

295 - SEGURIDAD

Hacking ético web: escanea tu laboratorio con ZAP

Monta una tienda vulnerable a propósito en tu equipo y aprende a encontrar fallos web con ZAP para saber proteger tus propias webs.



NIVEL
Avanzado

TIEMPO
60 min

CATEGORÍA
Seguridad

WEB
soporteinformatico360.com

La mejor forma de entender los fallos de una web es verlos en un entorno seguro. Vas a levantar OWASP Juice Shop, una tienda creada para practicar, y analizarla con ZAP, un escáner gratuito y de código abierto. Todo ocurre dentro de tu propio ordenador.

■ Qué necesitas

- ✓ Un ordenador con Docker instalado
- ✓ ZAP descargado de su web oficial (zapproxy.org)
- ✓ 8 GB de RAM o más
- ✓ Hacerlo solo en tu laboratorio

■ Paso a paso

01

Levanta la tienda vulnerable

Arranca Juice Shop en un contenedor. Solo se publica en tu propio equipo, en el puerto 3000.

Terminal

```
$ docker run --rm -p 127.0.0.1:3000:3000 bkimminich/juice-shop
$
```

02

Comprueba que funciona

Abre el navegador y entra en <http://localhost:3000>. Deberías ver una tienda de zumos de ejemplo.

Navegador

```
http://localhost:3000
OWASP Juice Shop
```

03

Abre ZAP y elige el escaneo

Inicia ZAP, acepta no guardar la sesión y pulsa «Automated Scan» en la pantalla de inicio.



04

Apunta solo a tu laboratorio

En «URL to attack» escribe `http://localhost:3000` y pulsa «Attack». Nunca pongas la dirección de una web que no sea tuya.

ZAP - Automated Scan

URL to attack:
`http://localhost:3000`

Attack

05

Lee las alertas

En la pestaña «Alerts» verás fallos ordenados por riesgo: alto, medio, bajo e informativo. Cada alerta explica el problema y cómo corregirlo.

06

Aplicalo a lo tuyo

Usa lo aprendido para revisar tu propia web con su desarrollador: cabeceras de seguridad, formularios y versiones antiguas.



07

Apaga el laboratorio

Al terminar, pulsa `Ctrl + C` en la terminal de Docker. Con `--rm` el contenedor se borra solo.



■ Consejos

CONSEJO 1

Antes de escanear tu web real en producción, haz una copia de seguridad y avisa a tu proveedor de alojamiento.

CONSEJO 2

Empieza por el escaneo pasivo: solo observa el tráfico y no modifica nada.

CONSEJO 3

Si las alertas te superan, un técnico puede ayudarte a priorizar qué corregir primero.



Importante: Usa ZAP solo contra tu laboratorio o webs propias con permiso por escrito. Escanear o atacar sistemas ajenos sin autorización es delito. Un escaneo activo puede llenar formularios y bases de datos de prueba, así que nunca lo lances contra una web real sin preparación.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar. sosporte@soporteinformatico360.com
En taller, a domicilio en Madrid o por asistencia remota. soporteinformatico360.com

910 117 112