Blandskron

Informe de Identificación de Vulnerabilidades – OWASP Juice Shop

Fecha: 11 de junio de 2025

---

1. Alcance y Objetivos

Este informe documenta la identificación de una vulnerabilidad crítica en OWASP Juice Shop, aplicación web desplegada en el puerto 3000. Su propósito es evaluar el riesgo, aportar evidencia y proponer controles alineados con ISO/IEC 27001:2022 para garantizar la confidencialidad e integridad de las credenciales de sesión.

2. Metodología

1. **Reconocimiento**
    - Inspección de almacenamiento local en navegador (Developer Tools → Application → Local Storage).
2. **Análisis de la vulnerabilidad**
    - Lectura del valor almacenado en `localStorage.token`.
    - Decodificación del JWT mediante herramientas online o librerías (`atob`, `jwt.io`).
3. **Evaluación de riesgo**
    - Impacto sobre la confidencialidad de la sesión.
    - Probabilidad de explotación mediante ataques XSS.

3. Hallazgo

- **Vulnerabilidad:** Almacenamiento del token JWT en `localStorage`.
- **Descripción:** El token de autenticación (`JWT`) con rol de administrador queda accesible para JavaScript. Un atacante que inyecte código malicioso (XSS) puede sustraerlo y suplantar la sesión.
- **Tipo:** Exposición de credenciales / Takeover de sesión.
- **Nivel de riesgo:** Alto

4. Evaluación de riesgos (ISO 27005)

Parámetro	Valor	Justificación
Impacto	Alto	Acceso total a funciones administrativas.
Probabilidad	Media–Alta	XSS es común en aplicaciones web complejas.
Nivel de riesgo	Alto	Conjunción de impacto severo y facilidad de explotación.

5. Controles y recomendaciones (Annex A ISO/IEC 27001)

Control	Descripción	Acción recomendada
A.9: Control de acceso	Garantizar acceso restringido a funciones sensibles.	Almacenar el JWT en **cookie** con flags `HttpOnly` y `Secure` (A.10.1.2), evitando que JavaScript acceda al token.
A.10: Criptografía	Uso de técnicas criptográficas para proteger la información.	Firmar tokens con algoritmo robusto (RS256), implementar expiración corta y **refresh tokens** gestionados en servidor.
A.12.2: Seguridad de operaciones	Proteger la aplicación frente a malware y scripts no autorizados.	Definir una **Content Security Policy** (CSP) estricta para bloquear ejecución de código no confiable (A.14.2).
A.14: Seguridad en el desarrollo	Integrar seguridad en el ciclo de vida de desarrollo.	Emplear validación y saneado de todas las entradas para prevenir XSS. Realizar **revisiones de código** periódicas.

A.18.2: Cumplimiento técnico	Revisar que las medidas técnicas cumplen la política de seguridad.	Programar auditorías trimestrales de dependencias y configuraciones de almacenamiento de tokens.

6. Evidencia

Local Storage

Key: token

Value: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9…

-

JWT decodificado


```
{
  "status": "success",
  "data": {
    "id": 1,
    "email": "admin@juice-sh.op",
    "role": "admin",
    "isActive": true,
    "createdAt": "2025-06-08T18:38:31.736Z"
  },
  "iat": 1749409956
}
```


-

7. Conclusiones

El almacenamiento de JWT en `localStorage` contraviene las buenas prácticas de gestión de sesiones y genera un riesgo alto de secuestro de cuenta administrativa ante un XSS. La implementación de cookies seguras, CSP y revisión de código apunta directamente a los controles de ISO/IEC 27001, reduciendo sustancialmente el riesgo y alineándose con un Sistema de Gestión de Seguridad de la Información (SGSI) maduro.