📘 Glosario: Vulnerabilidades en APIs RESTful

---

1. API RESTful

Interfaz de programación que permite la comunicación entre sistemas a través de peticiones HTTP utilizando principios del estilo arquitectónico REST (Representational State Transfer).

---

2. Endpoint

Ruta específica de una API a la que se puede acceder para realizar una operación (GET, POST, PUT, DELETE). Representa un recurso o acción.

---

3. Autenticación (Authentication)

Proceso que verifica la identidad de un usuario o aplicación. En APIs, suele implementarse mediante tokens, claves API o protocolos como OAuth.

---

4. Autorización (Authorization)

Proceso que determina si una entidad autenticada tiene permisos para realizar una acción o acceder a un recurso específico.

---

5. Broken Authentication

Vulnerabilidad en la cual un atacante puede suplantar a otro usuario debido a una gestión insegura de credenciales, tokens o sesiones.

---

6. Broken Authorization

Falla en la aplicación de controles de acceso que permite a usuarios acceder a recursos fuera de su alcance autorizado (escalamiento de privilegios).

---

7. Validación de Entradas

Mecanismo para asegurar que los datos ingresados por el usuario sean seguros, estén en el formato esperado y no contengan contenido malicioso.

---

8. SQL Injection (SQLi)

Tipo de ataque que permite modificar consultas a bases de datos mediante la inyección de código SQL malicioso a través de parámetros inseguros.

---

9. Cross-Site Scripting (XSS)

Vulnerabilidad que permite inyectar scripts maliciosos en una aplicación web, los cuales se ejecutan en el navegador de otros usuarios.

---

10. Command Injection

Ataque que consiste en insertar comandos del sistema operativo en una entrada de usuario mal filtrada para ejecutar instrucciones en el servidor.

---

11. Cabeceras HTTP (HTTP Headers)

Información adicional enviada en cada petición o respuesta HTTP que puede influir en aspectos como autenticación, seguridad, tipo de contenido, etc.

---

12. CORS (Cross-Origin Resource Sharing)

Política de seguridad que define qué dominios externos pueden realizar solicitudes a una API o aplicación web.

---

13. Token (JWT / Bearer Token)

Cadena de texto firmada que representa la identidad de un usuario y sus permisos. Se usa para autorizar accesos sin almacenar sesiones en el servidor.

---

14. OWASP ZAP

Herramienta de código abierto para análisis de seguridad en aplicaciones web. Permite escaneo automático, scripting y pruebas de fuzzing.

---

15. Burp Suite

Suite profesional de herramientas para pruebas de penetración en aplicaciones web. Incluye funcionalidades como interceptación, modificación de solicitudes, automatización de ataques, etc.

---

16. Postman

Plataforma para el desarrollo, prueba y documentación de APIs. Permite enviar solicitudes estructuradas y analizar respuestas de forma detallada.

---

17. RBAC (Role-Based Access Control)

Modelo de control de acceso en el que los permisos se asignan a roles, y los roles a usuarios, en lugar de asignaciones directas.

---

18. Content Security Policy (CSP)

Política de seguridad web que permite restringir las fuentes desde las cuales se pueden cargar scripts, estilos, imágenes y otros recursos.

---

19. Strict-Transport-Security (HSTS)

Cabecera HTTP que obliga al navegador a comunicarse únicamente mediante HTTPS con un servidor, incluso si el usuario intenta acceder por HTTP.

---

20. Fuzzing

Técnica automatizada de prueba que consiste en enviar grandes cantidades de entradas aleatorias o malformadas a una API para detectar fallos o vulnerabilidades.
