🛠️ Ejercicio Práctico

📌 **Título:** Auditoría de seguridad a una API RESTful mediante Burp Suite y Postman

---

🎯 Objetivo:

Simular una auditoría ética sobre una **API RESTful simulada**, con el propósito de identificar **fallas de control de acceso, validación de entradas y seguridad de tokens JWT**, utilizando **Postman para pruebas funcionales** y **Burp Suite para análisis interceptado y fuzzing**.

🧱 Escenario:

La API `http://localhost:3000/api` contiene los siguientes endpoints:

Método	Endpoint	Descripción
POST	/auth/login	Autenticación, retorna JWT
GET	/users/me	Perfil del usuario autenticado
GET	/users	Lista todos los usuarios (solo admin)
PUT	/users/:id/role	Cambia el rol de un usuario (solo admin)

Tienes un **JWT válido de un usuario estándar** y acceso a herramientas como **Postman y Burp Suite**.

✅ Parte 1 – Análisis funcional con Postman

1. Usa el endpoint `/auth/login` para autenticarte como usuario estándar.
2. Copia el token JWT recibido.
3. Realiza una solicitud `GET /users/me` con el token en la cabecera:
   `Authorization: Bearer <TOKEN>`
4. Verifica que el perfil del usuario se muestre correctamente.

✅ Parte 2 – Interceptar tráfico con Burp Suite

1. Configura tu navegador para usar el proxy local (`127.0.0.1:8080`).
2. Repite las solicitudes desde Postman o el navegador, pero redirige el tráfico por Burp.
3. Observa si puedes modificar el JWT manualmente (decodifica, edita el payload, vuelve a firmar si es posible).
4. Intenta modificar el rol a “admin” en el token y acceder a `GET /users`.

✅ Parte 3 – Validación de control de acceso

1. Sin cambiar el token, intenta realizar un `GET /users`.
2. ¿La API devuelve la lista completa o un error `403 Forbidden`?
3. Si lograste modificar el token, ¿puedes ahora cambiar el rol de otro usuario con `PUT /users/2/role`?

🧪 Criterios de Evaluación (máximo 10 puntos)

1. **Uso correcto de Postman para autenticación (2 pts)**
   El estudiante obtiene y usa adecuadamente el token para acceder a recursos protegidos.

2. **Configuración e interceptación con Burp Suite (2 pts)**
   El tráfico es interceptado con éxito y se analiza el contenido de las solicitudes JWT.

3. **Manipulación ética del JWT (1.5 pts)**
   El estudiante demuestra si es posible alterar el token, entendiendo los límites del control de acceso.

4. **Validación del control de privilegios (2 pts)**
   Se documenta correctamente si el sistema protege los endpoints con lógica adecuada.

5. **Registro profesional de hallazgos (1.5 pts)**
   Informe claro con evidencias (capturas, payloads), explicación de impacto y comportamiento de la API.

6. **Reflexión ética y de seguridad (1 pt)**
   Se destaca la importancia de validar los roles, proteger los tokens y aplicar principios seguros de autenticación.

📚 Recursos de Apoyo y Herramientas Recomendadas

🛡️ Herramientas de prueba

- **Postman – Pruebas funcionales de APIs.**
- **Burp Suite Community – Interceptación y manipulación de tráfico HTTP.**
- **JWT.io – Decodificación y análisis de JWT.**

📘 Documentación técnica y lecturas

- **OWASP API Security Top 10**
- **Autenticación y autorización con JWT**
- **Control de acceso inseguro – OWASP**

🗒️ Reflexión Final

> **“Los tokens JWT no solo son llaves de acceso, también son puntos críticos de seguridad. Evaluar su manipulación, validación y los controles de acceso asociados es clave para prevenir escaladas de privilegio y fugas de datos.”**
