📘 Glosario – Seguridad en Aplicaciones Web Modernas

---

1. API RESTful (Representational State Transfer)

Arquitectura de diseño para interfaces de programación que permite la comunicación entre sistemas distribuidos a través de protocolos estándar como HTTP. Las APIs RESTful son ampliamente utilizadas en aplicaciones web modernas por su escalabilidad y simplicidad.

---

2. SQL Injection (Inyección SQL)

Vulnerabilidad que permite insertar código SQL malicioso en una consulta mediante entradas no validadas. Puede llevar al acceso no autorizado a bases de datos, extracción de información sensible o modificación de datos.

---

3. Cross-Site Scripting (XSS)

Tipo de vulnerabilidad que permite a un atacante inyectar scripts maliciosos en páginas vistas por otros usuarios. Comúnmente utilizado para el robo de cookies, redireccionamientos o manipulación del DOM.

---

4. Cross-Site Request Forgery (CSRF)

Ataque que explota la confianza que una aplicación tiene en el navegador del usuario autenticado, forzando la ejecución de acciones no deseadas sin el consentimiento explícito del usuario.

---

5. JSON Web Token (JWT)

Formato compacto basado en JSON utilizado para transmitir información entre partes de forma segura. Comúnmente utilizado para autenticación sin estado (stateless) en aplicaciones distribuidas. Incluye firma digital para validar integridad.

---

6. OAuth 2.0

Protocolo de autorización ampliamente utilizado que permite a las aplicaciones acceder a recursos protegidos en nombre de un usuario, delegando la autenticación a un proveedor externo sin exponer credenciales.

---

7. Role-Based Access Control (RBAC)

Modelo de control de acceso que asigna permisos a roles y roles a usuarios, permitiendo una gestión granular y estructurada de los privilegios en una aplicación.

---

8. Sanitización de entradas

Proceso de limpieza de datos suministrados por el usuario para eliminar caracteres o estructuras potencialmente peligrosas que puedan ser utilizadas para ataques como XSS o SQLi.

---

9. Cifrado en tránsito / en reposo

Técnicas de protección de datos mediante criptografía durante su transmisión (por ejemplo, usando TLS) o mientras están almacenados (por ejemplo, cifrado AES en bases de datos o discos).

---

10. IAM (Identity and Access Management)

Sistema o conjunto de políticas y herramientas que gestionan las identidades digitales y los accesos a recursos en un entorno de TI. Fundamental en entornos cloud como AWS, Azure o GCP.

---

11. SIEM (Security Information and Event Management)

Soluciones que integran monitoreo, detección, análisis y respuesta ante incidentes de seguridad en tiempo real, mediante la correlación de eventos de múltiples fuentes.

---

12. OWASP (Open Web Application Security Project)

Organización sin fines de lucro que promueve prácticas seguras en el desarrollo de software. Su guía **OWASP Top 10** es un estándar de facto para la identificación de vulnerabilidades críticas en aplicaciones web.

---

13. OWASP Top 10

Listado actualizado periódicamente que enumera las 10 principales amenazas de seguridad en aplicaciones web. Ejemplos incluyen: Broken Access Control, Injection, Insecure Design, y SSRF.

---

14. SSRF (Server-Side Request Forgery)

Vulnerabilidad que permite a un atacante hacer que un servidor realice solicitudes no autorizadas hacia recursos internos o externos, potencialmente accediendo a servicios protegidos.

---

15. DevSecOps

Práctica que integra la seguridad dentro del ciclo de vida de desarrollo de software (DevOps), promoviendo automatización en análisis de vulnerabilidades, pruebas, revisión de código y cumplimiento normativo.

---

16. Gestión de parches (Patch Management)

Proceso sistemático de aplicar actualizaciones de seguridad a sistemas, aplicaciones y dependencias para corregir vulnerabilidades conocidas y prevenir explotación.

---

17. Seguridad por diseño (Security by Design)

Enfoque que incorpora la seguridad como un principio fundamental desde las etapas iniciales del diseño del sistema, en lugar de agregarla como una capa posterior.

---

18. MFA (Multi-Factor Authentication)

Mecanismo de autenticación que requiere al menos dos factores distintos de verificación (algo que sabes, algo que tienes, algo que eres), para proteger accesos a sistemas sensibles.

---

19. Token CSRF

Valor aleatorio, único por sesión, incluido en formularios o peticiones para verificar que la acción fue iniciada desde un origen legítimo y no desde un sitio externo malicioso.

---

20. Seguridad en la nube (Cloud Security)

Conjunto de controles, prácticas y herramientas diseñadas para proteger datos, aplicaciones e infraestructura en entornos de computación en la nube, considerando el modelo de responsabilidad compartida.
