



## Módulo introducción a la ciberseguridad

**Objetivo:** Realización de un proyecto de auditoria web básica

### Contenido:

- Information gathering
- OWASP Top 10
- Uso de herramientas de seguridad como sqlmap, nmap o burp proxy
- Realización de un informe de auditoría

## PRÁCTICA

En esta práctica aplicarás diversas herramientas y conocimientos aprendidos durante este módulo. De cara a la realización de la práctica y su cumplimiento se deben seguir los siguientes pasos:

### Primera parte

Esta práctica se centra en la auditoría, solución y escritura de un informe sobre una aplicación web vulnerable. La aplicación web que se utilizará durante la práctica será WebGoat versión 8.1.0, <https://github.com/WebGoat/WebGoat>.

En primer lugar se debe ejecutar este entorno la recomendación es hacerlo con Docker:

- `docker run --name webgoat -it -p 127.0.0.1:8080:8080 -p 127.0.0.1:9090:9090 -e TZ=Europe/Amsterdam webgoat/webgoat`
- `docker start webgoat`
- La aplicación a auditar se encuentra en `http://127.0.0.1:8080/WebGoat`

### Segunda parte reconocimiento

Una vez desplegada la aplicación se realizará un reconocimiento sobre la misma identificando la máxima información posible, como:

- Puertos abiertos
- Sistema Operativo
- Lenguajes de programación utilizados en la aplicación web



## Tercera parte detección y explotación de vulnerabilidades

Al ser esta la primera práctica se ha proporcionado un entorno guiado con diversas vulnerabilidades previamente indicadas.

De cara a una completa realización de la práctica se han de conseguir explotar las siguientes vulnerabilidades:

- A3 Injection - SQL Injection (intro) - Apartado 11
- Intenta obtener toda la información que puedas de la base de datos utilizando los fallos disponibles en la sección A3 Injection - SQL Injection
- A3 Injection - Cross Site Scripting - Apartado - Apartado 7
- A5 Security Misconfiguration - Apartado 4
- A6 Vuln & outdated Components - Apartado 5
- A7 Identity & Auth Failure - Secure Passwords Apartado 4

Opcionalmente también se podrán realizar más ejercicios de otras secciones que serán corregidos.

## Cuarta parte informe de auditoría

Tras haber completado los ejercicios se debe realizar un informe de auditoría indicando todas las pruebas y procesos realizados durante la práctica.

Este informe de auditoría ha de contar con las siguientes secciones como mínimo:

1. Ámbito y alcance de la auditoría
2. Informe ejecutivo
  - a. Breve resumen del proceso realizado
  - b. Vulnerabilidades destacadas
  - c. Conclusiones
  - d. Recomendaciones
3. Descripción del proceso de auditoría
  - a. Reconocimiento/Information gathering
  - b. Explotación de vulnerabilidades detectadas
  - c. Post-explotación
  - d. Posibles mitigaciones
  - e. Herramientas utilizadas

## EVALUACIÓN

Es **obligatorio** la entrega de algún **informe** de auditoría para considerar como **APTA** la práctica. Este informe ha de contener como **mínimo** la explotación de las **vulnerabilidades** indicadas en el **TERCER** apartado.