



# Explotación de Vulnerabilidades en Aplicaciones Web

## Objetivo General

Esta lección tiene como finalidad comprender las bases de la explotación de vulnerabilidades web, abordando técnicas como **SQLi**, **XSS** y **CSRF**. Se busca aplicar herramientas profesionales, como **Burp Suite** y **OWASP ZAP**, en entornos controlados para reforzar el análisis técnico y ético.



## ¿Qué es una Vulnerabilidad Web?

Una **vulnerabilidad en una aplicación web** representa una falla en su diseño, configuración o desarrollo, que puede ser explotada para comprometer la seguridad del sistema. Su existencia puede impactar directamente la confidencialidad, integridad o disponibilidad de los datos.



## ¿Qué es la Explotación?

La explotación consiste en utilizar de forma intencionada una vulnerabilidad para acceder, alterar o destruir información dentro de un sistema. Esta práctica puede ser maliciosa o ética, dependiendo de si es realizada por un atacante o un auditor autorizado.





## Técnicas de Explotación Comunes

Entre las técnicas más críticas se encuentran **SQL Injection**, **Cross-Site Scripting**, **CSRF** y ejecución de código malicioso. Estas pueden activarse a través de formularios, **URLs** o cargas de archivos, comprometiendo tanto servidores como usuarios.



## Herramientas Profesionales de Análisis

**Burp Suite y OWASP ZAP** son herramientas clave en el pentesting web. Ambas permiten interceptar tráfico, automatizar pruebas de vulnerabilidades y generar reportes. Su uso en entornos éticos permite validar fallas sin comprometer sistemas reales.





## Ejercicio en Entorno Controlado

Plataformas como **DVWA (Damn Vulnerable Web Application)** permiten practicar técnicas reales en un entorno simulado. Estas prácticas fortalecen la comprensión del comportamiento de las vulnerabilidades y su mitigación, respetando principios éticos.



## Conclusión

La explotación de vulnerabilidades no es un acto de daño, sino una auditoría técnica y ética destinada a mejorar la seguridad. Aplicada correctamente, permite identificar debilidades antes que los atacantes, protegiendo así los activos críticos de una organización.





