Blandskron

Informe de Laboratorio

Ejercicio 2: Clasificación y Ética de Ciberatacantes
Fecha: 5 de junio de 2025
Herramienta utilizada: OWASP Juice Shop (vía Docker)

Parte 1: Implementación del entorno vulnerable

Se desplegó el entorno vulnerable OWASP Juice Shop utilizando Docker Compose.
El archivo `docker-compose.yml` se configuró con el siguiente contenido:

```
version: "3.8"

services:
  juice-shop:
    image: bkimminich/juice-shop
    container_name: juice-shop
    ports:
      - "3000:3000"
    restart: unless-stopped
```

El entorno fue iniciado correctamente con el comando:

```
docker-compose up -d
```

Posteriormente, se accedió a la aplicación mediante el navegador en http://localhost:3000.

Parte 2: Acceso por credenciales por defecto

Se realizó un intento de acceso con credenciales conocidas, comunes en entornos inseguros:

- **Intento 1:**
  Email: `admin@juice-sh.op`
  Contraseña: `admin123`
  → Resultado: acceso exitoso.

- **Intento 2:**
  Email: `jim@juice-sh.op`
  Contraseña: `ncc-1701`
  → Resultado: acceso exitoso.

Análisis:
La aplicación permite iniciar sesión con credenciales predecibles, lo cual evidencia una configuración insegura sin verificación de contraseñas fuertes ni monitoreo de accesos sospechosos. Esto es una práctica comúnmente explotada por atacantes de tipo **Black Hat**.

Parte 3: Prueba de inyección SQL en el login

Se realizó una prueba de inyección SQL básica en el campo de email con los siguientes datos:

- Email: `' OR 1=1--`
  Contraseña: cualquier valor
  → Resultado: acceso no autorizado exitoso.

- Email: `' OR '1'='1`
  Contraseña: anything
  → Resultado: acceso no autorizado exitoso.

Análisis:
Se comprobó que la aplicación es vulnerable a inyecciones SQL, lo cual demuestra que no existe sanitización ni validación adecuada de entradas. Esta vulnerabilidad crítica puede permitir a un atacante acceder sin necesidad de credenciales válidas, comprometiendo totalmente la integridad del sistema.

Clasificación del tipo de ciberatacantes

Tipo de Ciberatacante	Características	Aplicación en el ejercicio
Black Hat	Usa técnicas maliciosas para beneficio propio, sin consentimiento	Usaría las credenciales por defecto o la inyección SQL para acceder y explotar el sistema
White Hat	Hacker ético que reporta vulnerabilidades con fines de mejora	Utiliza las mismas técnicas pero reporta la falla al equipo de seguridad
Gray Hat	Puede explotar sistemas sin intención maliciosa pero sin autorización previa	Podría acceder con fines de exploración sin dañar, pero sin consentimiento del propietario

Medidas recomendadas para mitigar los riesgos

1. Forzar el cambio de contraseñas por defecto al primer inicio de sesión.
2. Implementar políticas de contraseñas seguras y autenticación multifactor.
3. Añadir validación y sanitización de todos los datos ingresados por el usuario.
4. Utilizar sentencias preparadas (prepared statements) para proteger contra inyecciones SQL.
5. Monitorear accesos y registrar intentos fallidos de inicio de sesión.
6. Realizar auditorías periódicas de seguridad sobre las rutas de autenticación.

Reflexión Final

Este laboratorio permitió observar que las mismas herramientas técnicas pueden ser utilizadas tanto para proteger como para atacar un sistema, dependiendo del enfoque ético del individuo que las utiliza. Acceder con credenciales débiles o explotar una inyección SQL es trivial en entornos mal configurados, como lo demuestra OWASP Juice Shop. Sin embargo, lo relevante no es el acceso, sino la intención detrás de ello.

Un **hacker de sombrero negro** aprovecharía estas vulnerabilidades para robar datos, manipular información o escalar privilegios. En cambio, un **hacker ético** reportaría estos fallos y ayudaría a reforzar la seguridad del sistema antes de que sean explotados.

Aplicar medidas preventivas adecuadas no solo protege la información, sino también la reputación de la organización. Este ejercicio refuerza la idea de que la ética es una parte inseparable de la ciberseguridad profesional.