📘 Glosario: Ataques de Inyección y Manipulación de Datos

---

1. Inyección SQL (SQLi)

Técnica que consiste en insertar instrucciones SQL maliciosas a través de formularios o parámetros no validados, con el fin de manipular la base de datos.

---

2. Inyección de Comandos (Command Injection)

Tipo de ataque que permite ejecutar comandos del sistema operativo a través de aplicaciones vulnerables, aprovechando entradas mal validadas.

---

3. Payload

Fragmento de código, texto o instrucción maliciosa diseñado para ser insertado en un sistema vulnerable con el fin de provocar un comportamiento no previsto.

---

4. Sanitización

Proceso de limpieza y codificación de entradas de usuario para eliminar o neutralizar caracteres peligrosos que puedan alterar la lógica de un sistema.

---

5. Validación de Entrada

Conjunto de reglas que determinan si los datos ingresados por un usuario cumplen con los requisitos esperados antes de ser procesados por la aplicación.

---

6. Consulta Parametrizada (Prepared Statement)

Mecanismo de ejecución de sentencias SQL que separa la lógica de la consulta de los datos del usuario, previniendo ataques por inyección.

7. Logs (Registros)

Archivos o estructuras donde se almacena información sobre eventos del sistema. Si no son protegidos, pueden ser manipulados para ocultar o insertar código malicioso.

---

8. Envenenamiento de Logs (Log Poisoning)

Técnica que introduce código malicioso en registros del sistema con el objetivo de ejecutar instrucciones en futuras visualizaciones o análisis.

---

9. Burp Suite

Herramienta avanzada de análisis de seguridad web que permite interceptar, modificar, repetir y automatizar peticiones HTTP/S para detectar vulnerabilidades.

---

10. SQLMap

Herramienta de código abierto que automatiza la detección y explotación de vulnerabilidades de inyección SQL.

---

11. Commix

Utilidad enfocada en detectar y explotar vulnerabilidades de inyección de comandos en aplicaciones web.

---

12. Metasploit

Framework de pruebas de penetración que permite desarrollar, lanzar y automatizar exploits contra sistemas vulnerables.

---

13. Principio de Mínimo Privilegio

Norma de seguridad que establece que cada componente o usuario debe tener únicamente los permisos necesarios para realizar sus funciones, ni más ni menos.

---

14. DVWA (Damn Vulnerable Web Application)

Aplicación web deliberadamente insegura utilizada para prácticas de hacking ético, pruebas de herramientas y aprendizaje en seguridad ofensiva.

---

15. Escalamiento de Privilegios

Proceso mediante el cual un atacante obtiene niveles de acceso más altos de los que debería tener, explotando fallas de control de acceso.
