🛠️ Ejercicio Práctico

📌 **Título:** Análisis de control de acceso y manipulación de tokens en una API RESTful simulada

---

🎯 Objetivo:

Simular una evaluación de seguridad sobre una API RESTful protegida por tokens JWT. El objetivo es identificar **fallos de autorización y exposición de datos**, así como comprobar si es posible **forjar o reutilizar tokens** para acceder a información restringida.

🧱 Escenario:

Una aplicación ofrece los siguientes endpoints protegidos con autenticación tipo **Bearer Token (JWT)**:

Método	Endpoint	Descripción
GET	/api/users/me	Retorna datos del usuario autenticado
GET	/api/users	Lista todos los usuarios (solo admin)
PUT	/api/users/:id/role	Modifica rol de un usuario (solo admin)

Se te proporciona un token JWT válido de un **usuario estándar**:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...

🧪 Actividades:

✅ Parte 1 – Acceso a información propia

1. Realiza una petición `GET /api/users/me` usando el token JWT.

2. Confirma que puedes ver tu propio perfil, sin errores.

✅ Parte 2 – Intento de escalamiento horizontal

3. Intenta acceder a `GET /api/users` con el mismo token.
    - ¿Recibes los datos de todos los usuarios?
    - ¿Obtienes un error 403 o la respuesta completa?

✅ Parte 3 – Manipulación del token JWT

4. Decodifica el JWT usando jwt.io y modifica el campo `"role": "user"` a `"role": "admin"`.
5. Firma el token modificado con la misma clave secreta si es conocida (ej: `"secret"`).
6. Intenta ahora ejecutar `PUT /api/users/2/role` con el token modificado.

✅ Parte 4 – Análisis de cabeceras de seguridad

7. Revisa las cabeceras de respuesta del servidor:
    - ¿Se incluye `Cache-Control`, `Content-Security-Policy`, `Strict-Transport-Security`?
    - ¿Se exponen tokens, cookies o metadatos innecesarios?

📋 Entregables esperados:

1. Captura de las peticiones y respuestas observadas.
2. Resultados obtenidos en cada prueba.

3. Identificación de posibles vulnerabilidades:
    - Falta de verificación de firma
    - Acceso indebido
    - Cabeceras inseguras
4. Recomendaciones de mitigación para cada hallazgo.

🧠 Preguntas de reflexión:

- ¿Qué riesgos implica aceptar tokens JWT sin verificar su firma?
- ¿Por qué el control de roles debe hacerse del lado del servidor y no del cliente?
- ¿Qué tipo de cabeceras deberían incluirse para proteger las respuestas de una API?
