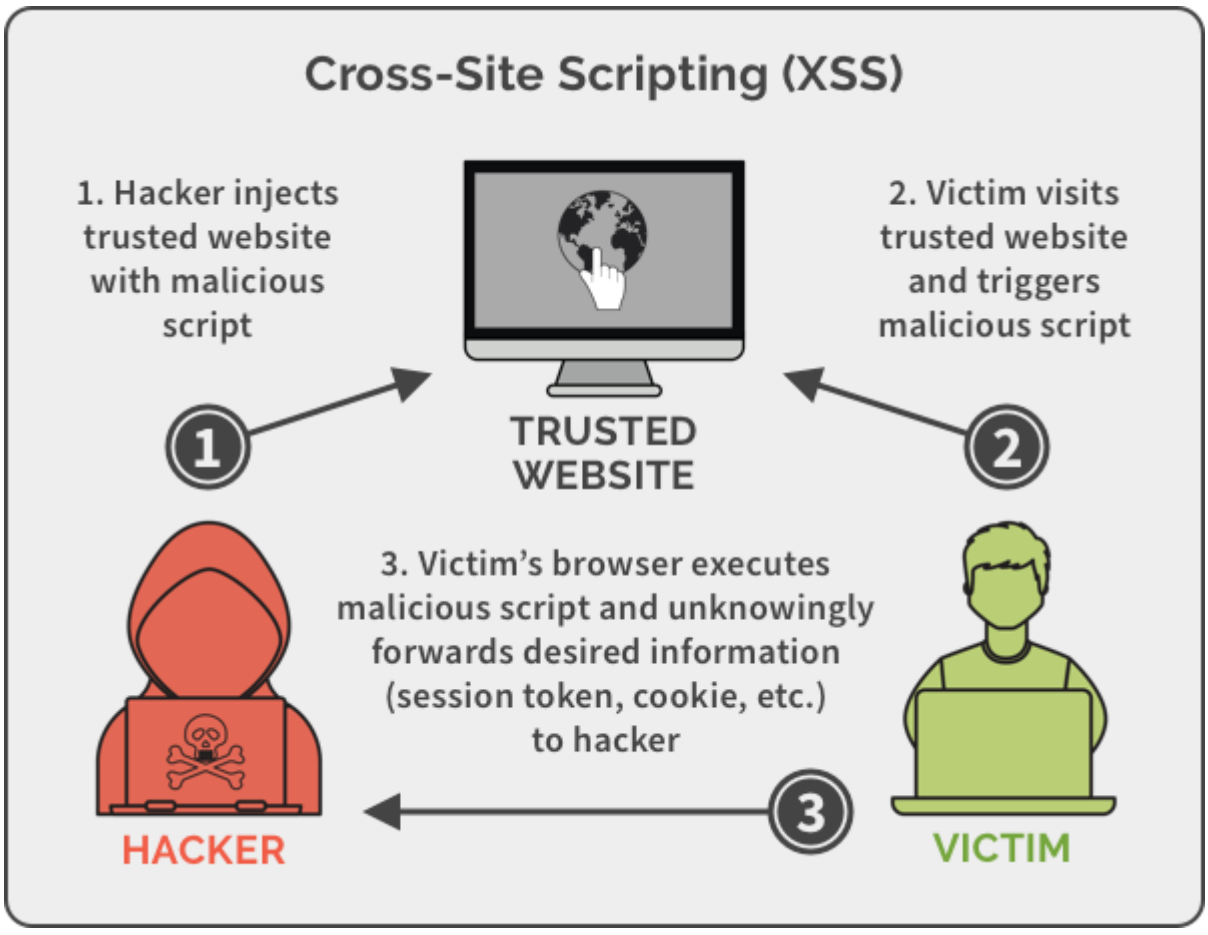
GLOSARIO CIBERSEGURIDAD (ORIENTADO A WEB)

Cifrar: Es la conversión de datos legibles a unos cifrados y solo se puede descifrar con una clave de cifrado.

Confidencialidad: Garantización de nivel necesario de secretismo a la información y de su tratamiento, para prevenir su divulgación no autorizada.

Cross-Site Scripting (XSS): Es un ataque que logra inyectar código malicioso en una web donde ha encontrado un agujero de seguridad para luego pasar el enlace a los usuarios para luego ser ejecutado y enviar la información al atacante. Engañar al servidor haciéndolo creer que tú eres otro cliente.



Disponibilidad: Asegura que los usuarios autorizados puedan acceder a la información cuando lo necesiten.

DoS: Hacer que una web no esté disponible sobrecargándola con peticiones. Tirar una página a fuerza bruta.

DDoS: Es lo mismo que DoS (Denial of Service) pero con la contribución de muchos equipos.

Exploits: Un software de aprovechamiento de vulnerabilidades para alterar el funcionamiento normal de una web que tú ejecutas. Para poder escribir uno de estos debes ser excelente en sistemas operativos y redes. Para ejecutarlos solo necesitas dinero. Hacer estos programas no son delitos, pero usarlos sí.

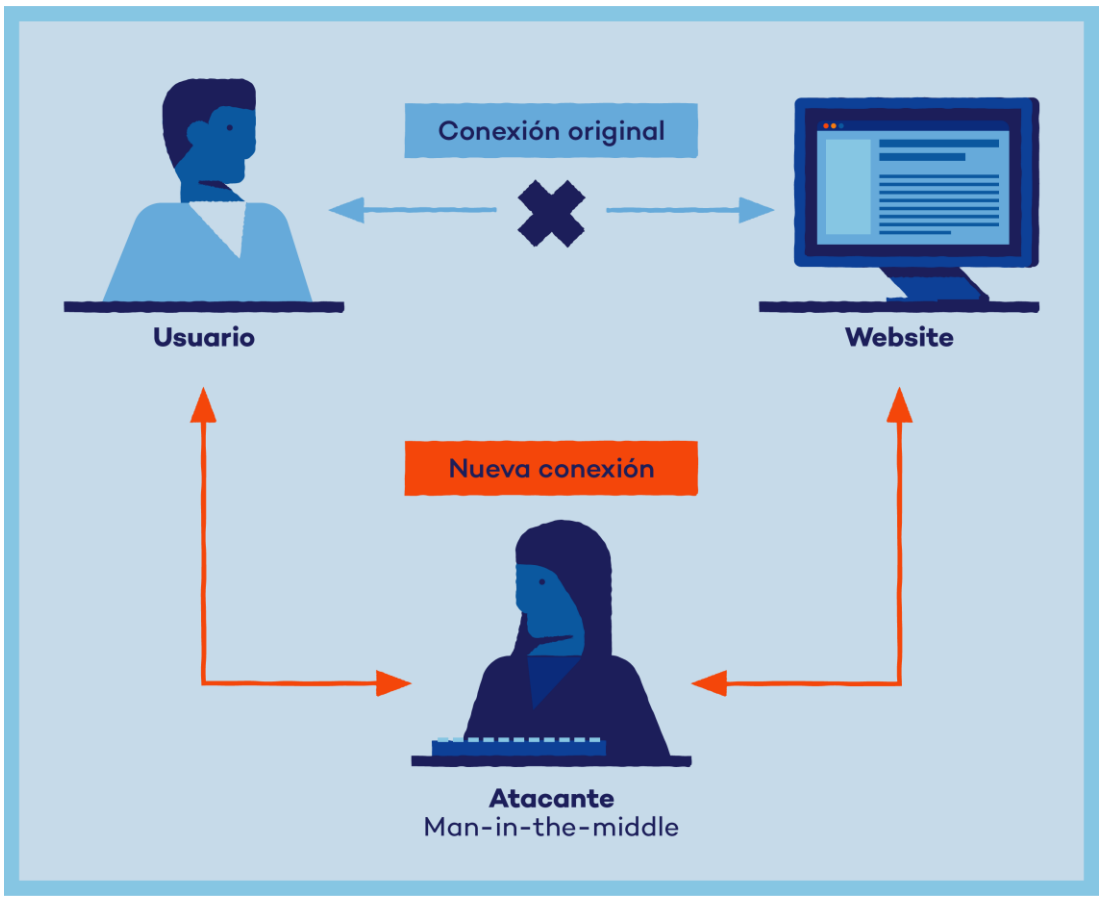
Ingeniería social: Técnicas de manipulación usada para obtener información confidencial. Por ejemplo, haciéndose pasar por tu empresa bancaria diciendo que ha habido un problema en tu cuenta y te pide identificarte (para robarte los datos). No sé cómo desarrollarlo más

Integridad: La capacidad para garantizar la fiabilidad de los datos y asegurar que no se han modificado ni manipulado.

Inyección SQL: Infiltración de código mediante una vulnerabilidad en el nivel de validación para realizar operaciones sobre la base de datos. Escribir sentencias sql en el registro de usuario para conseguir ejecutar instrucciones SQL.

Malware: Programa maligno que se ejecuta sin ser detectado y realiza funciones perjudícales.

Man-in-the-Middle: Es un ataque donde el criminal se posiciona entre el usuario y la aplicación web y puede leer, insertar y/o modificar.



Ransomware: Es un programa que restringe el acceso a determinadas partes mediante cifrado y pide un rescate para quitar esa restricción.

2. Medidas de protección básicas

Autenticación Multifactor (MFA): Método de seguridad para identificar a los usuarios, no dependiendo solo de una contraseña. Se suele dividir en 3 partes: 1. Algo que el usuario sabe (contraseña), algo que el usuario tiene (teléfono) y algo que el usuario es (identificación facial)

Roles y permisos:

Reglas de firewall:

Firewall: Software pensado para impedir el tráfico de una red con otra (se toma en la capa de red, si fuera en la de transporte o la de aplicación es proxy porque mira el paquete)

Filtrado de puertos y protocolos:

Routers: Poner en contacto una red con otra

Monitoreo:

Auditoría: