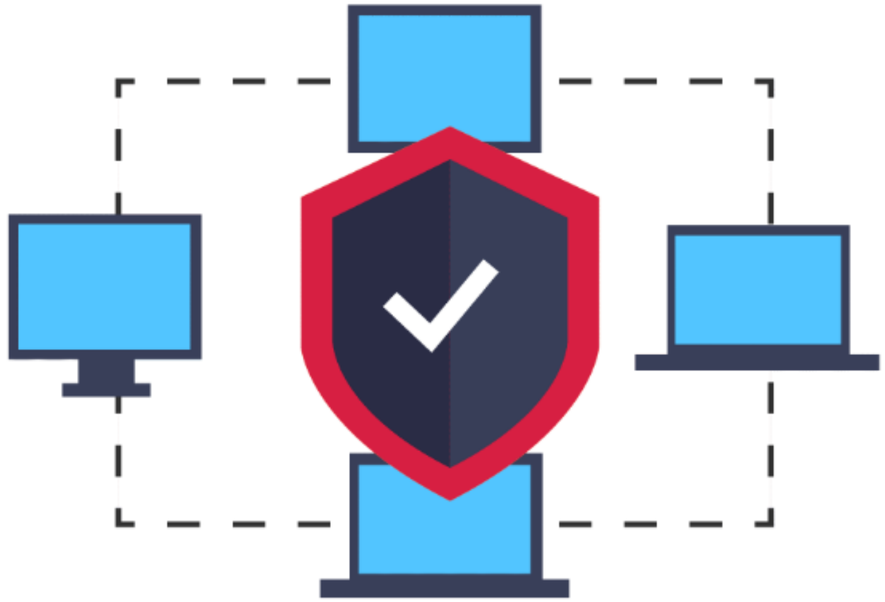
sustantiva
CON•SENTIDO

VULNERABILIDADES EN APIS RESTFUL

Objetivos de la Lección

Objetivos de la Lección

Las **APIs RESTful** son fundamentales en las arquitecturas modernas, pero también representan una **superficie de ataque crítica**. Esta lección busca identificar las **principales vulnerabilidades**, explorar **técnicas de explotación controlada** con herramientas profesionales y aplicar **estrategias de mitigación** alineadas con los estándares de **OWASP**.



APIs RESTful – Riesgos y Complejidad

Aunque su diseño se basa en protocolos simples como **HTTP**, y estructuras como **JSON** o **XML**, las APIs RESTful pueden ocultar una **complejidad de seguridad subestimada**. Cada punto de exposición mal protegido puede convertirse en un **vector de ataque**, haciendo de estas interfaces uno de los blancos más frecuentes en ciberseguridad moderna.

Vulnerabilidades Comunes en APIs

Vulnerabilidades Comunes en APIs

Las fallas más críticas en APIs RESTful incluyen:

- **Autenticación débil**, que permite ataques de fuerza bruta o **robo de credenciales**.
- **Autorización deficiente**, que habilita accesos indebidos (escalamiento de privilegios).
- **Validación laxa de entradas**, que expone al sistema a **inyecciones SQL, XSS o comandos**.
- **Cabeceras HTTP mal configuradas**, que permiten **ataques entre orígenes** o elusión de controles.

Explotación de Fallos Críticos

Explotación de Fallos Críticos

Los errores de **autenticación** como el mal manejo de tokens o sesiones pueden llevar a **suplantación de identidad**. Por otro lado, los fallos en la **autorización** permiten a usuarios acceder a datos o acciones fuera de su nivel de privilegio (**Vertical u Horizontal Privilege Escalation**), representando un riesgo grave de **filtración o modificación de información**.

Manipulación de Datos y Cabeceras

Manipulación de Datos y Cabeceras

La **falta de validación de entradas** convierte al sistema en ejecutor de instrucciones maliciosas (como **SQLi, XSS o command injection**). Además, la **manipulación de cabeceras HTTP** mediante tokens vulnerables, **CORS permisivo** o cookies sin flags de seguridad puede abrir puertas a **exfiltración de datos** o **acceso no autorizado** desde orígenes externos.

Herramientas Profesionales para

Herramientas Profesionales para Evaluación

- **Burp Suite** permite interceptar y manipular solicitudes, probar autenticación y validaciones.

- **OWASP ZAP,** herramienta libre, automatiza pruebas como fuzzing, modificación de cabeceras e inyecciones.

- **Postman** facilita el envío estructurado de peticiones y análisis de endpoints.

  ✅ Estas herramientas son esenciales para realizar **auditorías técnicas controladas** en APIs RESTful.

Diseño Seguro y Mitigación

Asegurar APIs RESTful requiere una **estrategia proactiva**:

- Validar entradas con **listas blancas**.
- Usar **OAuth 2.0** o **JWT** bien configurado.
- Aplicar **autorización basada en roles (RBAC)**.
- Configurar **cabeceras de seguridad** (HSTS, CSP, SameSite, HttpOnly).
- Restringir **CORS**.
- Integrar estas prácticas en el ciclo **DevSecOps**.

  ✅ La clave está en combinar **diseño seguro**, **pruebas regulares** y **mantenimiento constante**.


Energiza!