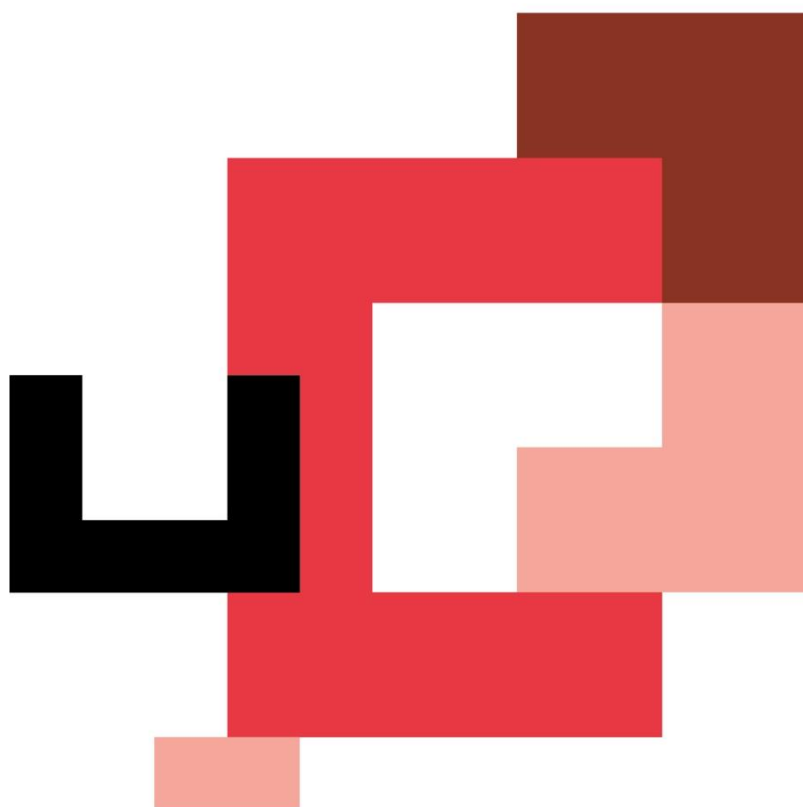




BOOTCAMP

Ciberseguridad en formato online



TEAM CHALLENGE WAF

Prerrequisitos

Para el desarrollo de la siguiente actividad debemos contar con la máquina **Redweb**. En esta máquina debemos instalar **ModSecurity**. Si ya la tienes configurada del Challenge de la unidad 1 puedes reutilizar la misma máquina.

También deberemos contar con nuestra máquina **Kali**, para poder conectarnos a la aplicación DVWA. Para ello debemos conectar las dos máquinas en **RedNat**.

En esta ocasión el nivel de la DVWA la estableceremos en nivel **Medium**

Ejercicio

Para el Team Challenge deberás realizar las reglas para las distintas vulnerabilidades que hemos estudiado sobre aplicaciones web. En esta ocasión deberás hacer uso de la máquina DVWA en nivel medio.

- **Path Traversal**
- **Local File Inclusion (LFI)**
- **Remote File Inclusion (RFI)**
- **Cross Site Scripting reflejado (XSS reflected)**
- **SQL Injection (SQLi)**
- **Remote Code Execution (RCE)**

Una vez creadas las reglas para las siguientes vulnerabilidades deberás acceder a la aplicación web DVWA, establecerla en nivel **Medium**, y corroborar su funcionamiento.





**THE
BRIDGE**

