiten detectar y explotar vulnerabilidades antes que un atacante real.
- Requieren autorización ética y legal.
 - Qué es? Evaluación controlada para descubrir vulnerabilidades explotables.
 - Simula ataques reales para validar la seguridad.



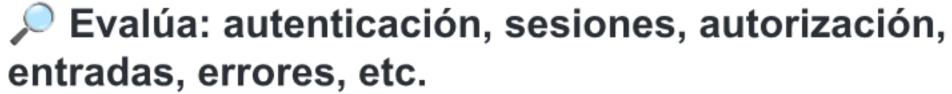


Metodología OWASP Testing Guide



Metodología OWASP Testing Guide

- Fases principales:
 - Planificación
 - Recolección de información
 - Evaluación activa (XSS, SQLi, CSRF)
 - Reporte técnico







Metodología PTES y Comparación



Metodología PTES y Comparación

PTES: 7 fases desde el pre-compromiso hasta el reporte final.

Aplica a redes, infraestructuras y apps críticas.

OWASP vs PTES

OWASP TG	PTES
Web Apps	Infraestructura
4	7
Técnico-web	Multientorno
Auditoría Web	Pentesting Pro
	Web Apps 4 Técnico-web





Técnica – Inyección SQL (SQLi)



Técnica – Inyección SQL (SQLi)

Ataque: Manipula consultas SQL inseguras
P Ejemplo:

SELECT usuario FROM clientes WHERE id = ' ' + usuario_id + ' '; usuario_id = ' OR '1'='1

Prevención:

- Consultas parametrizadas
- Validación de entradas
- Gestión de errores





Técnica – XSS y CSRF



Técnica – XSS y CSRF

- XSS (Cross-Site Scripting)
 <script>alert('XSS Vulnerability!');</script>
- Prevención: Validación, codificación, CSP
- CSRF (Cross-Site Request Forgery)
 Prevención:
 - Tokens antiforgery
 - Validación de Referer
 - Cookies SameSite



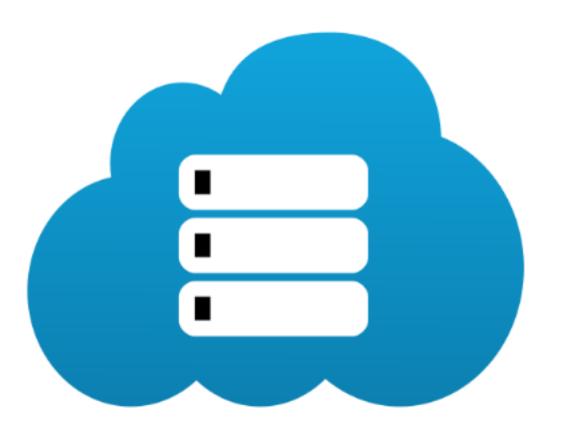


Herramienta – Metasploit Framework



Herramienta – Metasploit Framework

- Plataforma para explotación y post-explotación Características:
 - Exploits clasificados
 - Simulación de ataques
- Ideal junto a Nmap y OpenVAS





Herramienta – Burp Suite



Herramienta – Burp Suite

- Análisis de seguridad para aplicaciones web Módulos:
 - Proxy interceptante
 - Spider, Intruder, Repeater
 - **V** Detecta: SQLi, XSS, CSRF y más





Ética Profesional y Legalidad



Ética Profesional y Legalidad

- Las pruebas requieren autorización explícita
- Cumplir estándares éticos y legales
- Documentar toda actividad
- Uso indebido = consecuencias legales graves





Conclusión



Conclusión

- **W**OWASP y PTES son marcos robustos
- SQLi, XSS y CSRF siguen siendo amenazas frecuentes
- Metasploit y Burp Suite permiten simular ataques reales
- La ética profesional garantiza pruebas responsables
- Un sistema solo es tan fuerte como su última prueba de seguridad



Energiza!