Se trata de un tipo de inseguridad informática en sitios web, que permite a una persona inyectar en sitios web código JavaScript u otro lenguaje similar, evitando medidas de control como la Política del mismo origen.

En español, este tipo de inseguridades se conocen como Secuencias de órdenes en sitios cruzados.
Es común encontrar estas vulnerabilidades en sitios web cuyas funciones sean presentar la información en un navegador web o en otro contenedor de páginas web. También existen aplicaciones locales vulnerables, por lo que no únicamente existen en sitios en Internet.

Este tipo de ataque puede ser utilizado para el robo de información, robar sesiones de usuario y comprometer al navegador. Las vulnerabilidades XSS han existido prácticamente desde que comenzó Internet.

Normalmente, se obtiene la vulnerabilidad al no validar de forma correcta los datos de entrada que se utilizan en alguna aplicación, o al no verificar adecuadamente la salida para su presentación como página web.

Se puede presentar esta vulnerabilidad en dos formas, directa e indirecta.

•Directa, denominada también persistente, consisten en la inserción de código HTML peligroso en páginas que lo permitan, incluyendo etiquetas como <script> o <iframe>.
•Indirecta, también llamada reflejada, consiste en modificar los valores que la aplicación web usa para el paso de variables entre dos páginas, sin utilizar sesiones y ocurre cuando hay un mensaje o una ruta en la URL del navegador, en una cookie o cualquier otra cabecera HTTP.

Un ejemplo de una inyección XSS indirecta, puede ser la inserción de un código JavaScript para un bucle de mensaje de alerta, que más que algo malo, se podría considerar como una broma. Sin embargo, un atacante podría insertar códigos que roben información de cookies o

sesiones de usuarios.

El uso de AJAX en XSS no es muy común, pero es bastante peligroso. Se utiliza cualquier tipo de vulnerabilidad se XSS para introducir un objeto XMLHTTP y usarlo para el envío de contenido POST, GET, sin que el usuario lo sepa.

Es muy común este tipo de ataques mediante gusanos de XSS, que se multiplican por medio de las vulnerabilidades de XSS persistentes.