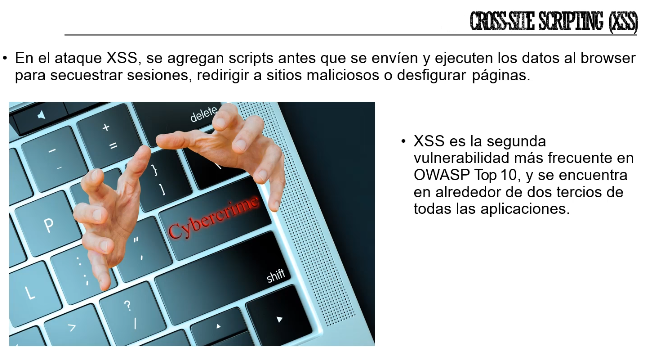
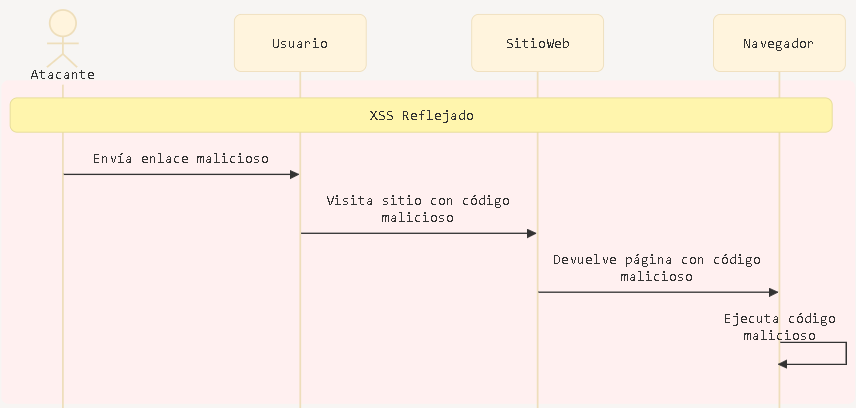
**Cross Site Scripting (XSS)**

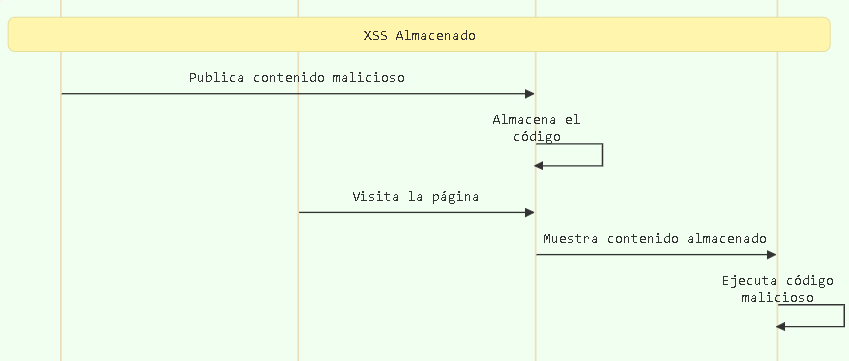
****

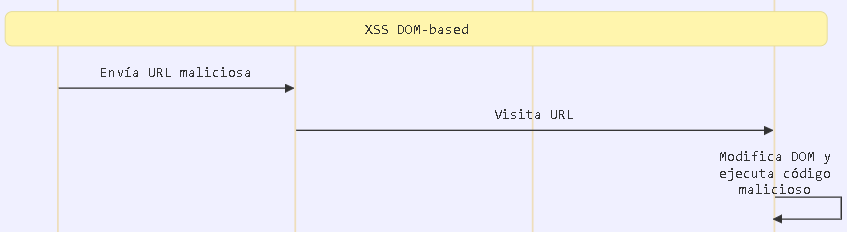
Este ataque hace que en nuestro navegador web se ejecuten scripts maliciosos para, por ejemplo, secuestrar sesiones, redirigir a otros sitios donde tiene acceso el hacker, engañando al cliente, haciéndole creer que está en nuestra aplicación cuando realmente no lo está. Este ataque puede emular una web bancaria o reconfigurar o configurar páginas, creando y diluyendo componentes en ellas.

Esta vulnerabilidad, aunque parece poco frecuente, realmente no lo es, porque son muchos los que tienen JavaScript que intentan hackear nuestras páginas web. Se estima que se encuentra en alrededor de dos tercios de todas nuestras aplicaciones.

El Cross-Site Scripting (XSS) es una vulnerabilidad de seguridad web que permite a los atacantes inyectar código malicioso en sitios web legítimos. Este código se ejecuta en el navegador de los usuarios que visitan el sitio, permitiendo acciones como robar credenciales o redirigir usuarios a sitios maliciosos.







En el diagrama anterior podemos ver las tres formas principales de ataques XSS:

XSS Reflejado: El atacante envía un enlace malicioso al usuario, quien lo visita, permitiendo que el código se ejecute en su navegador.

XSS Almacenado: El código malicioso se guarda primero en el sitio web y luego afecta a todos los usuarios que visitan esa página.

XSS DOM-based: El ataque ocurre completamente en el navegador del usuario sin necesidad de almacenamiento en el servidor.

Ejemplo práctico de XSS reflejado

Un atacante puede crear un enlace que parece normal pero contiene código malicioso que se ejecutará cuando el usuario haga clic.

