sustantiva
CON•SENTIDO

Energiza!

ATAQUES DE DOMINIO CRUZADO: CROSS-SITE SCRIPTING (XSS)

Objetivos de la Lección

Objetivos de la Lección

Comprender los **ataques de dominio cruzado** permite identificar vulnerabilidades que explotan la confianza entre navegador y servidor. Esta lección te ayudará a diferenciar los tipos de **XSS**, analizar cómo funciona **CSRF**, utilizar **herramientas de explotación ética**, y aplicar **estrategias de mitigación** efectivas en entornos reales.

¿Qué son los ataques Cross-Domain?

¿Qué son los ataques Cross-Domain?

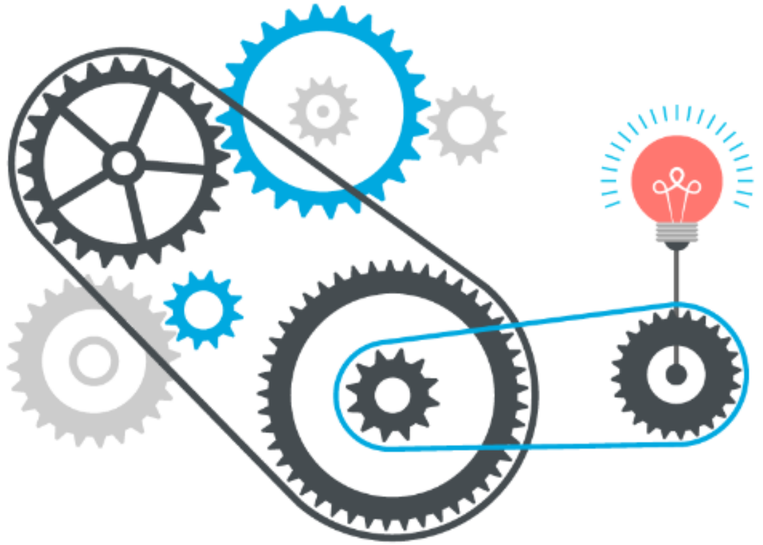
Los ataques de **dominio cruzado** son vulnerabilidades que se aprovechan de la **confianza implícita** entre el navegador del usuario y el sitio web visitado. Estos ataques, como **XSS** y **CSRF**, no necesariamente vulneran el servidor, sino que manipulan el comportamiento del cliente para lograr **acceso o ejecución no autorizada**.

API INTERFACE

XSS – Cross-Site Scripting

XSS – Cross-Site Scripting

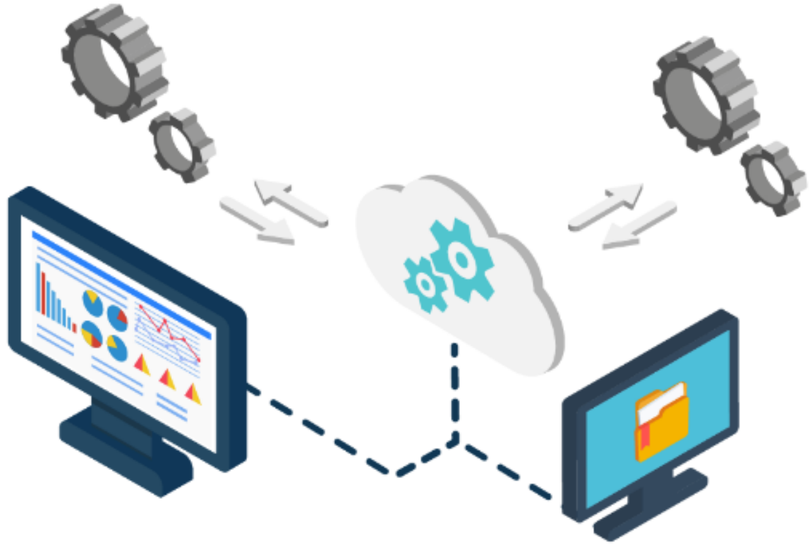
El **Cross-Site Scripting (XSS)** permite al atacante **inyectar scripts maliciosos** en páginas legítimas. Este código se ejecuta en el **navegador del usuario**, robando información, manipulando sesiones o redirigiendo tráfico. XSS explota la **confianza del navegador en el contenido del sitio web** sin necesidad de vulnerar el servidor.



XSS – Cross-Site Scripting

XSS – Cross-Site Scripting

El **Cross-Site Scripting (XSS)** permite al atacante **inyectar scripts maliciosos** en páginas legítimas. Este código se ejecuta en el **navegador del usuario**, robando información, manipulando sesiones o redirigiendo tráfico. XSS explota la **confianza del navegador en el contenido del sitio web** sin necesidad de vulnerar el servidor.



Tipos de XSS según OWASP

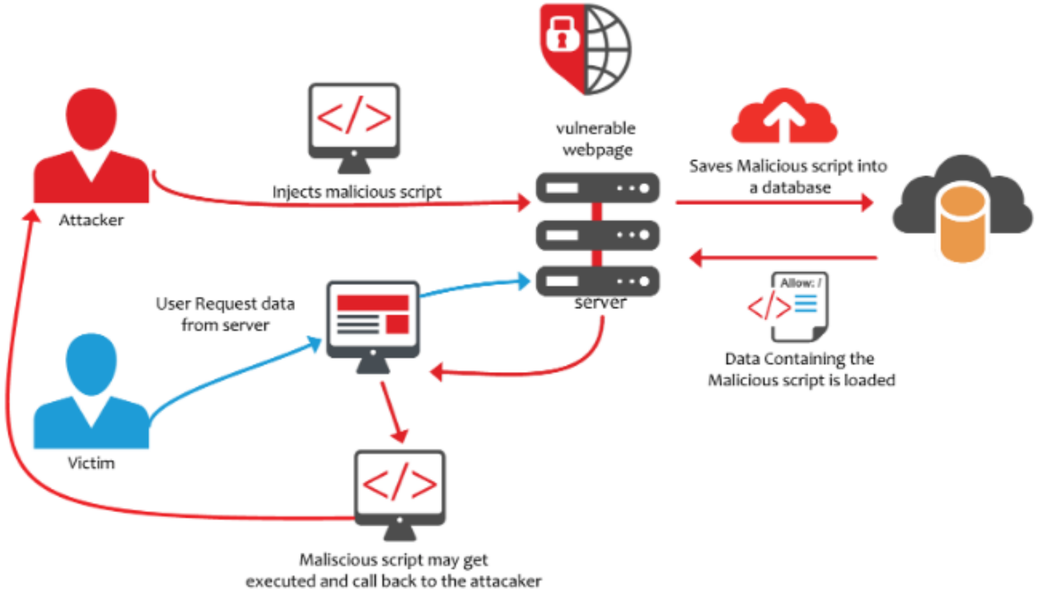
Tipos de XSS según OWASP

- **Reflejado (Reflected):** el script se ejecuta inmediatamente desde la URL.
- **Almacenado (Stored):** el script queda **guardado** en la base de datos y se ejecuta cada vez que otros usuarios lo cargan.
- **DOM-Based:** manipula el **DOM del navegador** sin interacción directa con el servidor.
  Cada tipo requiere enfoques específicos de **detección y mitigación**.

¿Qué es CSRF y cómo funciona?

¿Qué es CSRF y cómo funciona?

El **Cross-Site Request Forgery (CSRF)** consiste en hacer que un usuario autenticado realice acciones sin su consentimiento. El navegador envía **peticiones válidas** a una aplicación confiable, pero **iniciadas maliciosamente** desde otro sitio. Puede afectar acciones críticas como **transferencias de dinero**, **cambios de contraseña** o **borrado de cuentas**.



Herramientas de Explotación Ética

Herramientas de Explotación Ética

Herramientas como **Burp Suite** y **OWASP ZAP** permiten interceptar, modificar y automatizar solicitudes para detectar **XSS y CSRF**. Simulan ataques en entornos controlados y generan **reportes detallados**, ayudando a validar vulnerabilidades antes de que sean explotadas por actores maliciosos.

Mitigación Efectiva de XSS y CSRF

Mitigación Efectiva de XSS y CSRF

Para **XSS**, se deben **codificar caracteres especiales**, **validar entradas**, y aplicar **Content Security Policy (CSP)**. Para **CSRF**, es esencial usar **tokens únicos**, **cookies con atributo SameSite**, y verificar el **origen de las solicitudes**. Estas medidas deben implementarse tanto en el **cliente** como en el **servidor**.

Conclusión

Conclusión

Los ataques **XSS y CSRF** son silenciosos pero muy comunes. Afectan tanto al **usuario final** como a la **lógica del servidor**. Su mitigación exige **educación del desarrollador**, uso de **herramientas profesionales** y aplicación de **buenas prácticas de seguridad desde el diseño**. Dominar estos conceptos es vital para construir **aplicaciones realmente seguras**.


Energiza!