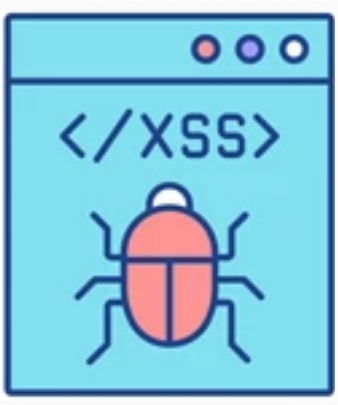
José Gilberto Guzmán Gutiérrez

Tipos de ataques en un sistema. Web.

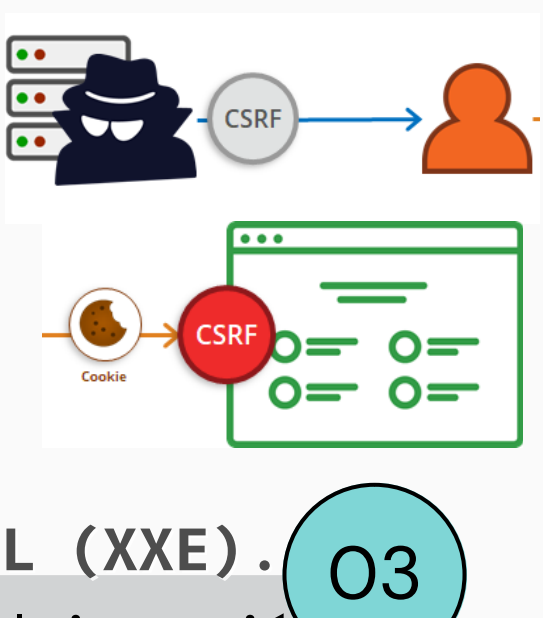
01 Secuencias de comandos entre sitios (XSS).

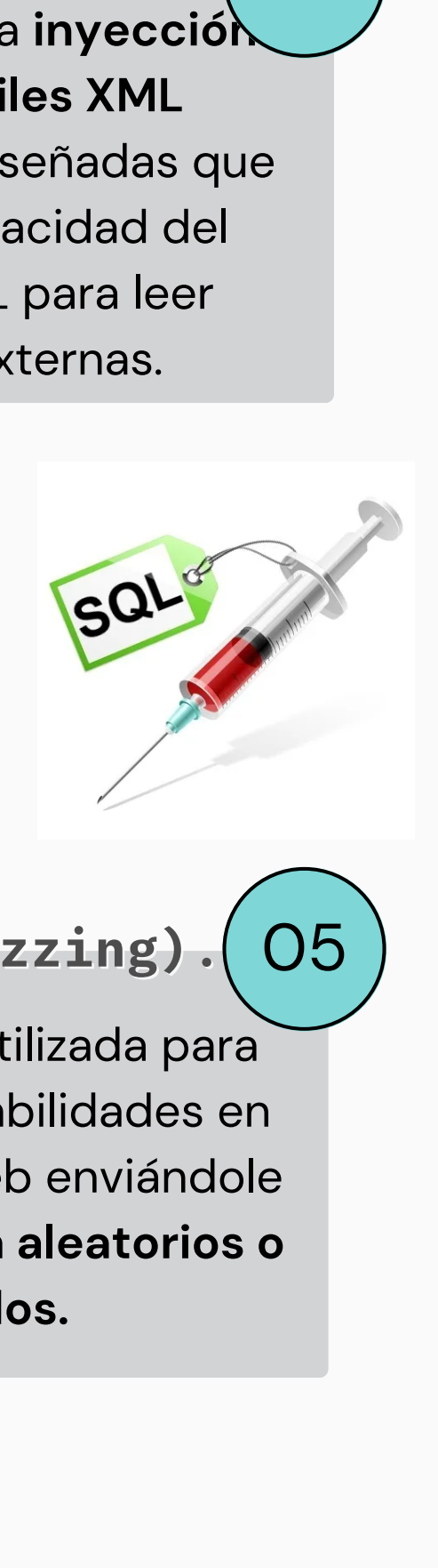


implica **inyectar scripts** maliciosos en páginas web que ven otros usuarios.

02 Falsificación de solicitudes entre sitios (CSRF).

Engaña a un usuario para que **ejecute una acción no deseada** en una aplicación web en la que ya está autenticado.





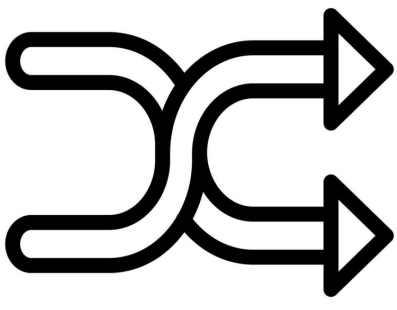
03 Entidad externa XML (XXE).

Suelen implicar la **inyección de cargas útiles XML** especialmente diseñadas que explotan la capacidad del analizador XML para leer entidades externas.

04 Ataques de inyección.

Implican la **inserción de código malicioso** en una aplicación web, normalmente en forma de datos de entrada, como consultas **SQL**.

05 Prueba de fuzz (fuzzing).

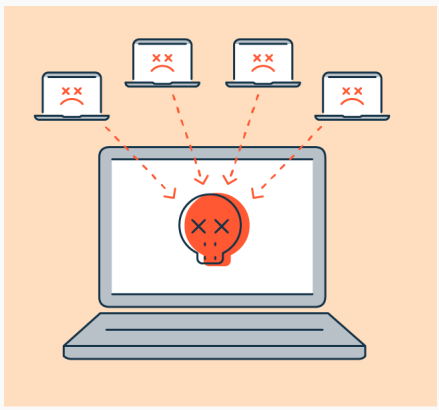


Es una técnica utilizada para descubrir vulnerabilidades en una aplicación web enviándole **datos de entrada aleatorios o no válidos.**

José Gilberto Guzmán Gutiérrez

DDoS (Denegación de servicio distribuida).

06



implica sobrecargar una aplicación web con un **gran volumen de tráfico procedente de múltiples fuentes**, como botnets o dispositivos comprometidos.

07

Ataque de fuerza bruta.

Utilizan herramientas de software para **probar diferentes combinaciones** de nombres de usuario y contraseñas hasta que logran adivinar la correcta.

Recorrido del camino.

08

implica **manipular rutas de archivos** en una aplicación web para acceder a archivos o directorios no autorizados en el servidor.

Móvil.

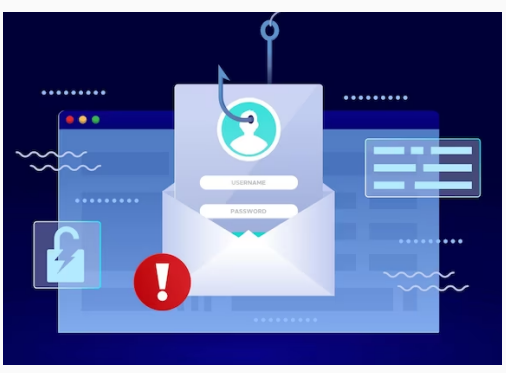
01

Apk Malicioso.

Crean aplicaciones móviles maliciosas con la intención de **robar datos o controlar el dispositivo** del usuario.

Relleno de credenciales (Credential stuffing)

02



Prueban **combinaciones** de nombres de usuario y contraseñas **previamente filtradas** en otras brechas de seguridad para acceder a cuentas.

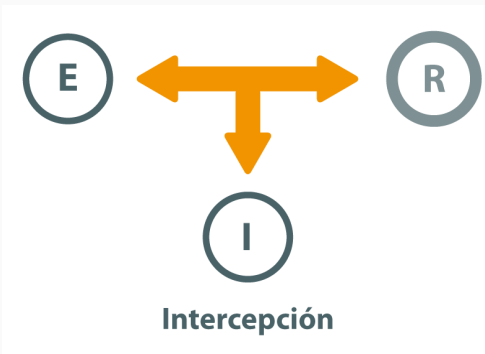
03

Reversing de aplicaciones.

Descompilan y analizan aplicaciones móviles **para descubrir vulnerabilidades y exploits**.

José Gilberto Guzmán Gutiérrez

04 Ataques de intercepción de tráfico.

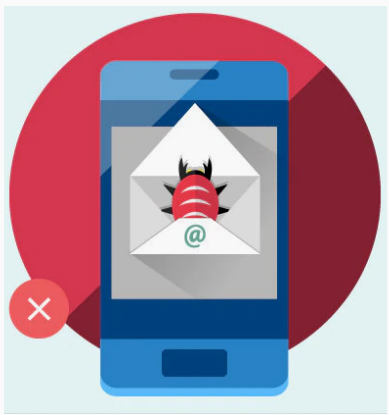


Intentan interceptar el **tráfico de red** entre la aplicación móvil y los servidores **para robar datos confidenciales**.

05 Rooting o Jailbreaking.

Los atacantes pueden intentar **desbloquear las restricciones del sistema operativo** para ganar acceso no autorizado y control total sobre el dispositivo.

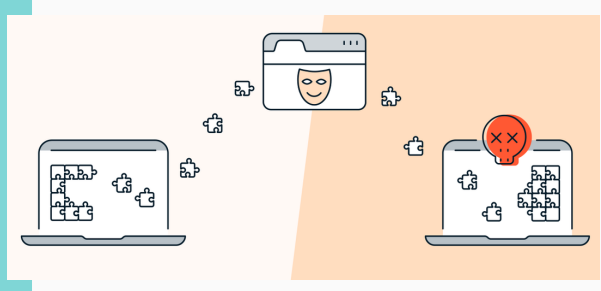
06 Malware móvil.



Suelen implicar la **inyección de cargas útiles XML** especialmente diseñadas que explotan la capacidad del analizador XML para leer entidades externas.

07 Ataques de suplantación (spoofing).

Pueden **falsificar la identidad de una aplicación legítima** para engañar a los usuarios y robar sus datos.



08 Ataques de ingeniería social.

Manipulan a los usuarios para que instalen aplicaciones maliciosas o revelen información confidencial.

Bibliografías.

- 8 types of web application attacks and protecting your organization. (2023, mayo 10). Bright Security. https://brightsec.com/blog/8-types-of-web-application-attacks-and-protecting-your-organization/
- Bull, T. (2022, marzo 30). What are the most popular attacks on mobile devices? Two River Computer. https://www.tworivercomputer.com/popular-attacks-mobile-devices/