



## Ejercicio 1 (Portafolio): Identificación de Vulnerabilidades


### Actividad: Exposición y decodificación del token JWT en OWASP Juice Shop

---

Según lo visto en la **Lección 1**, ya hemos aprendido cómo activar la aplicación vulnerable **OWASP Juice Shop** utilizando **Docker** con una imagen virtual. Ahora, aprovecharemos esa instalación para realizar el siguiente análisis de seguridad:

#### Instrucciones del ejercicio:

1. **Abriremos la aplicación vulnerable OWASP Juice Shop** en el navegador:  
 <http://localhost:3000/#/>
2. **Iniciaremos sesión** con una cuenta válida (puedes crear una o usar la de prueba):
  - Email: [admin@juice-sh.op](mailto:admin@juice-sh.op)
  - Password: [admin123](#)
3. Luego, **inspeccionaremos el almacenamiento local (localStorage)** del navegador para encontrar el token JWT:
  - Presiona **F12** o clic derecho → "Inspeccionar"
  - Ve a la pestaña "**Application**" (o "Almacenamiento")
  - En el menú izquierdo, selecciona "**Local Storage**" → <http://localhost:3000>
  - Busca la clave llamada **token**
4. **Copia el valor completo** de ese token JWT.

5. Abre el sitio web  <https://jwt.io>
  6. **Pega el token en el campo izquierdo** del sitio para **decodificarlo automáticamente**.
  7. Analiza su contenido: ¿qué información contiene? (Ej: usuario, email, rol, etc.)
- 

### **Formato de documento para el portafolio (sugerido)**

Elemento	Descripción
Vulnerabilidad Identificada	Token JWT almacenado en <code>localStorage</code>
Tipo	Exposición de credenciales / sesión
Riesgo Estimado	Alto (susceptible a XSS → robo de token)
Evidencia	Captura de <code>localStorage</code> mostrando el token
Contenido del JWT	Decodificado en <a href="https://jwt.io">jwt.io</a> (incluir captura o transcripción)
Recomendación de mitigación	Usar cookies <code>httpOnly</code> , restringir acceso desde JavaScript

---

### **Reflexión técnica (opcional):**

- ¿Qué implicaciones de seguridad tiene exponer un token en el frontend?
  - ¿Cómo podría un atacante explotar esta vulnerabilidad con un XSS?
  - ¿Qué buenas prácticas se recomiendan para manejar sesiones seguras?
-



## Instrumento de Evaluación – Ejercicio Práctico

Identificación de Vulnerabilidades – Exposición del token JWT (OWASP Juice Shop)

Puntaje total: 10 puntos

Nota mínima para aprobar: 6 puntos

Criterio Evaluado	Puntaje
Acceso correcto a OWASP Juice Shop en el navegador (desde Docker)	1 pt
Inicio de sesión exitoso con credenciales válidas	1 pt
Identificación y copia del token JWT desde <code>localStorage</code>	2 pts
Decodificación correcta del token en <a href="https://jwt.io">https://jwt.io</a>	2 pts
Documentación clara del riesgo y tipo de vulnerabilidad	2 pts
Recomendación adecuada para mitigar el problema (cookies httpOnly, etc.)	1 pt
Reflexión técnica clara y fundamentada (mínimo 1 respuesta bien argumentada)	1 pt

---