🛠️ Ejercicio Práctico

📌 Título: *Exploración de vulnerabilidades web con OWASP Juice Shop*

🎯 Objetivo del ejercicio:

Familiarizarte con el uso de herramientas de seguridad web a través de la **exploración de vulnerabilidades** en una aplicación web vulnerable. Aprenderás a identificar problemas de seguridad comunes y cómo mitigarlos.

📝 Escenario:

Tienes acceso a una aplicación web vulnerable llamada **OWASP Juice Shop**, diseñada específicamente para enseñar sobre seguridad en aplicaciones web. Tu tarea es explorar y encontrar al menos **3 vulnerabilidades** de seguridad en la aplicación, comprender cómo afectan a la seguridad de la aplicación y, en algunos casos, cómo podrían explotarse.

OWASP Juice Shop es un entorno seguro donde los usuarios pueden **practicar** técnicas de pruebas de penetración y **mejorar sus habilidades de seguridad**.

🔍 Tu tarea:

Paso 1 – Acceso a la Aplicación:

1. **Inicia OWASP Juice Shop** en tu máquina local o en un entorno controlado.
   Puedes descargarla e instalarla desde su página oficial, o utilizar su versión en línea disponible en su entorno demo.

Paso 2 – Identificar Vulnerabilidades Comunes:

1. Navega por la aplicación e intenta realizar las siguientes actividades:

- Realiza una **inyección SQL** en el formulario de búsqueda (si está permitido).
- Explora cualquier posible **vulnerabilidad de XSS (Cross-Site Scripting)** al insertar código malicioso en los formularios.
- Identifica cualquier **exposición de información sensible** como contraseñas o tokens en la interfaz de usuario o en las solicitudes de red.

Paso 3 – Documentar las Vulnerabilidades:

1. **Describe las vulnerabilidades** encontradas, explicando qué tipo de vulnerabilidad es, cómo puede ser explotada por un atacante y cuál es el impacto en la aplicación.
    - Ejemplo: "La **inyección SQL** permite a un atacante manipular las consultas a la base de datos para obtener información confidencial."
2. **Anota las soluciones** recomendadas para cada vulnerabilidad. Por ejemplo, si encontraste una vulnerabilidad de XSS, la solución podría ser la validación y escape de las entradas de los usuarios.

Paso 4 – Pruebas de Seguridad:

1. Realiza una **prueba de penetración básica** utilizando herramientas como:
    - **OWASP ZAP** para escanear la aplicación en busca de vulnerabilidades conocidas.
    - **Burp Suite** para interceptar y modificar solicitudes HTTP.

✅ Resultado esperado:

- **Vulnerabilidades identificadas**: Como mínimo, debes encontrar 3 vulnerabilidades diferentes.
- **Análisis de impacto**: Explica cómo una vulnerabilidad podría ser explotada por un atacante.
- **Soluciones recomendadas**: Describe las mejores prácticas y medidas para mitigar cada vulnerabilidad identificada.
- **Uso de herramientas de seguridad**: Debes haber utilizado herramientas como OWASP ZAP o Burp Suite para probar y validar las vulnerabilidades.

📄 Entrega sugerida:

- Capturas de pantalla de las vulnerabilidades encontradas en la aplicación (por ejemplo, inyección SQL, XSS).
- Documentación sobre cada vulnerabilidad y la recomendación de solución.
- Resultados de las pruebas realizadas con herramientas como OWASP ZAP o Burp Suite.

🧰 Herramientas recomendadas (opcional):

- **OWASP Juice Shop**
- **OWASP ZAP**
- **Burp Suite** (versión gratuita)
- **Google Chrome Developer Tools** (para inspeccionar las solicitudes y respuestas HTTP)
