Actividades Seguridad.

Actividad 1.

# Foro: ¿Qué otras vulnerabilidades conoces en entornos Web que no se mencionen en el top 10?

Actividad 2: Investigación de otras metodologías de desarrollo de aplicaciones Web seguras

[Entregar tarea de nuevo](https://micampus.unir.net/courses/5815/assignments/88488)

* **Fecha límite** 5 de jul hasta 23:55

* **Puntos** 1.3
* **Presentando** un cuadro de entrada de texto o una carga de archivo
* **Disponible** 28 de abr en 10:00-8 de sep en 23:59 4 meses

El trabajo deberá contener una pequeña descripción sobre otras metodologías de Desarrollo Web Seguro además de las ya vistas en el temario o elegir solo una y profundizar más en ella.

Además, deberás elaborar un manual de prácticas básicas de las seguridad de la red informática mundial.

Extensión máxima: 5 páginas.

Actividad 3.

Práctica guiada con WebGoat

[Entregar tarea de nuevo](https://micampus.unir.net/courses/5815/assignments/88489)

* **Fecha límite** 26 de jul hasta 23:55

* **Puntos** 3.4
* **Presentando** un cuadro de entrada de texto o una carga de archivo
* **Disponible** 28 de abr en 10:00-8 de sep en 23:59 4 meses

En esta actividad deberás realizar la [práctica guiada con WebGoatPreview the document](https://micampus.unir.net/courses/5815/files/844275/download?wrap=1). (Tema2/Enunciado\_WebGoat)

La práctica consistirá en un ataque a una aplicación web desplegada mediante la herramienta WebGoat, diseñada a tal efecto.

Para ello, deberá elegir una de las lecciones propuestas por WebGoat y llevarla a la práctica.

El entregable será un documento explicativo con la extensión que considere necesaria (sin límite) donde indique qué realizó para conseguir que el ataque fuera fructífero, escribiendo todos los pasos que haya llevado a cabo y todos los detalles de cómo lo llevó a cabo. Y por último qué efecto produjo sobre la aplicación.

Actividad 4.

Análisis de vulnerabilidades con herramientas Proxy HTTP

**Fecha límite** 16 de ago hasta 23:55

* **Puntos** 4
* **Presentando** un cuadro de entrada de texto o una carga de archivo
* **Disponible** 28 de abr en 10:00-8 de sep en 23:59 4 meses

La práctica consiste en instalar una herramienta Proxy HTTP siguiendo la documentación adjunta.

[Descarga el documento para realizar la actividadPreview the document](https://micampus.unir.net/courses/5815/files/845157/download?wrap=1) (Tema\_2/ PracticaOpcional-ProxyHTTP)

Una vez instalada, deberá elegir una de las lecciones de WebGoat de entre las que es necesario utilizar una herramienta tipo Proxy como WebScarab para conseguir llevar a cabo el ataque.

Algunos de los ataques de WebGoat que requieren el uso de WebScarab u otra herramienta similar son:

* Basic Authentication
* Multi Level Login 1
* Multi Level Login 2
* Command Injection
* Numeric SQL Injection
* Exploit Hidden Fields
* Exploit Unchecked emails

No es obligatorio que elija una de estos. Puede elegir el que más le convenga.

Deberá entregar un documento en PDF de la extensión que considere necesaria donde explique cómo utilizo la herramienta de Proxy HTTP para hacer fructífero el ataque. Se valorará que se ajuntes capturas de pantalla (screenshots), que complementen la explicación y que lo hagan más visual.