Informe de exposición y decodificación de token JWT

– OWASP Juice-Shop web app

Título del informe: Informe de Reconocimiento Pasivo – OWASP Juice-Shop web app	
Portafolio: Lección 4: Informe de exposición y decodificación de token JWT.	Entorno: Imagen de OWASP Juice-Shop levantada con Docker Compose.
Clasificación del documento: Estudio de información pública y decodificación de información sensible.	Modulo: Análisis de Amenazas y Vulnerabilidades en Aplicaciones Web
Autor(es): Sebastián Hernández Téllez	Fecha de elaboración: 23 de agosto de 2025

---

1. Resumen Ejecutivo

El presente informe documenta el análisis de seguridad realizado sobre la aplicación **OWASP Juice-Shop**, desplegada en un entorno controlado mediante Docker Compose. El objetivo fue identificar vulnerabilidades relacionadas con la gestión de autenticación, almacenamiento de tokens y exposición de información sensible.

Principales hallazgos

- **VULN-01 – Token JWT almacenado en localStorage:** Se identificó que la aplicación almacena el token de autenticación JWT en localStorage. Este enfoque supone un riesgo crítico, ya que el token puede ser robado mediante ataques de Cross-Site Scripting (XSS) o mediante el acceso local al navegador. La decodificación del token evidenció información sensible de usuarios y credenciales de autenticación que podrían ser explotadas por un atacante en un entorno real.

- **Riesgo principal*:*** secuestro de sesión y suplantación de identidad, que en un contexto de e-commerce podría permitir accesos no autorizados a información de clientes,

manipulación de datos de pedidos y escalamiento de privilegios si el token pertenece a un administrador.

Recomendaciones clave

1. Migrar el almacenamiento de tokens a cookies seguras con atributos HttpOnly, Secure y SameSite.
2. Reducir el tiempo de vida (TTL) de los tokens y aplicar mecanismos de rotación y revocación.
3. Implementar cabeceras de seguridad (CSP, HSTS, X-Frame-Options) para reducir la superficie de ataque.
4. Fortalecer el ciclo de desarrollo seguro (SSDLC) aplicando OWASP ASVS y controles de sesión recomendados por NIST 800-53 e ISO 27001.

Nivel de riesgo general

El nivel de riesgo global de los hallazgos se clasifica como **Alto**, debido a la **alta probabilidad de explotación** y al **impacto crítico** que tendría la exposición de tokens JWT en un entorno de producción.

---

2. Alcance de la Evaluación

El presente análisis tuvo como finalidad identificar vulnerabilidades relacionadas con la gestión de sesiones y exposición de información sensible dentro de la aplicación OWASP Juice Shop v18.0.0, desplegada en un entorno controlado mediante contenedores Docker.

Tipo de aplicación evaluada

- Aplicación de e-commerce intencionalmente vulnerable, orientada a la práctica de pruebas de seguridad.

Entorno evaluado

- Imagen oficial de OWASP Juice Shop desplegada mediante Docker Compose.
- Acceso a la aplicación a través del puerto 3000/TCP desde navegador web (Google Chrome).

Objetivos específicos

- Verificar cómo la aplicación gestiona los tokens de autenticación (JWT).
- Identificar riesgos asociados al almacenamiento de credenciales y tokens en el cliente.
- Evaluar la exposición de información sensible mediante la decodificación de tokens.
- Clasificar los hallazgos conforme a OWASP Top 10, NIST SP 800-53 e ISO/IEC 27001.

Exclusiones / Limitaciones

- No se realizaron pruebas de explotación activas sobre XSS ni inyecciones SQL.
- No se descifraron contraseñas ni credenciales contenidas en los tokens.
- El análisis se restringió únicamente a técnicas de reconocimiento pasivo y decodificación de información pública.

---

4. Metodología

La evaluación de seguridad se realizó bajo un enfoque de análisis de amenazas y vulnerabilidades en aplicaciones web, aplicando metodologías reconocidas internacionalmente para garantizar la validez de los hallazgos.

Estándares y marcos utilizados

- OWASP Testing Guide v4: para la identificación de vulnerabilidades comunes en aplicaciones web.
- OWASP Top 10 – 2021: referencia principal para la clasificación de los hallazgos.
- OWASP ASVS (Application Security Verification Standard): lineamientos para verificar el correcto manejo de sesiones y tokens.
- NIST SP 800-53 (Rev. 5): controles relacionados con gestión de identidad, autenticación y sesiones.
- ISO/IEC 27001:2022 – Anexo A: controles relacionados con la protección de la información sensible y gestión de accesos.

Técnicas aplicadas

- Reconocimiento pasivo: análisis de la aplicación sin explotación activa, identificando recursos públicos y comportamiento del cliente.
- Inspección del almacenamiento del navegador: verificación del uso de localStorage y sessionStorage.
- Decodificación de JWT: extracción de información sensible contenida en el token a través de herramientas públicas (jwt.io).
- Análisis de configuración de sesión: revisión del tiempo de vida de tokens y ausencia de mecanismos de rotación/revocación

Herramientas utilizadas

- Docker + Docker Compose: despliegue controlado del entorno vulnerable (OWASP Juice Shop).
- Navegador web (Google Chrome): exploración de la aplicación y uso de herramientas de desarrollador para la inspección de almacenamiento local.
- jwt.io: decodificación de los tokens JWT expuestos.
- Documentación OWASP Juice Shop: referencia técnica para comprender el funcionamiento del entorno evaluado.

---

5. Enfoque de la evaluación

1. **Preparación del entorno**: despliegue de la aplicación vulnerable en un contenedor Docker.

2. **Acceso inicial**: autenticación con credenciales por defecto.

3. **Revisión de almacenamiento en cliente**: identificación de tokens persistidos en localStorage.

4. **Decodificación de información sensible**: análisis de la data contenida en el JWT expuesto.

5. **Clasificación de hallazgos**: mapeo contra OWASP Top 10, NIST e ISO 27001.

6. **Evaluación del riesgo**: determinación de probabilidad e impacto, generando la matriz de riesgo.

7. **Recomendaciones de mitigación**: propuestas alineadas con buenas prácticas internacionales y controles de seguridad reconocidos.

---

6. Hallazgos de Seguridad

6.1 VULN-01: Token JWT almacenado en localStorage

1. Identificador: VULN-01

2. Descripción: La aplicación almacena el token JWT en localStorage. Esta práctica expone el token a posibles ataques de **Cross-Site Scripting (XSS)**, permitiendo que un atacante ejecute código malicioso en el navegador y extraiga el token de sesión. Una vez obtenido, el atacante puede hacerse pasar por el usuario legítimo sin necesidad de conocer sus credenciales.

3. Clasificación: OWASP Top 10 – *A07:2021 Identification and Authentication Failures* y *A03:2021 Injection (XSS)*.

4. Impacto potencial:

- **Secuestro de sesión**: uso indebido de credenciales para acceder con privilegios elevados.
- **Exposición de datos sensibles**: acceso a información personal, financiera o de clientes.
- **Escalada de privilegios**: si el token pertenece a un usuario administrador, el atacante podría tomar control total de la aplicación.
- **Persistencia de ataque**: tokens comprometidos pueden reutilizarse mientras sigan siendo válidos, incluso desde ubicaciones distintas.

5. Evidencia técnica:

Fotografias de anexo A-F

6. Reproducción paso a paso:

1. Levantamiento de imagen de OWASP Juice Shop por medio de Docker Compose.
2. Ingreso a la aplicación por medio del puerto 3000 desde el navegador web.
3. Inicio de sesión por medio de credenciales por defecto.
4. Exploración visual de la aplicación a través del modo inspección.

5. Decodificación de token expuesto.

6. Obtención de información sensible.

7. Recomendación de mitigación:

- Almacenar tokens únicamente en **cookies seguras con atributos HttpOnly y Secure**, para evitar acceso por JavaScript y transmisión insegura.
- Configurar **SameSite=strict** en cookies para prevenir *Cross-Site Request Forgery (CSRF)*.
- Implementar **rotación periódica de tokens** y **revocación inmediata** en caso de compromiso.
- Reducir el tiempo de vida (TTL) de los tokens para limitar la ventana de explotación.
- Monitorear y alertar accesos sospechosos a cuentas (NIST SP 800-53 – *Audit and Accountability*).

8. Nivel de riesgo: Alto (Probabilidad: Alta, Impacto: Alto).

---

7. Evaluación de Riesgos

7.1 Matriz de Riesgo

Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Recomendación Prioritaria
VULN-01 – Exposición de JWT en localStorage	Alta	Alta	Crítico	Migrar tokens a cookies seguras con HttpOnly y Secure; implementar rotación y expiración temprana.

7.2 Resumen por Categoría OWASP

Categoría OWASP	Vulnerabilidades Detectadas	Severidad Promedio
A07:2021 Identification and Authentication Failures	JWT en localStorage	Crítico

---

8. Recomendaciones Generales

1. Aplicar OWASP ASVS (Application Security Verification Standard) nivel 2 para aplicaciones con autenticación sensible.
2. Adoptar controles de NIST 800-53 (IA-2, SC-23, AC-7) sobre gestión de sesiones y autenticación.
3. Implementar un Ciclo de Vida de Desarrollo Seguro (SSDLC) que contemple revisiones de seguridad en cada fase.
4. Fortalecer las cabeceras de seguridad HTTP (Content-Security-Policy, X-Frame-Options, Strict-Transport-Security).
5. Monitorear continuamente la seguridad de la aplicación mediante pruebas DAST/SAST.

---

9. Conclusiones

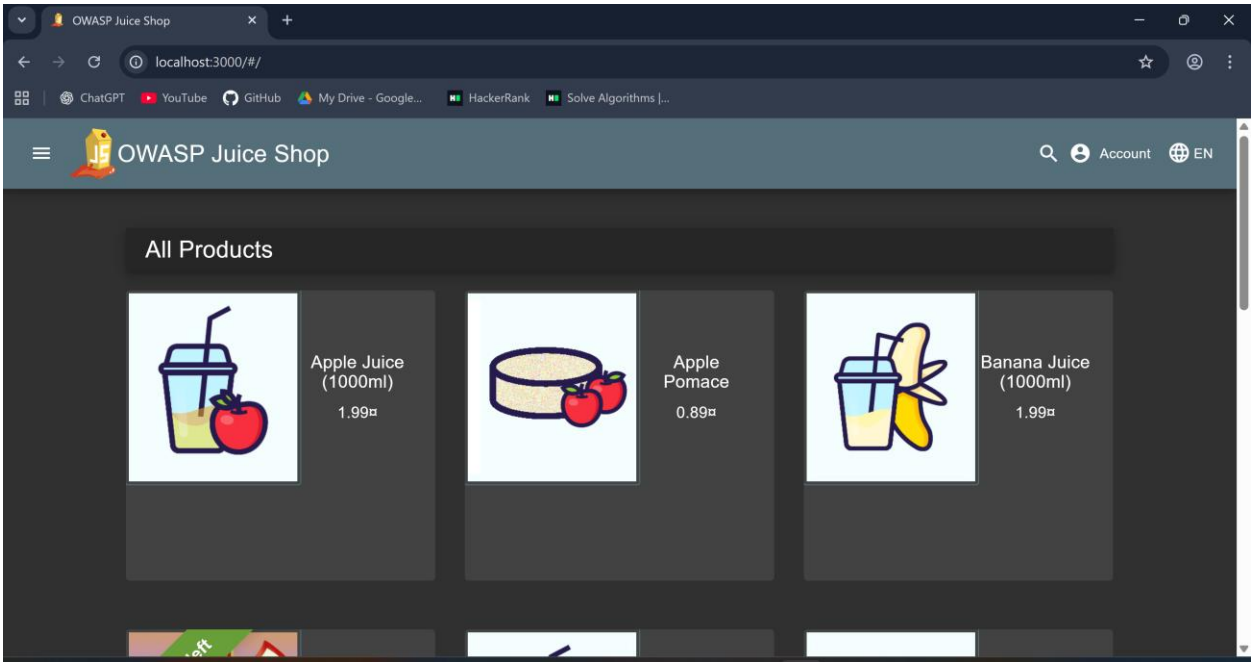
El almacenamiento de tokens JWT en localStorage representa un riesgo crítico en escenarios reales. En caso de explotación, un atacante podría tomar control de sesiones legítimas, acceder a información sensible de usuarios y escalar privilegios. Esta vulnerabilidad es especialmente peligrosa en aplicaciones de e-commerce, banca en línea o cualquier entorno donde se procesen datos personales o financieros.

La mitigación debe priorizarse con migración de tokens a cookies seguras, reducción de TTL, monitoreo de actividad sospechosa y aplicación de controles de sesión conforme a OWASP, NIST e ISO 27001.

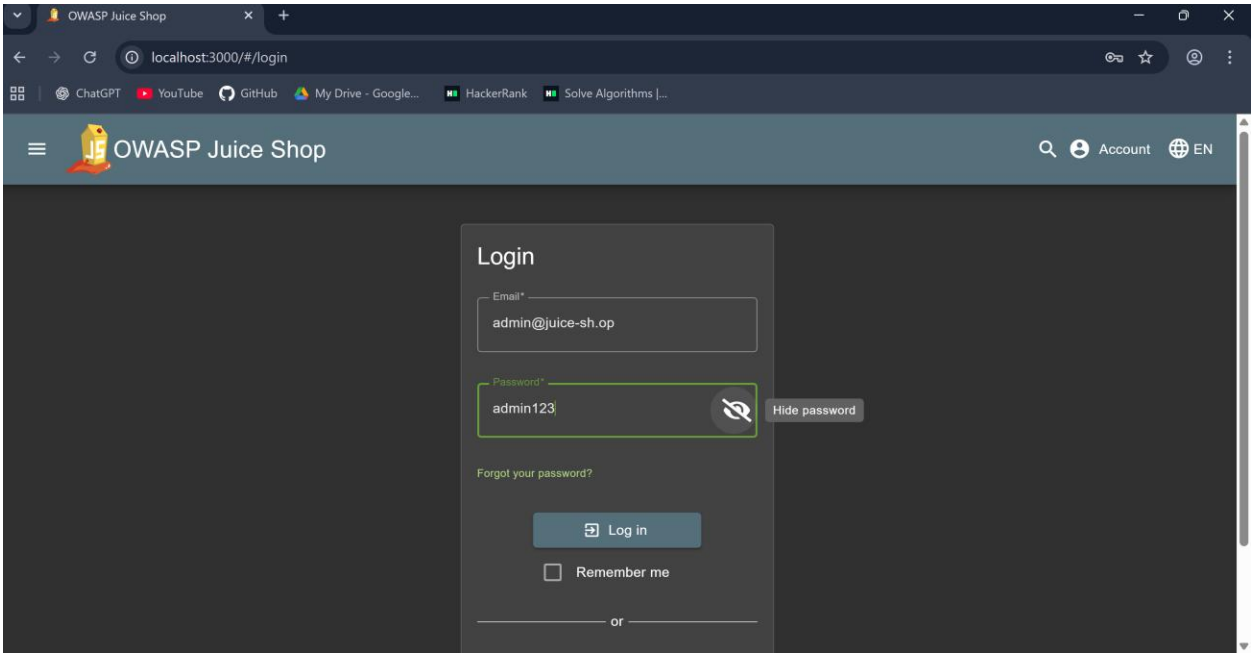
---

10. Anexos

Anexo A – Acceso a OWASP Juice-Shop a través de puerto 3000



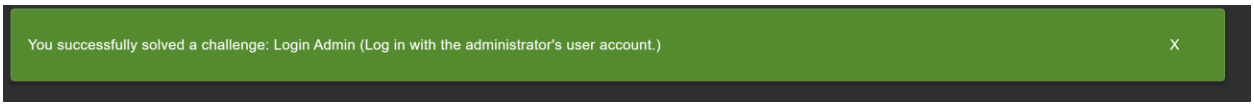
Anexo B– Acceso con credenciales por defecto



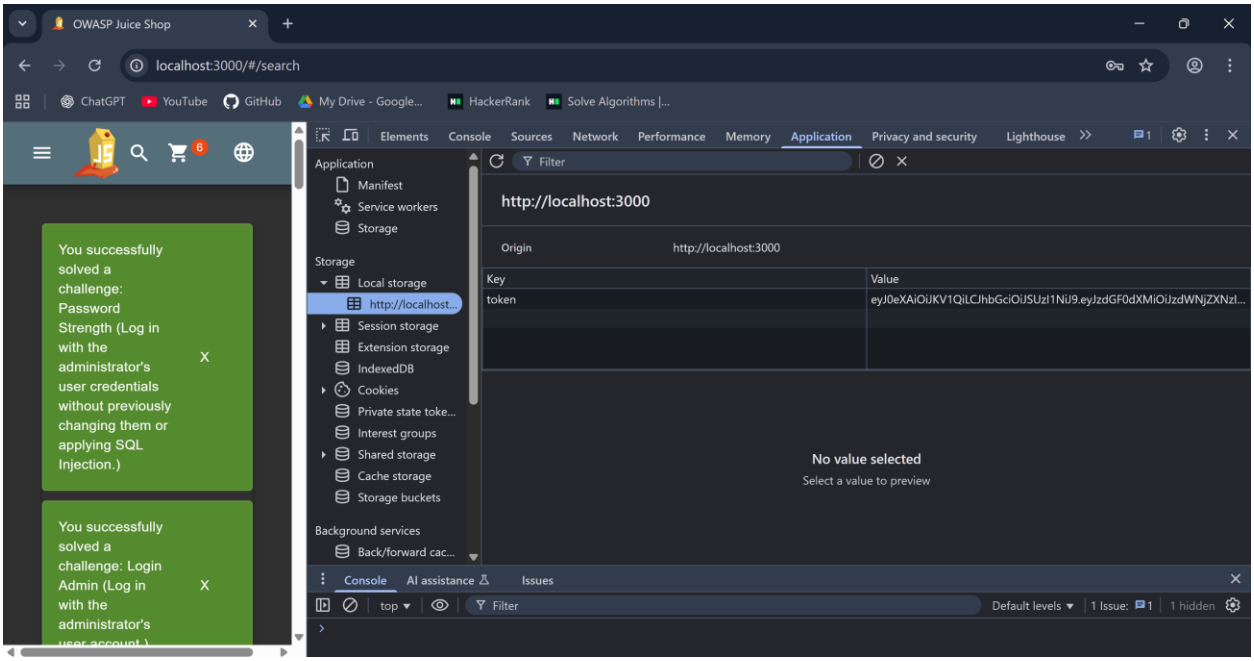
Credenciales:

- Email: admin@juice-sh.op

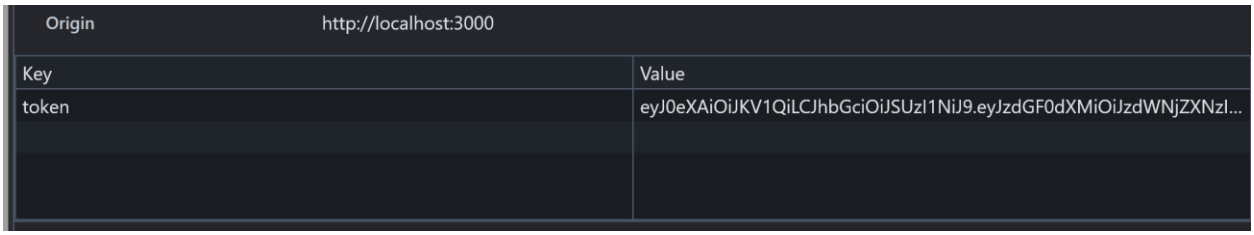
- Clave: admin123



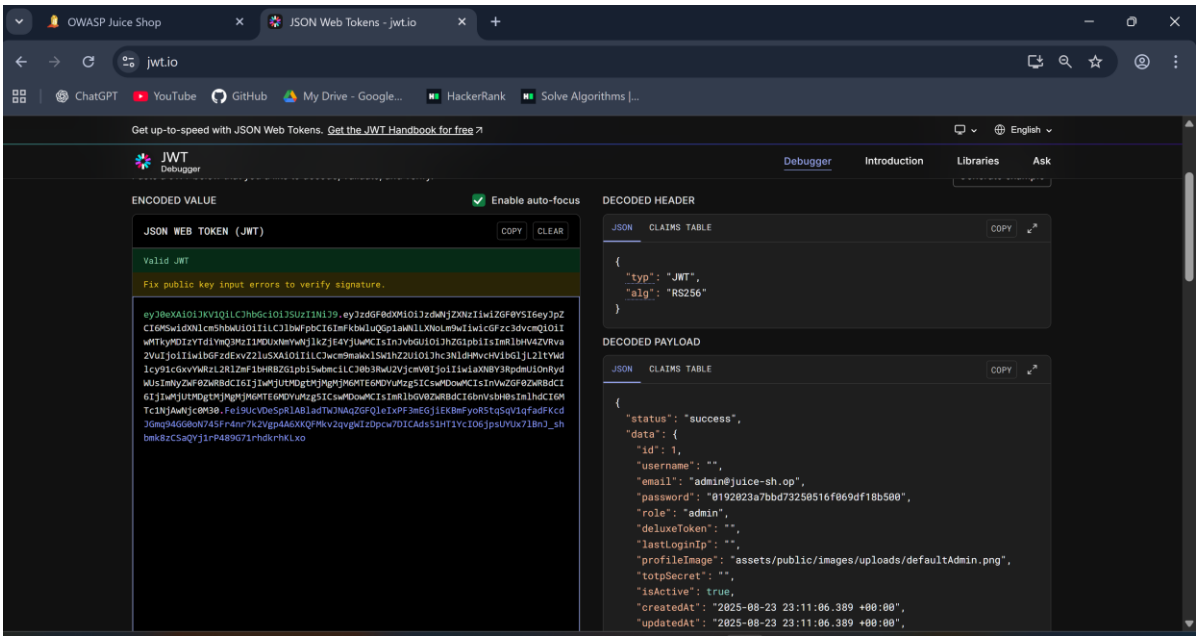
Anexo C – Inspección de Local Storage



Anexo D – token visible en LocalStorage



Anexo E – decodificación del token por medio de jwt.io



Anexo F – exposición de información sensible