



Pruebas de Penetración: Metodologías,  
Técnicas y Herramientas Especializadas

## 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

### Fases principales:

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


 **Evalúa:** autenticación, sesiones, autorización, entradas, errores, etc.





## 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

Aspecto	OWASP TG	PTES
Enfoque	Web Apps	Infraestructura
Fases	4	7
Nivel	Técnico-web	Multientorno
Uso	Auditoría Web	Pentesting Pro



## Técnica – Inyección SQL (SQLi)

💣 Ataque: Manipula consultas SQL inseguras

📌 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

 **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

 **Plataforma para explotación y post-explotación**

 **Características:**

- Exploits clasificados
- Simulación de ataques

 **Ideal junto a Nmap y OpenVAS**





## Herramienta – Burp Suite

 **Análisis de seguridad para aplicaciones web**

 **Módulos:**

- Proxy interceptante
- Spider, Intruder, Repeater
- ✓ **Detecta: SQLi, XSS, CSRF y más**





## Ética Profesional y Legalidad

⚠ Las pruebas requieren **autorización explícita**

👤 Cumplir estándares éticos y legales

📄 Documentar toda actividad

! Uso indebido = consecuencias legales graves



## Conclusión

- ✓ OWASP y PTES son marcos robustos
- ✓ SQLi, XSS y CSRF siguen siendo amenazas frecuentes
- ✓ Herramientas como **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



