TEC | Tecnológico de Costa Rica

1. Crear la Máquina Virtual (VirtualBox)

Antes de instalar Juice Shop, necesitarás una máquina virtual con un sistema operativo Linux.

1. **Descarga e Instalación de VirtualBox:**
   - Descarga la última versión de **Oracle VM VirtualBox** y el **Extension Pack** desde el sitio web oficial.
   - Instala VirtualBox en tu sistema operativo anfitrión (Windows, macOS o Linux).
2. **Descarga de la Imagen ISO de Linux:**
   - Descarga la imagen **ISO** de la distribución Linux que prefieras (por ejemplo, Ubuntu Desktop LTS o Kali Linux).
3. **Creación de la MV:**
   - Abre VirtualBox y haz clic en **"Nueva"** (o `Ctrl+N`).
   - **Nombre y Sistema Operativo:**
     - **Nombre:** Asigna un nombre (ej: `JuiceShop-Linux`).
     - **Tipo:** `Linux`.
     - **Versión:** Elige la versión específica de tu ISO (ej: `Ubuntu (64-bit)`).
   - **Memoria RAM:**
     - Asigna al menos **2048 MB (2 GB)** de RAM. Si tu equipo lo permite, 4 GB es mejor.
   - **Disco Duro:**
     - Selecciona **"Crear un disco duro virtual ahora"**.
     - **Tipo de archivo de disco duro:** Elige **VDI** (VirtualBox Disk Image).
     - **Almacenamiento en unidad de disco duro física:** Selecciona **"Reservado dinámicamente"** para que el archivo crezca según se necesite (recomendado).
     - **Ubicación y tamaño:** Asigna un tamaño de disco duro de al menos **20 GB** (para Linux y Docker).
   - Haz clic en **"Crear"**.
4. **Configuración de la MV:**
   - Selecciona la MV recién creada y haz clic en **"Configuración"**.
   - **Sistema > Procesador:** Asigna al menos **2 CPUs** (si tu máquina física tiene suficientes núcleos).
   - **Almacenamiento:**
     - En el controlador **IDE/SATA**, selecciona el disco óptico (vacío) y haz clic en el icono del disco para **"Seleccionar un archivo de disco"** y elige la imagen ISO de Linux que descargaste.
   - **Red:**

- Para empezar, deja el **Adaptador 1** en modo **NAT** (por defecto), lo que permitirá que la MV acceda a Internet.

2. Instalación del Sistema Operativo Linux

1. **Iniciar la MV:**
   - Inicia la máquina virtual. El proceso debería arrancar desde la imagen ISO.
2. **Instalar Linux:**
   - Sigue las instrucciones en pantalla para instalar el sistema operativo. Esto incluirá seleccionar el idioma, la distribución del teclado, crear tu usuario y contraseña, y formatear el disco virtual.
3. **Primeros Pasos en Linux:**
   - Una vez terminada la instalación, retira la ISO (o VirtualBox te lo pedirá) y reinicia la MV.
   - Abre una terminal. Es fundamental que el sistema esté actualizado:

     Bash

     ```
     sudo apt update
     sudo apt upgrade -y
     ```

3. Instalación y Configuración de OWASP Juice Shop con Docker

La forma más sencilla y recomendada de ejecutar Juice Shop es usando **Docker**.

A. Instalar Docker en Linux

1. **Instalar paquetes necesarios:**

   Bash

   ```
   sudo apt install apt-transport-https ca-certificates curl
   software-properties-common -y
   ```

2. **Agregar la clave GPG oficial de Docker:**

   Bash

   ```
   curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo
   gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
   ```

(Si usas una distribución diferente a Ubuntu, verifica la URL correcta en la documentación de Docker.)

3. **Configurar el repositorio estable de Docker:**

   Bash

   ```
   echo "deb [arch=$(dpkg --print-architecture) signed-
   by=/usr/share/keyrings/docker-archive-keyring.gpg]
   https://download.docker.com/linux/ubuntu $(lsb_release -cs)
   stable" | sudo tee /etc/apt/sources.list.d/docker.list >
   /dev/null
   ```

4. **Instalar Docker:**

   Bash

   ```
   sudo apt update
   sudo apt install docker-ce docker-ce-cli containerd.io -y
   ```

5. **Añadir tu usuario al grupo `docker`** (para poder ejecutar comandos de Docker sin `sudo`):

   Bash

   ```
   sudo usermod -aG docker $USER
   ```

   - **Nota:** Debes **cerrar la sesión y volver a iniciarla** (o reiniciar la MV) para que este cambio surta efecto.

B. Descargar y Ejecutar OWASP Juice Shop

1. **Iniciar Docker (si no se inicia automáticamente):**

   Bash

   ```
   sudo systemctl start docker
   sudo systemctl enable docker
   ```

2. **Descargar la imagen de Juice Shop:**

   Bash

   ```
   docker pull bkimminich/juice-shop
   ```

3. **Ejecutar Juice Shop:** Este comando inicia un contenedor, mapea el puerto 3000 del contenedor al puerto 3000 de tu máquina virtual Linux, y lo ejecuta en segundo plano (`-d`):

   Bash

   ```
   docker run -d -p 3000:3000 bkimminich/juice-shop
   ```

4. Acceder a OWASP Juice Shop

1. **Verificar el estado:** Asegúrate de que el contenedor de Docker esté funcionando:

   Bash

   ```
   docker ps
   ```

   Deberías ver un contenedor de `bkimminich/juice-shop` con el estado `Up`.

2. **Acceder desde la MV (Linux):** Abre el navegador web dentro de tu máquina virtual y navega a:
3. `http://localhost:3000`
4. **Acceder desde el Anfitrión (Tu PC):** Si usaste el modo de red **NAT** y quieres acceder desde tu sistema anfitrión, necesitas obtener la dirección IP de tu MV Linux:

   Bash

   ```
   ip a
   # o si no tienes 'ip a':
   ifconfig
   ```

   Busca la dirección IP (ej: `10.0.2.15` si es NAT por defecto en VirtualBox) y luego en tu navegador anfitrión navega a:

   ```
   http://[IP_de_la_MV]:3000
   ```

   - **Nota de Redes:** Si deseas que la MV tenga una IP accesible en tu red local (como si fuera un equipo más), considera cambiar el adaptador de red de VirtualBox a **"Adaptador Puente" (Bridged Adapter)**.

Puedes ver la **instalación detallada de OWASP Juice Shop** mediante Docker y la resolución de vulnerabilidades en el siguiente video:

https://www.youtube.com/watch?v=2Q7SGy9dNd8

Este video es relevante porque ofrece un tutorial detallado sobre la instalación paso a paso de OWASP Juice Shop, que es el tema principal de tu solicitud.

5. Ejercicio práctico sencillo

Ataque de Inyección SQL (SQL Injection) para iniciar sesión como administrador sin conocer la contraseña.

Este ejercicio es de dificultad baja a media y te introduce al concepto de cómo la falta de validación de entradas puede comprometer la autenticación.

Ejercicio: Desafío "Login Admin" (Inyección SQL)

Contexto del Ejercicio

- **Vulnerabilidad: Inyección SQL (SQLi)**, que es la vulnerabilidad número 1 en el OWASP Top 10 (A03:2021 - Inyección).
- **Objetivo:** Iniciar sesión con la cuenta del administrador (cuyo correo electrónico es `admin@juice-sh.op`) sin conocer su contraseña, explotando una mala práctica de codificación en el formulario de inicio de sesión.
- **Funcionamiento Esperado:** El código detrás del login probablemente toma tu entrada y construye una consulta SQL similar a esta:

  SQL

  ```
  SELECT * FROM Users WHERE email = '[TU_EMAIL]' AND password =
  '[TU_PASSWORD_HASHEADA]';
  ```

- **El Ataque:** Inyectaremos una cadena especial en el campo de correo electrónico para alterar la lógica de la consulta SQL y forzar que la condición de `WHERE` siempre sea **verdadera** para el administrador.

Guía Paso a Paso

Paso 1: Acceder al Formulario de Inicio de Sesión

1. Abre tu navegador dentro de la máquina virtual (o en el anfitrión, si configuraste el acceso) y ve a la dirección de Juice Shop: `http://localhost:3000` (o la IP de tu MV en el puerto 3000).
2. Haz clic en el icono de la cuenta (👤) en la esquina superior derecha y selecciona **"Login"** (Iniciar sesión).

Paso 2: Preparar el Payload de Inyección SQL

Necesitas encontrar una cadena que, al ser insertada en el campo de correo electrónico, haga que la consulta devuelva verdadero y omita la verificación de la contraseña.

El *payload* (cadena de ataque) más común para este escenario es:

```
' or 1=1--
```

Donde:

- `'` **(comilla simple):** Cierra la comilla de apertura del campo email en la consulta SQL.
- **`or 1=1`:** Agrega una condición que siempre es verdadera a la consulta (`o verdadero`).
- **`--` (doble guion):** Es el símbolo de comentario en SQL. Esto hace que todo lo que venga después en la consulta (incluida la verificación de la contraseña) sea ignorado por el motor de la base de datos.

Paso 3: Ejecutar el Ataque

1. En el campo **Email (Correo Electrónico)**, ingresa la dirección de correo electrónico del administrador **seguida de tu payload de SQLI**:
2. `admin@juice-sh.op' or 1=1--`

   Nota: En algunas versiones o configuraciones de Juice Shop, solo necesitarás el payload `' or 1=1--` sin la dirección de correo electrónico del administrador, pero usarlo con el email asegura que se seleccione al administrador.

3. En el campo **Password (Contraseña)**, puedes escribir **cualquier cosa** (ej: `a`).
4. Haz clic en el botón **"Log in"** (Iniciar sesión).

Paso 4: Confirmación del Desafío

Si el ataque fue exitoso, la aplicación te permitirá **iniciar sesión como el usuario administrador**.

1. Verás que el icono de la cuenta ha cambiado y al hacer clic en él, verás opciones de "Administración".
2. En la esquina inferior derecha de la pantalla, aparecerá una notificación emergente indicando que has resuelto el desafío: **"Login Admin"**.

Explicación

Al inyectar la cadena, la consulta SQL que se ejecuta en el servidor se transforma de (ejemplo simplificado):

Consulta SQL original (con un intento fallido)

```
SELECT * FROM Users WHERE email = 'usuario@ejemplo.com' AND password =
'hash_incorrecto';
```

A esto (consulta inyectada):

Consulta SQL inyectada (exitosa)

```
SELECT * FROM Users WHERE email = 'admin@juice-sh.op' or 1=1-- ' AND
password = 'hash_de_a';
```

El motor de la base de datos interpreta lo siguiente:

- "Selecciona todos los usuarios donde el email es igual a 'admin@juice-sh.op' **O** donde 1 sea igual a 1."
- Como la condición `1=1` siempre es verdadera, la cláusula `OR` garantiza que la condición `WHERE` se cumpla, haciendo que la base de datos devuelva los datos del primer usuario que cumpla con la condición, que en este caso es el administrador.
- El `--` ignora el resto de la consulta, incluyendo la verificación de la contraseña.

Solución y Mitigación

Para prevenir esta vulnerabilidad en una aplicación real, los desarrolladores deben usar:

- **Consultas Preparadas (Prepared Statements):** El uso de *placeholders* o parámetros en el código hace que el input del usuario sea tratado siempre como un valor de dato y nunca como parte del comando SQL, neutralizando la inyección.
- **Validación de Entrada:** Aplicar un filtro estricto para asegurarse de que el email tenga el formato correcto y rechazar caracteres peligrosos como `'`, `--`, etc.

--- Ejercicio y configuración construido con IA