

Write-up Reto File Upload:

Hecho por *Th3Polyg0t* (parte funcional, y parte de la gráfica, realización del write-up) y Mario Castro (parte gráfica).

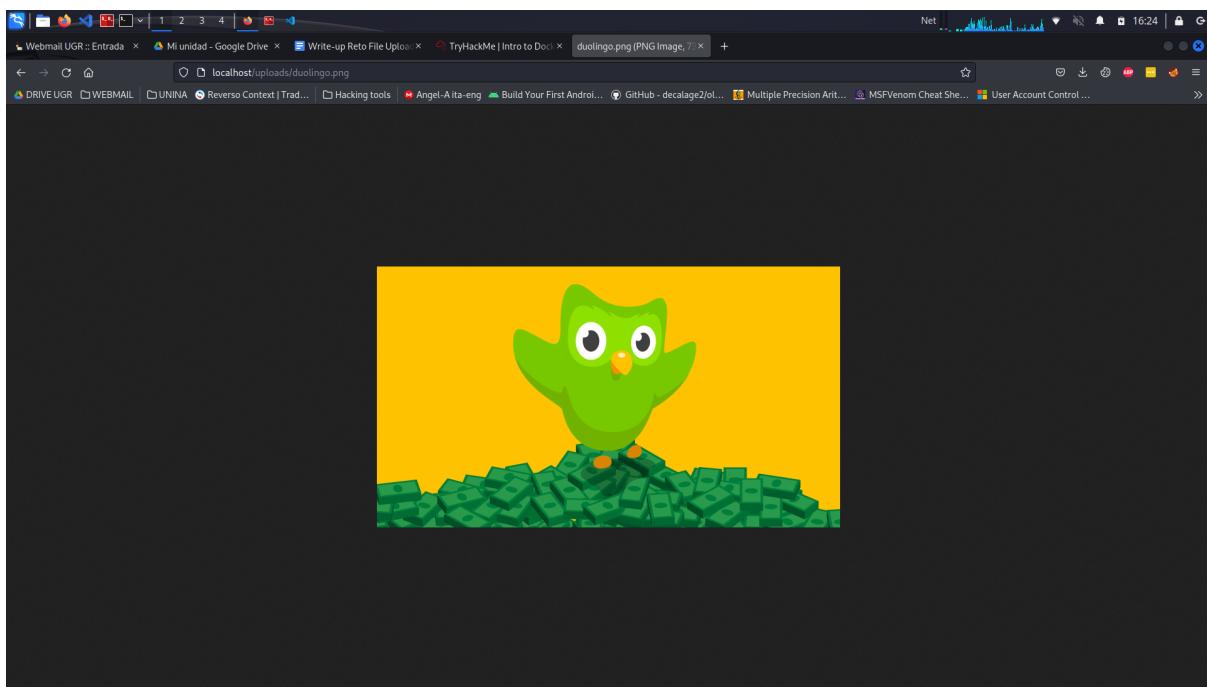
El reto consiste en sobreponer el filtro de una subida de archivos en un servidor web (file upload bypass), el servidor permite la subida de archivos a este pero tiene un filtro para sólo permitir archivos de tipo imagen según la extensión del archivo (jpg, png...).

Sin embargo, el filtro está mal diseñado y permite subir archivos que no sean imágenes con sus correspondientes extensiones.

Si accedemos al servidor se nos redirigirá a una página que nos permite subir imágenes al servidor web.

Si probamos a subir una imagen nos permitirá subirla si tiene una de las extensiones permitidas, si miramos el código HTML de la página veremos que la imagen mostrada en esta página se encuentra en la carpeta uploads/ del servidor de forma que si hemos subido una imagen llamada “prueba.jpg” podremos acceder a ella en el servidor si nos dirigimos a “<http://<IP o nombre del servidor>/uploads/prueba.jpg>”

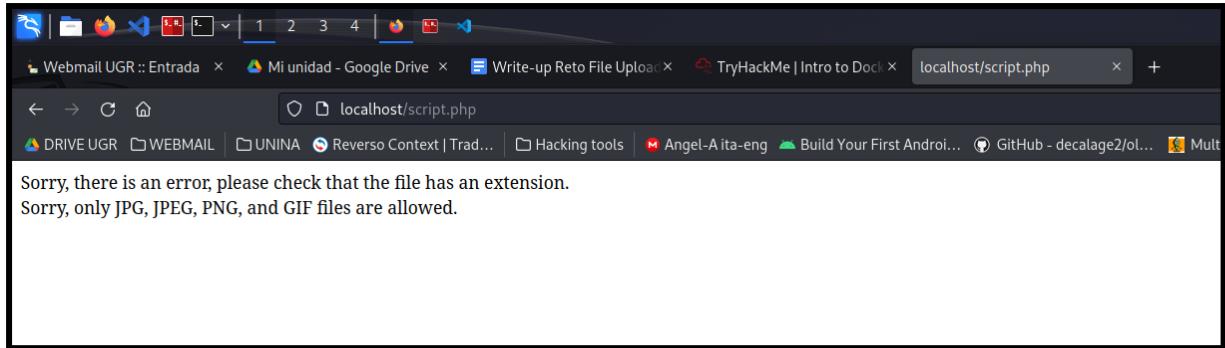




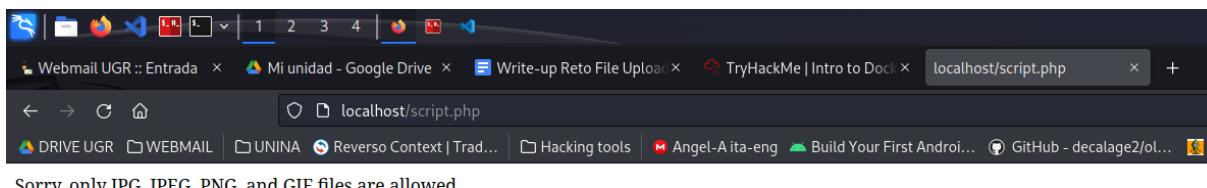
El objetivo del reto es acceder a la flag guardada en el servidor utilizando el código php dado en el propio reto. Si no lo sabías el servidor es un servidor Apache, el cuál ejecuta código php aparte de utilizar html, css... (El código de la página que gestiona la subida de las imágenes es php). Por lo tanto, lo más lógico es pensar que debemos subir este archivo php al servidor y acceder a él para ejecutarlo.

Si probamos a subir un archivo que no tenga extensión nos dará error indicando que hay algún problema con la extensión.





Vamos a probar a subir el archivo php directamente...

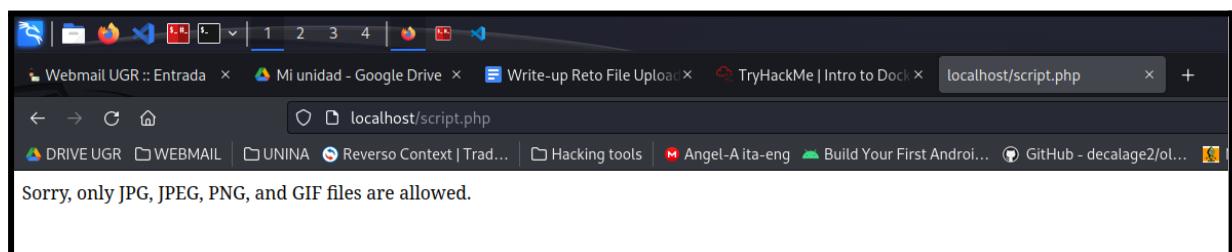


Como vemos, al intentar subir un archivo con la extensión php nos dará error indicando que solo están permitidas las extensiones jpg, jpeg, png y gif.

Si el filtro está comprobando que tenga extensión y que sea una de ellas, podemos probar a subir un archivo que tenga varias extensiones y comprobar que pasa.

Si subimos una imagen que contenga las extensiones .php.png, en ese orden, nos dará error indicando que las únicas extensiones permitidas son las relativas a imágenes (las que

hemos visto antes) lo que nos indica que realmente sólo está comprobando la primera extensión del archivo, por lo que si a nuestro archivos le añadimos .png o cualquier otra extensión después del nombre estos podemos subir el archivo al servidor.



Podemos entonces renombrar el archivo `readFlag.php` a `readFlag.png.php` y así poder subir el archivo al servidor. (ES MUY IMPORTANTE QUE EL ARCHIVO TERMINE EN `.php`, el servidor ejecutará el código `php` solo si la extensión del archivo al que acceder es una extensión `php`).

Por lo tanto solucionar el reto es tan fácil como darse cuenta de que el servidor sólo comprueba la primera extensión del archivo y renombrar el archivo `php` que se quiera subir a "nombre.png.php" (o cualquier otra extensión permitida en vez de "png"), después habría que acceder a este archivo en la carpeta `uploads/`, es decir:

`http://<ip del servidor>:<puerto>/uploads/<nombree>.png.php`

1. Renombrar `readFlag.php` en `readFlag.png.php`
2. Subir el archivo al servidor
3. Acceder a "`http://<IP o nombre del servidor>:<puerto>/uploads/readFlag.png.php`"

