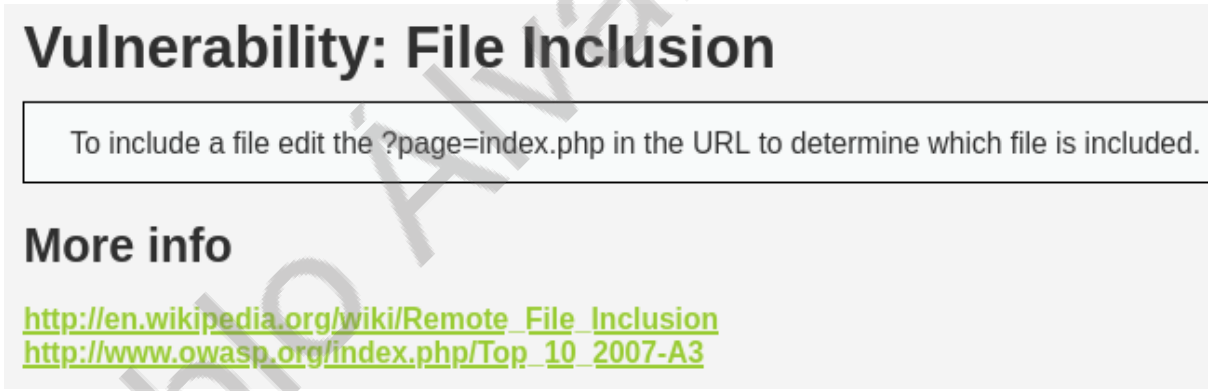
Vulnerabilidades Web para la eWPT

File Inclusion

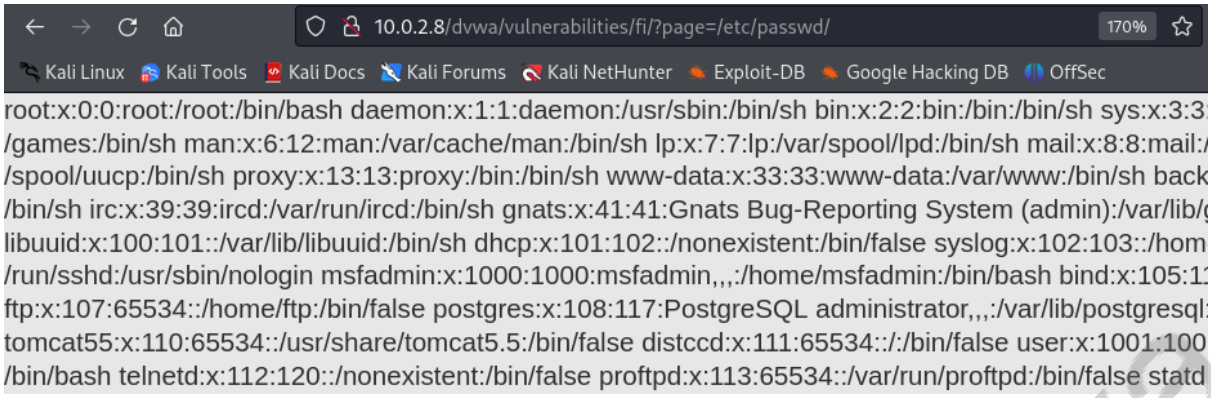
Comenzamos en la DVWA de Metasploitable seleccionando un nivel de dificultad bajo.



Y nos dirigimos a la sección de File Inclusion. Que comienza dándonos una pista de que debemos modificar el valor de la variable page que pasa por la URL por el método GET.

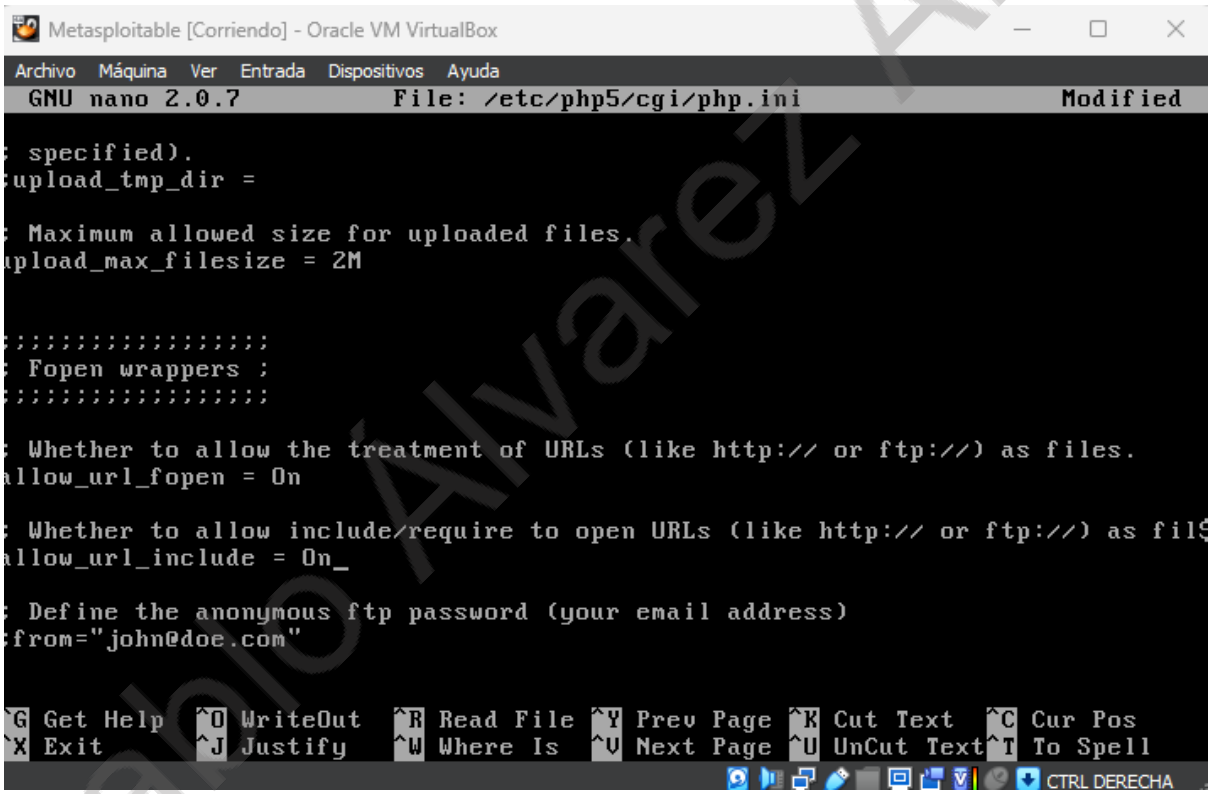
Entonces probaremos haciendo la inclusión de un código mediante lo que sería la URL de la página reemplazando el valor de la variable page por el siguiente comando:

Comando: /etc/passwd



Podemos ver que es posible solicitar información al servidor de manera indirecta.

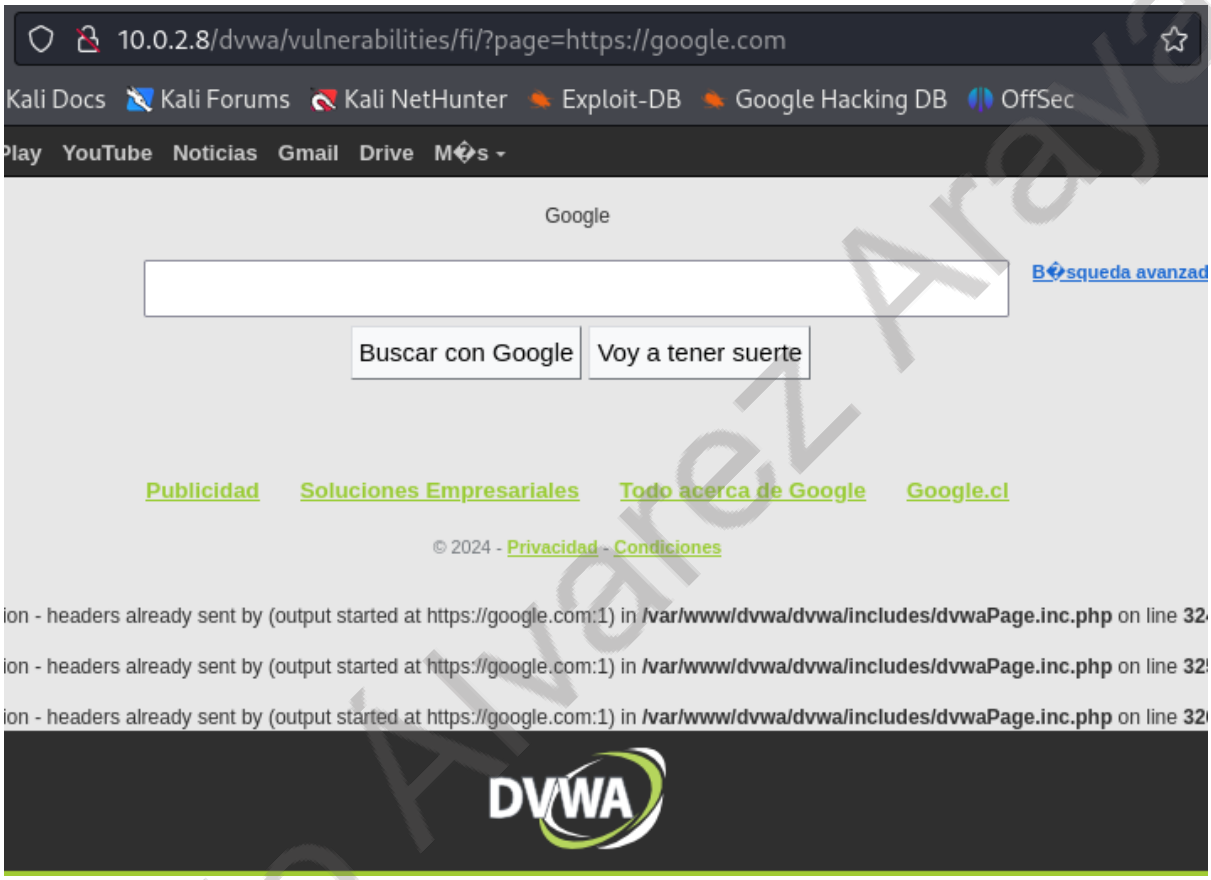
Para continuar con esta prueba de concepto iremos a nuestra máquina de Metasploitable a modificar el archivo php.ini de apache donde cambiaremos el calor de Allow_url_fofen = **On**



Guardamos los cambios y reiniciamos el servidor apache

Y esto lo que nos permitirá será incluir otros sitios web desde la URL donde modificamos la variable page

En este ejemplo podemos ver que he incluido en la propia página de DVWA el buscador de Google.



La idea sugiere que si podemos incluir servicios web, entonces podemos incluir archivos que vengan desde un servicio web.

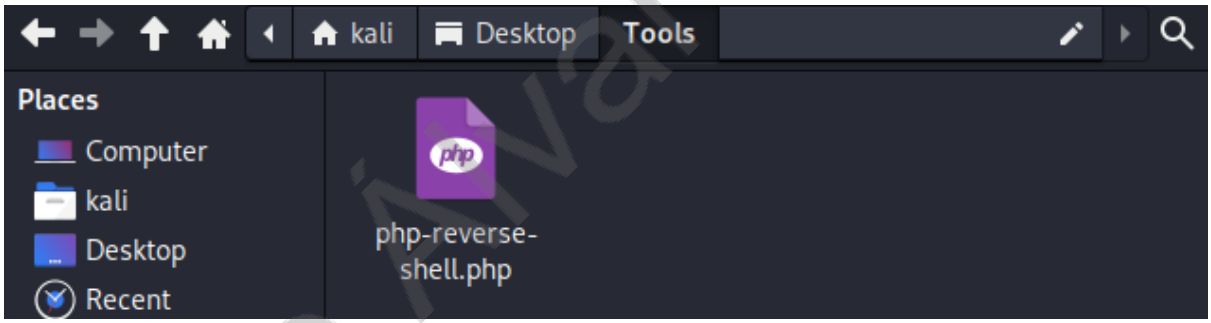
Para esto probaremos un método que consiste en levantar un servidor web con python para mandar a traer un archivo desde ese servidor:

Comando: sudo python3 -m http.server

Comando: wget 10.0.2.6:80/user.txt

Vemos que no ha sido posible efectuar el ataque con este método. Así que probaremos con un segundo método:

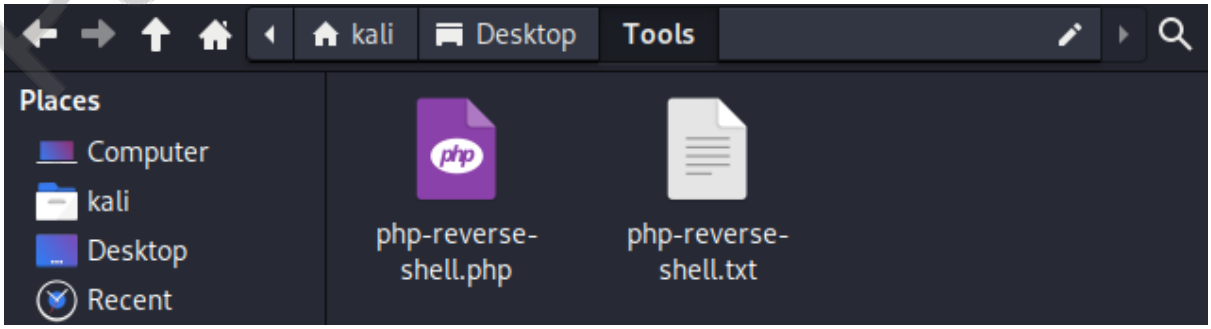
Tenemos un script llamado php-reverse-shell.php



El cuál podemos descargar de la siguiente utilidad:

https://github.com/pentestmonkey/php-reverse-shell/tree/master

Una vez descargado vamos a crear una copia con extensión .txt

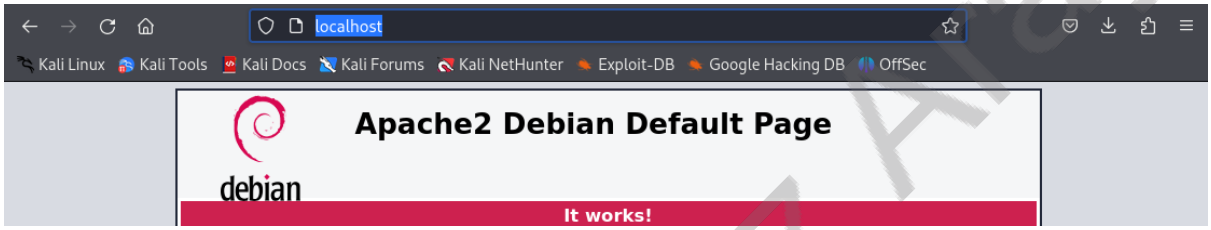


Entonces vamos a crear un servidor que nos permite incluir archivos de forma remota.

Para eso nos vamos a ubicar en la misma ruta donde tenemos el script y vamos a levantar un servidor apache

```
┌──(kali㉿kali)-[~/Desktop/Tools]
└─$ ls
php-reverse-shell.php  php-reverse-shell.txt

┌──(kali㉿kali)-[~/Desktop/Tools]
└─$ sudo service apache2 start
[sudo] password for kali:
```

Comando: sudo service apache2 start



Podemos verificar navegando a localhost que ya tenemos montado nuestro servidor apache.

Si nos movemos a /var/www/html podemos ver los archivos que mantienen nuestro servidor apache:

```
┌──(kali㉿kali)-[/var/www/html]
└─$ ls
index.html  index.nginx-debian.html
```

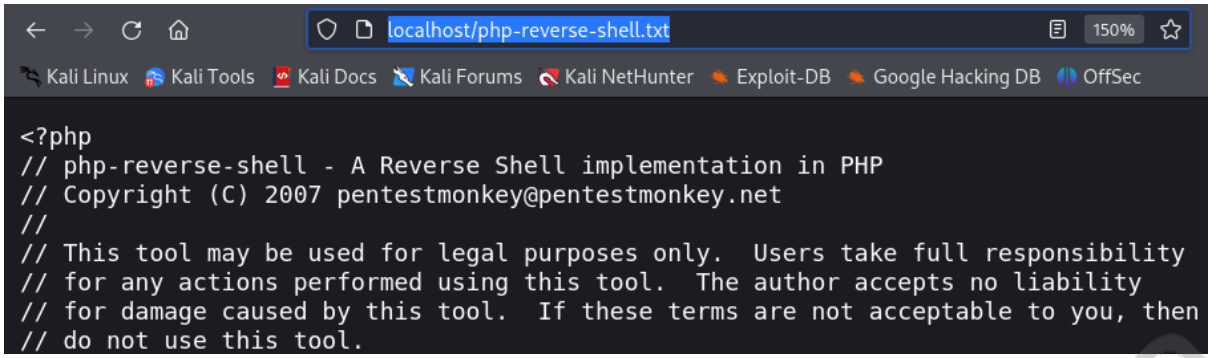
Comando: cd /var/www/html
Comando: ls

Así que moveremos a esa ruta nuestro script

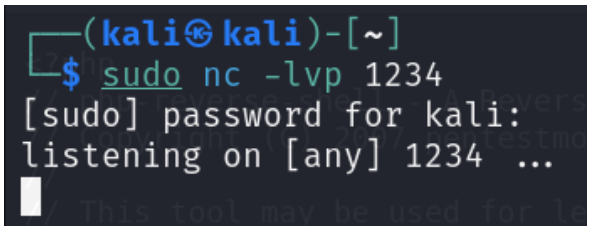
```
┌──(kali㉿kali)-[/var/www/html]
└─$ sudo mv /home/kali/Desktop/Tools/php-reverse-shell.txt /var/www/html

┌──(kali㉿kali)-[/var/www/html]
└─$ ls
index.html  index.nginx-debian.html  php-reverse-shell.txt
```

Comando: sudo mv /home/kali/Desktop/Tools/php-reverse-shell.txt /var/www/html

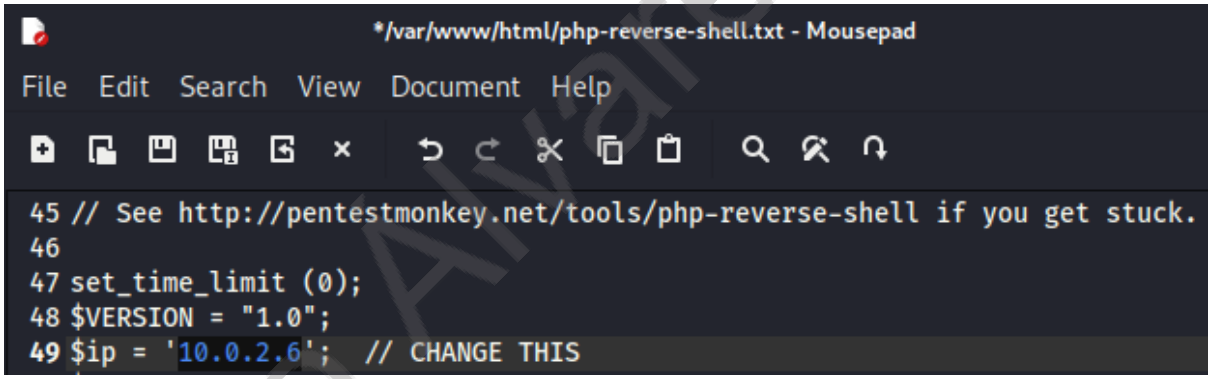
Como podemos ver, en este servidor ya tenemos el archivo a extraer



Nos pondremos a la escucha en Netcat

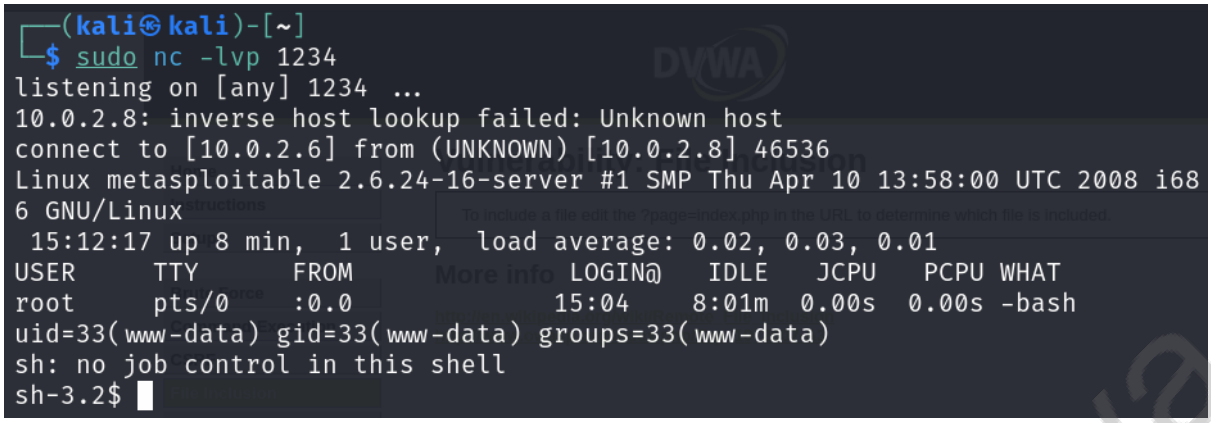


Para que nuestro ataque surta efecto vamos a modificar la IP de localhost por la de nuestra máquina atacante:



Finalmente, vamos a incluir la ruta donde se encuentra nuestro script por la URL

Con este método hemos ganado una reverse shell que nos ha dado acceso a la máquina



Impacto y consecuencias de la vulnerabilidad:

En conclusión; La vulnerabilidad de inclusión de archivos puede tener un impacto significativo y generar diversas consecuencias negativas. Algunas de ellas son:

Divulgación de información sensible.

Ejecución de código malicioso.

Manipulación del comportamiento de la aplicación.

Escalada de privilegios.