**EJERCICIOS INTRODUCCIÓN WEB**

**Prerrequisitos**

**Instalar BURP Suite en Kali Linux**

**Instalar FoxyProxy en Firefox de Kali Linux**

**Instalar una CA de BURP Suite en Firefox para análisis de tráfico HTTPS**

**Kali Linux con Dirbuster y Nikto**

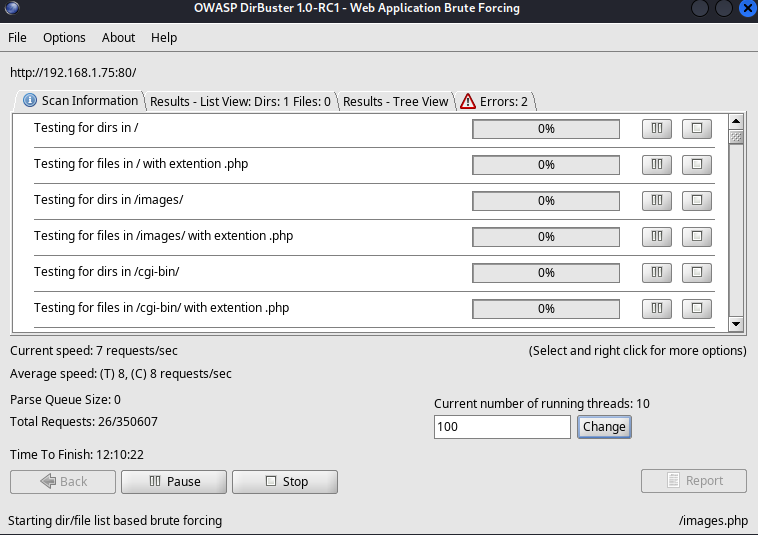
**Máquina OWASP BWA**

**NOTA: La máquina OWASP BWA tiene varias aplicaciones Web desplegadas en su servidor web. Una de ellas es la Multillidae, una aplicación LAMP que**

**iremos utilizando los próximos días para realizar sucesivos ataques Web. Está localizada en la ruta:** [**http://IP\_OWASP\_BWA/mutillidae**](http://ip_owasp_bwa/mutillidae)

**Ejercicio 1 Dirbuster**

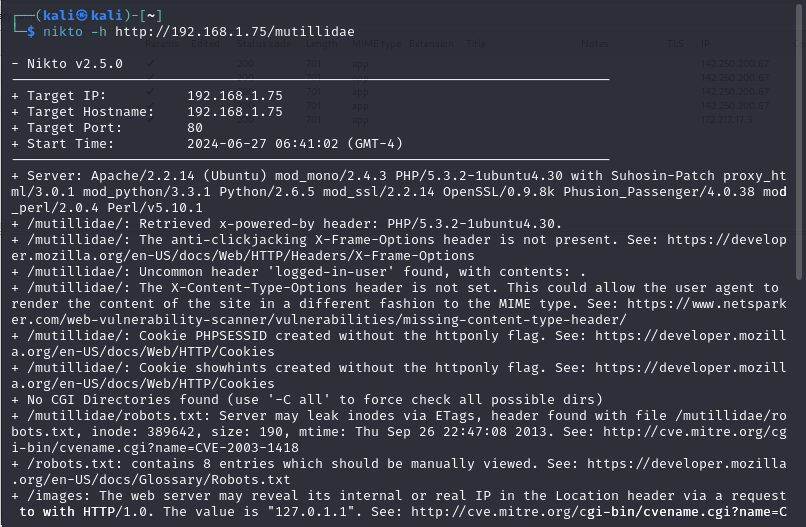
**Realizar un mapa de la aplicación web Mutillidae utilizando Dirbuster y un diccionario de nombres de tamaño medio.**

****

Va a tardar muchisimo tiempo pero basicamente solo queda esperar a que se complete.

**Ejercicio 2 Nikto**

**Realizar un análisis de vulnerabilidades a la aplicación web Multillidae utilizando Nikto.**

****

Lo mismo, estos ejercicios son más bien de esperar a que se procese todo, pero ya está en marcha.

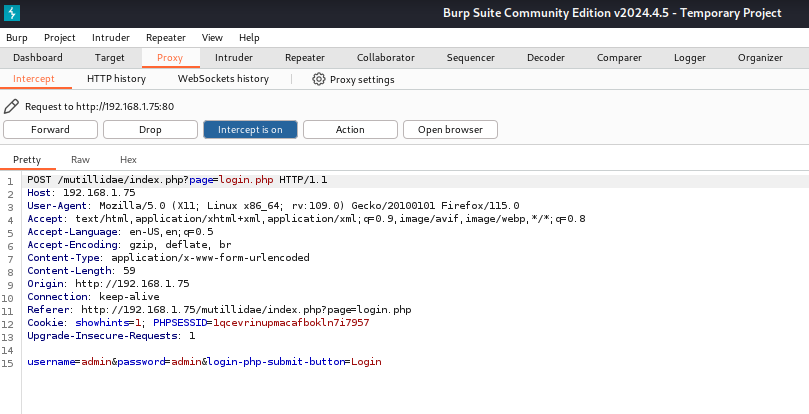
**Ejercicio 3 Burp Suite**

**Utilizando Burp Suite como proxy, y Firefox, cargar la web de Mutillidae, sección "Login/Register": http://IP\_OWASP\_BWA/mutillidae/index.php?**

**page=login.php**

**Interceptar la petición de login y password del formulario con las credenciales Username: admin - Password: admin**

**Continuar y acceder**

****

**Listar las peticiones HTTP que hemos hecho en Burp**

**Filtrar y listar únicamente las de: http://IP\_OWASP\_BWA/mutillidae**

