**# EJERCICIOS COMMAND INJECTION Y WEBSHELL**

**## Prerrequisitos**

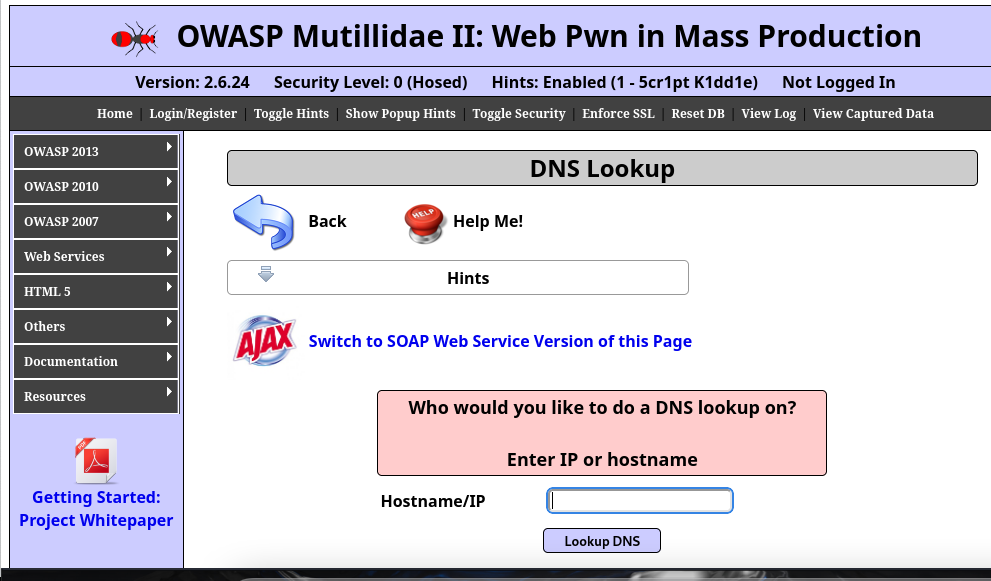
**- Máquina OWASP BWE levantada y Kali.**

**## Ejercicio 1**

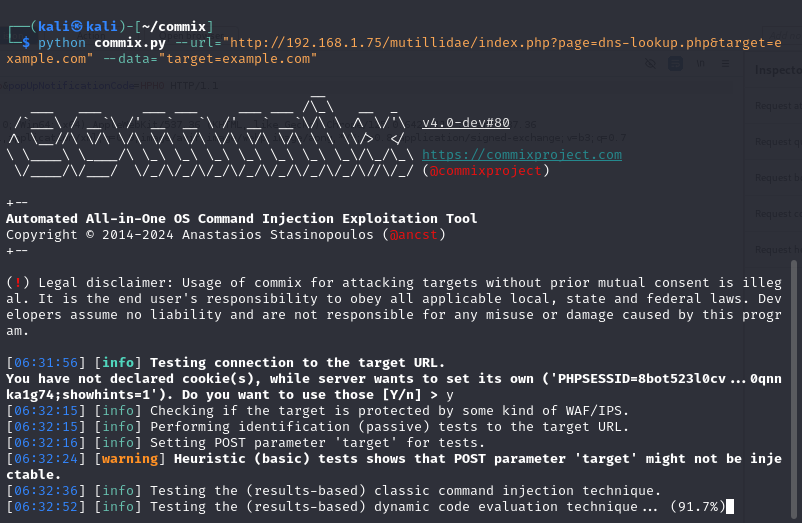
**- Realizar el ejercicio de Command Injection en la máquina Mutillidae:**

**- OWASP 2013 -&gt; A1 - Injection (Other) -&gt; Command Injection -&gt; DNS Lookup**

**- 1.De manera manual**

****

**- 2.Utilizando la herramienta commix**

****

**- 3.Utilizando una webshell C99 (PHP)**

**- Identificar:**

**- Usuario del servicio lanzado**

www-data

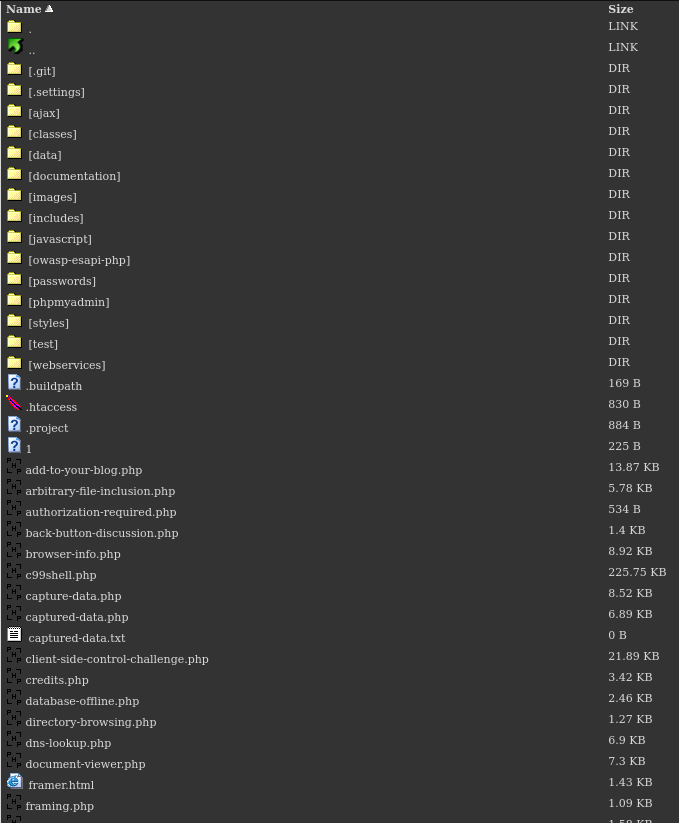
**- Ruta por defecto de la web de Mutillidae**

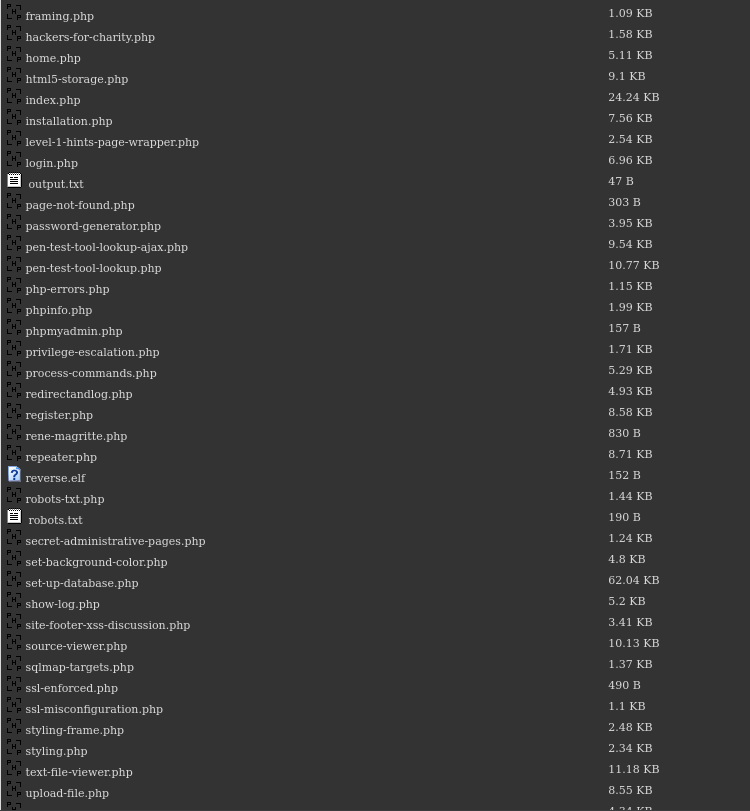
- /owaspwba/mutillidae-git

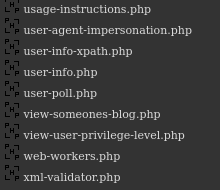
**- Si es administrador de la máquina o no**

No lo es

**- Mapa de la web completa**







**- Si hay ficheros de configuración de la herramienta Mutillidae**

