Introducción a OWASP ZAP y Badstore para análisis de seguridad web

---

¿Qué es OWASP ZAP?

OWASP ZAP (Zed Attack Proxy) es una herramienta gratuita y de código abierto diseñada para **detectar vulnerabilidades de seguridad en aplicaciones web**. Es mantenida por OWASP, una organización internacional reconocida por su labor educativa en seguridad informática.

¿Qué hace ZAP?

- Intercepta y analiza el tráfico entre tu navegador y un sitio web
- Detecta vulnerabilidades comunes como:
  - Inyección SQL (SQLi)
  - Cross-Site Scripting (XSS)
  - Cookies inseguras
  - Cabeceras mal configuradas
  - Rutas ocultas o expuestas
- Permite realizar escaneos pasivos (sin alterar el sitio) o activos (más invasivos)
- Ayuda a los desarrolladores y pentesters a encontrar errores antes de que lo hagan los atacantes

---

¿Cómo se usa OWASP ZAP?

ZAP puede ejecutarse de dos formas:

A. Desde Kali Linux:

```
bash
CopyEdit
zaproxy &
```

Luego debes configurar tu navegador para que use ZAP como proxy (generalmente en `127.0.0.1:8080`).

B. Desde Docker:

```
bash
CopyEdit
docker run -u zap -p 8080:8080 -i owasp/zap2docker-stable zap.sh
```

Al usar ZAP como proxy, puedes:

1. Navegar la aplicación normalmente
2. ZAP capturará todo el tráfico y lo analizará en tiempo real
3. Puedes lanzar un escaneo activo cuando estés listo

¿Qué resultados entrega ZAP?

- Una lista de alertas clasificadas por nivel de severidad
- Detalles técnicos: URL vulnerable, parámetro afectado, tipo de vulnerabilidad
- Recomendaciones para solucionar el problema
- Reportes en HTML o XML listos para entregar o documentar

¿Qué es Badstore?

Badstore es una aplicación web **intencionalmente vulnerable**, creada para prácticas de seguridad informática. Simula una tienda en línea, pero contiene errores comunes que pueden ser explotados por usuarios éticos en entornos de laboratorio.

¿Qué vulnerabilidades incluye Badstore?

- Formularios vulnerables a inyección SQL
- Campos de búsqueda sin sanitización (XSS)
- Cookies inseguras
- Listados de directorios sin protección
- Accesos administrativos sin autenticación adecuada

Es ideal para comparar con una aplicación "hecha desde cero" (como la de Flask o Node.js en este laboratorio), y así entender qué errores hay que evitar al programar.

¿Cómo se ejecuta Badstore?

Badstore puede correr fácilmente en un contenedor Docker:

```
bash
CopyEdit
git clone https://github.com/rapid7/Badstore-Docker.git
cd Badstore-Docker
docker build -t badstore .
docker run -d -p 8081:80 badstore
```

La aplicación quedará disponible en tu navegador en:

- http://localhost:8081

¿Por qué combinamos ZAP y Badstore?

Porque ZAP permite detectar automáticamente los errores que Badstore incluye de forma intencional. Al escanear Badstore con ZAP, los estudiantes pueden:

- Ver vulnerabilidades reales en acción
- Confirmar que ZAP puede detectarlas
- Comprender cómo y por qué ocurren esos fallos
- Aplicar este conocimiento a sitios propios o en desarrollo

Conclusiones

Herramienta	Propósito
Docker	Desplegar sitios vulnerables en minutos
ZAP	Detectar errores y fallos de seguridad web
Badstore	Simular errores comunes en desarrollo web

Estas herramientas combinadas permiten aprender cómo se realiza el análisis de seguridad desde el punto de vista de un atacante ético o un desarrollador que quiere entregar código más seguro.